Contents

An Introduction to Cybersecurity 4

Summary of Recent Attacks and Motivation for CAP Action 5

Activity Group One: Codes, Ciphers and Encryption Awareness 7

Unit Profile: Room 40 and Bletchley Park 14
Biography: Alan Turing 14

Concepts in Information Assurance and Cyber Warfare 15

Activity Group Two: Vulnerabilities and Basic Defense Skills 16

Unit Profile: USCYBERCOM 22
Patriot Bio: Gen. Keith Alexander 22

A Tale of Two Operating Systems: DOS and Windows and *NIX 16

Activity Group Three: Basic Probing Skills 17

Unit Profile: 24th Air Force & 67th Network Warfare Wing 36
Patriot Bio: Col. Kevin B. Wooton 36

Exploring Careers in Cybersecurity 37

Activity Group Four: Preparation for Cyber Patriot 41

Unit Profile: 688th Information Operations Wing 44
Patriot Bio: Col. Robert J. Skinner 44

Conclusion and Next Steps (Checklist for Action) 45

Activity Group Five: End of Module Exam 46

Appendices
A. Motivational Chronology of Cyber Warfare 37
B. Glossary of Terms, Threats and Countermeasures 54
C. Toolbox of Promotional Resources 68
D. Toolbox of Technical Resources 72
E. Solutions to Module Activities and Exam 74
An Introduction to Cybersecurity

Our Nation's Cyber Dependency

At all its various levels, the United States has become a “cybernation.”

Aviators will be amused to discover the prefix “cyber-“ is derived from the word cybernetic, which comes from a Greek word κυβερνητικός (kybernētēs) which means pilot, rudder, steersman, or governor. Some early cybernetic applications will be reviewed in the Chronology Appendix.

Every aspect of American culture, commerce, public safety, and national defense is now inextricably dependent upon systems of networked computers. These systems make our nation competitive and safe. However, our dependency on computers and networks is not without risk. Our economy and national defense would be seriously disrupted if the networked computer systems on which we depend became unreliable or unavailable. Anyone driving on the Eisenhower Interstate System eventually sees the signs and recognizes transportation to be a vital to national security and our economy. Should key data access be denied or corrupted, problems with signal lights at busy interchanges or intersections or with Air Traffic Control flight plans could grind our nation to a halt.

Cyber Attackers

Some individuals (“hackers”) electronically break into networked computer systems just to prove they can. In other cases, well organized groups break into systems to conduct illicit financial transactions including stealing people’s credit card numbers. Better funded groups have recently penetrated US systems to corrupt data, sabotage operations and conduct espionage to include capturing aircraft performance and avionics data.

Cybersecurity

Cybersecurity is the professional practice of identifying vulnerabilities and countering threats of exploitation or disruption to computers, smart phones and network systems. For most of us, it involves doing very simple things such as setting strong passwords, using encryption for our wireless networks, ignoring suspicious links or attachments and not responding to “phishing” emails. At management levels, we do not transmit DOD contractor design data across unsecured channels. At technical levels, we work to employ good configuration control with correct firewall and port settings, and router configurations. In all cases, we as patriots do the necessary things to ensure that the cybernetic systems on which we depend are trustworthy, confidential, accessible, and secure.

CAP Cybersecurity Module

The purpose of this module is to introduce all of our readers to current threats in Cyberspace and to provide some immediate activities for improving our collective awareness and defense. A summary of careers in computer and network security is provided. This module also serves as a primer for those seeking to compete in the Cyber Patriot Program sponsored by the Air Force Association.

The battlefield is vast and so we provide checklists, a chronology and a very practical glossary of common terms in the appendices. You can use the chronology to motivate recruits. You can use the glossary to look-up concepts and commands and rapidly build your understanding. Interactive and interlinked versions of this material are provided at the Civil Air Patrol’s Cyber Patriot Portal.
Summary of Recent Attacks and Motivation for Action

In August of 2003, CSX passenger and freight trains in the Washington D.C. area were stopped after the company's telecommunications network was overtaken by the Sobig.F worm.

The Sobig.F worm self-deactivated on September 10, 2003. Microsoft announced that they would pay $250,000 for information leading to the arrest of the creator of the Sobig worm. To date, the perpetrator has not been caught.

In 2007, McAfee, Inc. alleged that the People's Republic of China was actively involved in "cyberwar," and had initiated cyber-attacks on the nations of India, Germany, and the United States.

Two years later, McAfee releases a 37-page report observing that “The line between cyber crime and cyber war is blurred in large part because nation-states have already demonstrated that they are willing to tolerate, encourage or even direct criminal organizations and private citizens to attack enemy targets.”

In June of 2007, the Pentagon forced 1500 computers off line as a result of cyber attacks. "The nature of the threat is large and diverse, [...]" said US Navy Lt Cmdr Chit Peppler, a Pentagon spokesman.

In 2008, the Pentagon reported a total of 360 million attempts to break into its networks, up from just 6 million in 2006. This included a report in the Wall Street Journal about a successful cyberespionage attempt to hack into the $300 billion Joint Strike Fighter project and copy data about the aircraft's design and electronics systems.

In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. The intruders seek to navigate and map the infrastructure.

Many of the intrusions were detected, not by the companies in charge of the infrastructure, but rather by U.S. intelligence agencies. Intelligence officials maintain concerns that cyber-attackers could take control of electrical facilities, nuclear power plants or financial networks during a time of conflict.

In December 2009 through January 2010, a cyber-attack dubbed Operation Aurora was launched from China against Google and over 20 other companies. Google determined the attacks originated from China and is currently set to "review the feasibility" of its business operations in China.

In June of 2011, spear-phishing attacks on White House staffer Gmail accounts are traced to Jian, PRC. The People's Republic of China denied any involvement.
Sony PlayStation Network Hacked

In April of 2011, Sony’s PlayStation network was hacked and user account information to include names, passwords and credit card data was compromised.

Crackers later broke into Sony Pictures’ website and compromised the accounts of over 1 million users. The gaming company Sega was also violated with nearly 1.3 million users’ details compromised. Sega makes games for PlayStation and other gaming systems.

In June, an 18-year old was arrested in London under suspicion of “hacking into systems and mounting denial of service attacks against a number of international businesses and intelligence agencies,” police said. The thought was that this suspect was the leader of Lulz Security, or LulzSec, a band of hackers who appear to be responsible for a string of high-profile and sometimes embarrassing Internet attacks.

Their most notable strike was a distributed denial-of-service attack on 15 June 2011 that actually shut down the Central Intelligence Agency’s website for several hours. On 17 June, the group posted an irreverent denial that it was their leader who had been arrested.

"The main anti-LulzSec argument suggests that we’re going to bring down more Internet laws by continuing our public shenanigans, and that our actions are causing clowns with pens to write new rules for you,” the group wrote. "But what if we just hadn’t released anything? What if we were silent? That would mean we would be secretly inside FBI affiliates right now, inside PBS, inside Sony... watching... abusing... ."

On 1 August 2011, the arrested teenager was released on bail and soon after... Anonymous hackers penetrated FBI contractor ManTech International. Documents belonging to NATO, the U.S. Army, the U.S Department of Homeland Security and the U.S. State Department were said to have been compromised.

The message from some youthful leaders of various hacker organizations is that trusted agencies and employers need to do a much better job of ensuring our national and economic security. This seems to be supported by a recent audit by the Department of Justice, which found the FBI unprepared.

Operation Shady RAT

On 3 August 2011, a McAfee report revealed the scope of a five year long hacking offensive. The McAfee VP of threat research believes a state-sponsored attacker was after sensitive data to gain “military, diplomatic and economic advantage”, such as schematics, emails and negotiation info.

“This is the biggest transfer of wealth in terms of intellectual property in history. The scale at which this is occurring is really, really frightening. Companies and government agencies are getting [...] pillaged every day. They are losing economic advantage and national secrets to unscrupulous competitors," he said.

A few of McAfee's competitors dismiss the report and suggest that the firm may be “grandstanding.” However, there have been recent high-level resignations and the US-CERT (Computer Emergency Response Team) has advised that nation-states are most capable of funding and equipping individuals and teams of cyberespionage professionals.
Activity Group One: Codes, Ciphers and Encryption Awareness

In precise terms, a code is when a secret meaning is assigned to a word or a phrase. During World War II, code phrases were broadcast over radio programs to resistance fighters. In this activity group, we will explore the difference between codes, ciphers and professional encryption.

Activity 1.1: Caesar's Simple Substitution Cipher

Objective: The objective of this activity is to introduce early attempts to secure military messages with the simple and consistent substitution of one character for another. In the era before computers, an enemy who intercepted "such meaningless scribble" might completely disregard it. Others would at least be slowed to act by the time required to decipher. In the modern computer age, students will quickly see the flaw with this approach. The cipher can be broken by finding the most frequent character in the cipher text and translating this to the most frequent letter of the native alphabet.

Materials You Will Need:
1. Pencil and paper, ideally graph paper but any paper will do.
3. [Optional] Internet access to a preferred Search Engine for online cipher programs.

Mission Briefing:

Whenever Julius Caesar needed to send information of military importance, he would write it in a character transposition cipher, in which each letter of the plaintext message is shifted a key number of characters. This is called rotN encoding or a wheel cipher. The alphabet can be written on two concentric disks and the inner wheel rotated N characters left or right, to create a mapping.

Try to decipher the text in the third column to generate the original plaintext of the secret message.

Answers to selected activities are provided in the Solutions Appendix at the back of this module.

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Hint</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>rot-1</td>
<td>HAL Bnlotstdqr deehbdmskx rddj zmrvdq.</td>
<td></td>
</tr>
<tr>
<td>rot13</td>
<td>Tyvqref jvyy qrcneg ng qnja gb qryvire grnz puneyvr enatref gb gur evire oevqtr.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tpiewi hvmro qsvi Szepxmri.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ahuahv ghsduwhg vduglv zlwk d iohhw dqg wklubw-wkrxdqg kruvhphq</td>
<td></td>
</tr>
</tbody>
</table>

If you are having trouble, remember that the letter “e” has highest frequency of occurrence in the English language. For this reason, simple substitution ciphers are not considered encryption.

Wheel ciphers can be quickly broken by writing the standard alphabet in a line and then writing the rotated alphabet above it, starting at what you believe might be the letter E. Lets say the letter G had a high frequency in the cipher and the language was expected to be English.

GHIJKLmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ

7
You would then, of course, complete the mapping by moving to the beginning characters and filling those in as shown below. We use red text to distinguish the second step.

\[
\begin{align*}
\text{ABCDGHIJKLMNOPQRSTUVWXYZAB} \\
\text{ABCDEFGHIJKLMNOPQRSTUVWXYZ}
\end{align*}
\]

So when you encounter a G in the ciphertext, you write down the letter E and move to the next letter in the ciphertext. If that letter is N, you would write down L... and so on until you have deciphered the message into a readable plaintext.

**Conclusion**: You've seen how easy it is to crack Simple Substitution Ciphers by hand. It is even easier for computers to scan for most frequent characters and try potential shifts. You now understand why this approach is not considered a secure form of encryption.

**Questions for Further Consideration or Research:**
1. Can you find an online computer program to count the letters (or characters) of any ciphertext?
2. How might you use such a program?
3. Can you recall (or find) any substitution ciphers used throughout history, business or fiction?
4. Can you suggest any methods to overcome the limitations of substitution ciphers?

**Activity 1.2: Jefferson’s Cipher for the 1803 Lewis and Clark Expedition**

**Objective**: The objective of this activity is to experiment with President Jefferson’s chosen solution to address flaws in simple substitution ciphers. We introduce the concept of key-phrases and encryption keys. Students will quickly come to value having computer or internet applications which can rapidly perform the manipulations and look-ups required to decipher encrypted messages.

**Materials You Will Need**:
1. Pencil and paper, ideally graph paper for aligning the characters, but any paper will do.
2. [Optional] A print out of President Jefferson’s mapping matrix on the next page would be helpful.
3. [Optional] An excel spreadsheet could be prepared to crisply render Jefferson’s mapping matrix.

**Mission Briefing**:

During the famed expedition of 1803, President Jefferson wanted Meriwether Lewis to send regular dispatches from the field “putting into cipher whatever might do injury if betrayed.” He recognized the weakness of simple substitution ciphers and proposed different options to change the amount of shift for each letter of the message.
One version required the mapping matrix to the right along with a **keyword**. For instruction, he chose the word “antipodes” and wrote it above the **plaintext** message, repeating partially if needed.

He then used the mapping matrix to generate the ciphertext in combination with the key. He said, “look for the t (first letter of the plain text) in the first vertical column and the a (corresponding letter of the key) in the first horizontal column gives u.”

| key: | antipodesantipodesantipodes |
| plain: | themanwhosemindonvirtuebent |
| cipher: | uvyugb&mgtsfrcsssnjemcugitm |

This cipher is based upon the Vigenère Cipher which was widely used in Europe and considered unbreakable until the mid to late 1800s.

Thomas Jefferson was a legendary US president who sought to raise the level of education for all Americans. We highly recommend a visit to Monticello in person or online, taking special note of President Jefferson's cabinet (office) and the scientific equipment displayed there.

Given that wise minds are bent on both virtue and “aerospace” your mission is to decode the secret messages intercepted below. Remember to reverse the process described above. For example, find the letter of the keyword in the top row. Then draw your finger down the column until you find the corresponding cipher letter. Then draw your finger left across this row to the first column to find the letter of the original plaintext.

1. efnbkebfjdwslulytldswmnfxfwhw&fxkp
2. ojnvjjnpfokifxrjuibnrjqqgwkmnw
3. tjddxgwlljqsbytptuyfuggqaynsfnh
4. dtehtsujfklvpxvpuusnqtduwhqpsw

**Conclusion:** As you can see from your efforts, the same plaintext letter no longer corresponds to the same ciphertext letter, because of the **keyphrase**. When security systems are designed, engineers assume that details of the cryptographic algorithm are already known to the attacker.

This is known as Kerckhoffs' Principle summarized by "only secrecy of the key provides security." It has been demonstrated throughout history that the process of encryption is difficult to keep secret. A key is much easier to protect and may be quickly changed if it is believed to have been compromised.

**Questions for Further Consideration or Research:**
1. Is there any evidence that Lewis humored Jefferson with an encrypted report from the field?
2. Would the encryption be secure if a Wing AEO selected "aerospace" as a key? Why or why not?
3. What would be the best way to generate an encryption key?
4. Would you need a computer to generate an encryption key in this way? If so, why?
5. In 1883, Auguste Kerckhoff proposed six design principles for military ciphers. What are they?
6. Which “father of the computer” is first known to have broken a variant of the Vigenere Cipher?
Activity 1.3: The Kryptos Sculpture

**Objective:** The objective of this activity is to introduce students to the challenge presented by Jim Sanborn's *Kryptos sculpture* and to use it as a motivational tool for recruiting and learning. In the real world, solutions to puzzles will not be provided in the back of a textbook. The clock ticks waiting for the most ambitious to hone their skills to a level where they can provide solutions.

**Materials You Will Need:**
1. Computer with access to the internet
2. Printer and paper
3. Permission from school principal or squadron commander to post approved images.

**Mission Briefing:**

Look up Jim Sanborn's *Kryptos* sculpture, located on the campus of the CIA headquarters in Langley, VA. Print a large, detailed photo of it and post this image along with an easy to read transcript of the *ciphertext*. Posting it reminds us and others that although this sculpture was erected in 1990, it took over 8 years just to break one part. Still unsolved are the 97 characters of the fourth part, known as *K4*.

Using online tools, find the Latitude and Longitude of Kryptos. Lat: ____ Long: _____

Research and list online communities and groups working to complete the decryption process.

Research the cryptographer who instructed Mr. Sanborn in various methods of encryption.

Research which famous explorer and discovery is referenced in the decryption of *K3*.

**Conclusion:** Since the *Longitude Act of 1714*, whenever a society or government believes it has a worthy problem to solve, it will create a competition and offer a prize.

This is actually related history behind the *Ansari X-Prize* offered for a commercial, reusable space-vehicle. In the same way, Mr. Sanborn created a challenge for current and future analysts of the clandestine service and anyone else who might wish to make the effort.

**Questions for Further Consideration:**
1. How long did it take to break any one of the four sections?
2. Who was the first person to publicly announce solving the first three sections?
3. Name the analyst who likely first solved the three sections, but made no public announcement.
4. Are there any other sculptures of this nature? If so, where are they?
Activity 1.4: Other Codes, Ciphers and Encryption Methods

Objective: The objective of this activity is to have the student review the difference between a code and a cipher and to independently learn about other ciphers through some experimentation.

Materials You Will Need:
1. A computer with internet access to research various codes and ciphers.
2. Pencil and paper to write your definitions and work additional messages.

Mission Brief:

Define the terms below and derive the plaintext for the associated example codes or ciphers. We've done the first one for you.

<table>
<thead>
<tr>
<th>Code</th>
<th>When words or phrases have specific meanings, this is a code and not a cipher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>codetext</td>
<td>Climb Mount Nitaka.  (Hint: Maybe there's info already “out there” on this phrase?)</td>
</tr>
<tr>
<td>plaintext</td>
<td>____________________________________________________________________</td>
</tr>
<tr>
<td>Morse</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>codetext</td>
<td>.-- .... - - / .... - - .... / --. --- -. / --. -. --- .-. --. .... - ..-.--</td>
</tr>
<tr>
<td>plaintext</td>
<td>____________________________________________________________________</td>
</tr>
<tr>
<td>Baconian</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ciphertext</td>
<td>I eXTEnd My haNd In wElComE To You</td>
</tr>
<tr>
<td>plaintext</td>
<td>____________________________________________________________________</td>
</tr>
<tr>
<td>Railfence</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ciphertext</td>
<td>cainepeeeootcgogaigafrrzlwlwntrwdoiet</td>
</tr>
<tr>
<td>plaintext</td>
<td>____________________________________________________________________</td>
</tr>
<tr>
<td>Bifid</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ciphertext</td>
<td>EesphO Promgt 9/Bkmvna ve bvwnqa nt Vwchderb</td>
</tr>
<tr>
<td>plaintext</td>
<td>____________________________________________________________________</td>
</tr>
</tbody>
</table>

Conclusion: A code is when one entire word is substituted for another... or when phrases are used to deliver alternate meanings. A code-book might be vital to decoding these types of messages.

Questions for Further Consideration:
1. Name a truly American code used during World War II that used a non-English language.
2. What were some of the code phrases broadcast prior to the Invasion of Normandy?
3. What is the main advantage of Baconian Ciphertext? What is the cost paid for this advantage?
Activity 1.5: PGP Pretty Good Privacy and Gpg4win Software

Objective: The purpose of this optional advanced activity is to demonstrate how students may use modern encryption software to secure the privacy of their documents and email messages. We also introduce the concept of a hash algorithm and check-sum, for verifying the integrity of a download. We will learn more about Cryptographic Hash Functions in a later activity. Finally we learn about pass-phrases and the value of email signing.

Materials You Will Need:
1. A computer with access to the internet
2. A hard drive with sufficient space for a 40MB download.

Mission Brief:

PGP or Pretty Good Privacy is a computer program that provides authentication and cryptographic privacy for data communication. It was created by Phil Zimmermann in 1991. He also created ZRTP and Zfone which are encryption protocols for VoIP. Mr. Zimmerman has won numerous technical and humanitarian awards for his work.

GnuPG is a free software alternative to the PGP suite of cryptographic software. Gpg4win is a Windows installer package for email and file encryption using the core component GnuPG for Windows. It also includes both relevant cryptography standards, OpenPGP and S/MIME. Gpg4win is free software. Students should visit the Gpg4win Download Page to download and install this software, following all the directions provided there. The download might take awhile, and there is an online manual or compendium to review during the process. It includes detailed installation instructions.

You will have completed this activity when you have:
1. Downloaded, verified and completed the installation,
2. Read the sections of the Novice Manual,
3. Created a memorable and "unbreakable" pass-phrase for yourself,
4. Created a certificate using the included Kleopatra software,
5. Encrypted an email, (Never encrypt anything of a truly personal or sensitive nature.)
6. Signed an email, and
7. Demonstrated this process to others.

Conclusion: You have seen the complexity associated with implementing real encryption, of a quality that was recently considered "too strong to export."

Questions for Further Consideration:
1. PGP traffic is easily detected and provides proof of intent to conceal. How do you think these two facts are leveraged?
2. Which software security corporation recently acquired PGP in June of 2010?
3. Where was the RSA Public Key Cryptosystem developed? With what funding?
4. What reasons does Phil Zimmerman give for writing PGP?
5. What is a PGP Word List?
Activity 1.6: Encryption and Codebreaking to Promote Curiosity

Objective: At this point, students have already learned a great deal about the vital role of secure communications in military and business operations. The objective of this activity is to unleash student creativity to learn more about certain duties of the Technical Operations Officer. Students will review various awareness posters that have been created to remind people of the importance of OPSEC or Operational Security. Recent news events regarding cyberspace threats and targets should be reviewed. This current information should then be used in the construction of recruiting posters.

Materials You Will Need:
1. A computer with access to the internet.
2. Internet new service (Google News) to look for articles on “hacking” or “cybersecurity.”
3. A color printer with larger size paper (11 x 17) for the creation of posters.

Mission Brief:
Posters might be sufficient, but the future high-tech intelligence officers we seek expect to be challenged immediately. This personality type notices details and quietly asks questions.

Taking a lesson from President Jefferson and Jim Sanborn, we suggest you modify three standard Cybersecurity posters from Appendix C: Toolbox of Promotional Resources. You could also combine a fighter-jet graphic with a “cyberglobe image” and include an encrypted message of your choice along with the following prompt to design your own Recruiting Poster.

Opportunities, Prizes or Scholarships Available
If you can read the message above, send an email to coach@yourschoolorunit.edu

The email would belong to a teacher or CAP officer who you have “persuaded” to serve as your team coach. The posters should be numbered 1, 2 and 4 with poster number 4 having the most difficult cipher to crack. Allow your unit commander or school principal an opportunity to review and approve their secure posting. It will be amusing to see if anyone asks about the mysterious Poster Number 3.

Conclusion: There is a great deal of material to learn and very few individuals can process all of it independently. Working under the guidance that Together Everyone Achieves More, we seek to recruit individuals to form TEAMs and implement the principle of division of labor. In this way, each team member can become the local expert in one area of cybersecurity and brief the others.
Unit Profile: Room 40 and Bletchley Park

Room 40

Room 40 was the section in the British Admiralty associated with cryptoanalysis during World War I. It was formed in the fall of 1914 and housed in Whitehall's Admiralty Ripley building. The Director of Naval Intelligence, Admiral Oliver, would deliver German radio intercepts to Alfred Ewing, Director of Naval Education. Ewing recruited others, including German language translators, to assist him.

Room 40's most notable accomplishment was in decrypting the 1917 Zimmerman Telegram, a message with a plaintext to entice Mexico to join the war as a German ally. The section is credited with decrypting roughly 15,000 German wireless and telegraph communications. Several intercepts led to the Battles of Dogger Bank and the Battle of Jutland in the North Sea.

Various German losses in the field or at sea would lead to the capture of codebooks, which would be forwarded to the Admiralty. Russian capture of the German Cruiser Magdeberg resulted in Room 40 acquiring the SKM code book. They also acquired the HVB codebook and Diplomatic Code Book, Code No. 13040. This demonstrates real-world misfortunes leading to penetrations of "cyberspace" that result in, you guessed it, more real-world misfortunes.

In 1919, Room 40 was deactivated and merged with MI1b to form the Government Code and Cypher School, later to be housed at Bletchley Park during World War II.

Bletchley Park

Bletchley Park was the mansion home of the United Kingdom's main decryption unit, the Government Code and Cypher School (GC&CS) during World War II. Here the ciphers and codes of several Axis countries were decrypted, most notably those generated by the Enigma machines used in communication with German U-boats. The mansion also held a secret radio intercept station, StationX.

Cybersecurity was vital at Bletchley Park, as any hint that Enigma had been broken would result in a change. Churchill called Bletchley staff "The geese that laid the golden eggs and never cackled."

The movie U-571 gives a fictional but inaccurate flavor of the importance of code-breaking in the Battle of the Atlantic. It was the crew of HMS Bulldog that captured an Enigma Machine from U-110.

Biography: Alan Turing

Alan Turing was a mathematician and cryptanalyst who worked at Bletchley Park. He directed Hut 8, a section responsible for German naval cryptanalysis. There he devised innovative techniques for breaking German ciphers. One, called the bombe, was an electromechanical machine able to find settings for the German Enigma machine. In many ways, Turing's efforts led the Allies to victory in the Battle of the Atlantic.

After the war he created an early stored-program computer, the ACE. Many consider him the founding father of computer science and artificial intelligence.
Concepts in Information Assurance and Cyber Warfare

We define **Information Assurance** as the practice of managing risks related to the storage, processing and transmission of our information and data. This could include designs for modern aircraft and weapons systems. CAP members are familiar with **Operational Risk Management** (ORM) through CAP’s online safety programs, flight academies and required staff training. Numerous recent events have exposed significant penalties for not addressing obvious risks in cybersecurity.

Models of **Information Assurance** organize or group the risks so that we can be certain our checklists of action items will address all potential vulnerabilities and threats.

**The CIA-Triad and Five Pillars of Information Assurance**

The CIA Triad defines the attributes of information critical to its effective use. **Confidentiality** is the idea that certain information (troop movements, aircraft design, code keys) will be much more useful and valuable if they are kept secret from others. **Integrity** addresses the quality of the information, to include its completeness, its accuracy, and its relevance. If our information is adulterated with false rumors or red herrings, then it is less useful. **Availability** reveals a weakness for others to benefit if they can keep authorized users from accessing key information, even if they themselves cannot penetrate its confidentiality.

The DoD adds two other attributes to the CIA Triad to include **authentication** and **non-repudiation** to form the **Five Pillars of Information Assurance**. These terms are defined in the glossary.

If we take measures to ensure the confidentiality, integrity and availability of our military aircraft design data, then we would be able to effectively deploy new aircraft and weapons systems.

**Cyber Warfare**

Several western books define **cyberwarfare** as actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. However, the Shanghai Cooperation Organisation extends the definition of cyberwar to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states". This difference of opinion likely prevents western governments from signing certain global cyber arms control agreements.

Cyber Warfare consists of many different possible threats and countermeasures. **Cyber Espionage** and **Cyber Sabotage** are two fundamental classifications of attack, into which other threats may fall.

One detailed threat classification is called **STRIDE**, which is an acronym of the six threat categories to include: 1. **Spoofing of user identity** 2. **Tampering** 3. **Repudiation** 4. **Information disclosure** 5. **Denial of Service (DoS)** and 6. **Elevation of privilege**. Our glossary details these.

**Countermeasures** are procedures and devices which counter a vulnerability, threat or attack by preventing it, minimizing the resulting damage, or by detection so that corrective action can be taken. Current examples of cyberwarfare countermeasures include: **two-stage authentication**, firewalls and storage of vital materials on drives not connected to the internet.

In the case of cyber attacks against the electrical grid, one possible countermeasure might be to disconnect the power grid from the internet and run the grid with **droop speed control** only.
Activity Group Two: Vulnerabilities and Basic Defense Skills

A vulnerability is a weakness by which an attacker gains access to a private system. In this activity group we present some vulnerabilities and corresponding countermeasures.

Activity 2.1: Password Strength

Objective: "If it cannot be measured, it cannot be predicted and it cannot be controlled." This is the mantra of both business management and modern control theory. The objective of this activity is to expose the student to a quantitative evaluation of various passwords.

Materials You Will Need:
1. A computer with access to the internet.

Mission Brief:

Weak passwords are one of the biggest vulnerabilities to protecting our systems through user authentication. Passwords such as birthdays, airplane names, or favorite sport do not pass muster in today's threat environment.

Agent-Zero visited a local high school computer lab and installed the KeyGhost hardware-based keylogger. Shame on her. She found students using the passwords in the table below.

Your assignment is to rate these passwords as poor, good or excellent. Then get a numerical rating of the strength for each password from http://askthegeek.us/pwd_meter/index.htm and compare with your assessment.

<table>
<thead>
<tr>
<th>Password</th>
<th>Your Rating</th>
<th>NumRating</th>
<th>Password</th>
<th>Your Rating</th>
<th>NumRating</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat5</td>
<td></td>
<td></td>
<td>&amp;cat65Whz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>abc123</td>
<td></td>
<td></td>
<td>BlueKnight7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7041992</td>
<td></td>
<td></td>
<td>ih8mt3r</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mary$321</td>
<td></td>
<td></td>
<td>$6gK3m5o#</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

One way to generate a password is to think of a phrase that you will always remember. An example might be the phrase: "Good pilots are always trimming." Generate a shorter string by taking every nth letter from this phrase, ignoring the spaces. We choose n=3 to take every third letter to arrive at "oitrlyrmg." We then substitute numbers or symbols for various letters to arrive at "0i2lyr3g."

Conclusion: You can see from scores generated that the minimum requirements for a password are that it be at least 8 characters in length and contain 3/4 of the following items: uppercase, lowercase, numbers and symbols. Additional credit is given for usage of "middle numbers or symbols." In the next activity, we will see a further step that can be taken to protect access to a system.

Questions for Further Consideration:
1. Explain the trade-off between having a password that is easy to remember and having one that is difficult to crack.
2. Brainstorm some additional strategies to generate a complex password that you can remember, but that also scores well on the meter.
Activity 2.2: Two-Stage Authentication or Two-Step Verification

Anyone who has seen the original or remake of “Get Smart,” will quickly grasp the idea of multi-stage checks and authentication. Passwords can be compromised, so other devices are employed.

Biometric options include retinal scanners, fingerprint scanners, and facial scanners to authenticate.

RSA Security developed a device called SecurID consisting of a token which is assigned to a computer user and generates an authentication code at fixed intervals (usually 30 or 60 seconds) using a built-in clock and the card's factory-encoded random key, known as the seed. A user authenticating to a network resource would enter both their personal ID and the number being displayed at that moment on their token.

If this sounds too expensive for students and mentors, Google has implemented a version of Two-Step Verification using Gmail and the user's cellphone.

Objective: The objective of this activity is to allow the student to experience how professionals in DoD installations and sub-contractors might be two-stage authenticate to gain access to critical or top-secret information. The technology emulates the RSA SecureID device with the modern smart phone that some may already carry.

Materials You Will Need:
1. A computer with access to the internet.
2. A GMail account
3. A smart phone that can run the Google Authentication App

Mission Brief:
1. Sign-in to your gmail account and choose My Account.
2. In the Personal Settings – Security Group, choose Using 2-step verification
3. Follow the directions so that you will be sent a code by whatever device you have available. An Android phone version of this implementation is shown to the right.

Conclusion: The installation process for this tool is not too difficult to work through. If you configure an icon on your hand-held in an immediately accessible place, there will be minimal time spent finding and loading the random code. The ideal time to be running this application is during any competitive activities in which you are communicating designs and plans with team-mates over electronic channels. You wouldn't want your account hacked during this competition period.

Questions for Further Consideration or Research:
1. What are the advantages of Gmail?
2. What are the disadvantages of having all your emails electronically persistent online?
3. Do you believe the second step is worth the effort? Why or why not?
Activity 2.3: Internet Security Software

Objective: There is a great deal of software available to address tracking, virus and trojan-horse threats to our computers. Some of it is more effective than others. The purpose of this activity is to train our students to seek reviews and evaluations from reputable sources on these software packages. PCMag and CNET are common sources for Anti-virus and Anti-malware reviews.

Materials You Will Need:
1. Computer with free hard drive space and access to the internet.

Mission Brief:
For each of the products below, read independent reviews and scan the manual to determine how they work and the ways in which they are limited. If available, experiment with 30 day trial versions.

- McAfee Viruscan
- Norton 360 Version X.0
- Norton Antivirus 201X
- Spybot Search & Destroy
- AVG Anti-Virus Free X.0
- Windows Defender
- PCTools SpyWare Doctor
- HijackThis
- Anti-malware
- MRT
- BelArc Advisor
- CCleaner
- Anti-malware
- TrueCrypt

Here's an example review of CCleaner:

CNET rated it 5/5 calling it a "a must-have tool" and awarding a 2009 Editors Choice Award. In detail: “CCleaner supports the cleaning of […] unwanted files left by certain programs, including Internet Explorer, Safari, Google Chrome, Windows Media Player, eMule, Netscape, Microsoft Office, Nero, Adobe Acrobat, WinRAR, WinAce, WinZip, […] along with browsing history, cookies, Recycle bin, memory dumps, etc.”

Conclusion:
There are many options for internet security software tools, from Anti-virus to Anti-spyware and Anti-malware. Which-ever vendors and options we select, we need to remember to keep them updated.

One of the more interesting things to discover during this activity is the marketing battle between McAfee and Kapersky. This can be seen in the dialogue over McAfee's exposure of Operation Shady RAT and the magnitude of its impact.
Activity 2.4: Vulnerability Assessment

Objective: There is no reason to re-invent the wheel each time we conduct an audit of a facility, squadron or computer lab. Checklist tools abound to help guide us through the investigative process. The purpose of this activity to introduce this concept.

Materials You Will Need:
1. Paper print-out of the brief Cybersecurity Audit Checklist below.
2. Computer with internet to search for more detailed audit checklists.
   a. Search: "Computer Vulnerability Assessment Tool" or
   b. "Computer Security Audit Checklist"
3. Clipboard
4. Pencil

Mission Brief:

A mysterious, but benevolent, DOD contractor has offered to donate engines, servos, software and composite material to your school for a new Autonomous Aerial Vehicles Project, provided that you can demonstrate your computer labs are secure. If you cover the basics, their Cybersecurity consultants will visit to train you further in protecting your new designs. Your first step? Find any obvious vulnerabilities using the very basic audit checklist below.

<table>
<thead>
<tr>
<th>VulClass</th>
<th>Vulnerability Description</th>
<th>List any finding at home or school lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Lab walls are susceptible to penetration</td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td>Unguarded/unmonitored access to lab</td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td>Unlocked doors or windows</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>OS/SW lacks current updates/patches</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>High risk domains not filtered/blocked.</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>No user authentication required.</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Poorly written software installed: scripting, buffer overflows, crashes</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Deliberate holes: vendor backdoors, spyware/keyloggers, trojan horses</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Unencrypted network protocols</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Wireless network reaches the parking lot and/or evidence of war-chalking</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Connections to multiple networks</td>
<td></td>
</tr>
<tr>
<td>Comms</td>
<td>Unnecessary protocols allowed</td>
<td></td>
</tr>
<tr>
<td>Comms</td>
<td>No filtering between network segments</td>
<td></td>
</tr>
<tr>
<td>Human</td>
<td>Poorly defined procedures: No Incident Response Plan, violations not logged.</td>
<td></td>
</tr>
<tr>
<td>Human</td>
<td>Stolen credentials</td>
<td></td>
</tr>
</tbody>
</table>
Record whatever you find and see if a teacher, commander or principal would let you work with a system administrator to improve your computer lab as a model of good Cybersecurity techniques.

Next, consider expanding this checklist by looking at examples from other sources. Using your preferred search engine, search for "Computer Vulnerability Assessment Tool" or "Computer Security Audit Checklist" and see what you find. Many of these checklists are very long and will involve networking issues that are beyond our scope. Still, you may find something you can use.

**Conclusion:** The first time we conduct any audit, such as a computer system vulnerability assessment, we may be spending most of our time learning about what it is we are looking to find. This is acceptable provided that we intend to do it again. Once we have developed the knowledge and skills to complete the audit, the work moves much faster and we may even be able to receive compensation for our "findings."

**Questions for Further Consideration:**
1. Did you find anything obviously wrong that wasn't on the list? If so, add it to your audit checklist.
2. After you have done several of these, do you find common trends in vulnerabilities for school computer labs?

**Activity 2.5: Captain Cyber Patriot USB Flash Drive**

**Objective:** The objective of this activity to prepare our students to be "ready-on-the-spot" with diagnostic and corrective tools to help those who have been victimized by cyber-attacks. The perception that a student can actually do something about a problem actually raises their awareness and interest level.

**Materials You Will Need:**
1. One or more USB flash drives, many of which are now available as free giveaways or cheaply at the checkout counter.
2. Computer with internet access to download the recommended tools.

**Mission Brief:**

Many CAP Mission Pilots and Instructors travel extensively and maintain encrypted thumb drive volumes of Portable Applications, to include OpenOffice Portable and other tools.

You might have your own requirements for what software you need to keep on a handy key-chain flash drive, but please consider your patriotic duty to American Cybersecurity and Education when you outfit a USB flash drive with diagnostic and repair tools to assist others around you.

Here's our current recommendations for files and applications to maintain on this Thumb Drive.

**Documents**

[ ] This CAP Cybersecurity Module

[ ] **Cyber Patriot Instructional Power Points or PDF files**

[ ] Recruiting Posters and Graphics used for Promoting Awareness. See Appendix C for sources.
Conclusion: Once you have created the tool and placed it on a key chain, you will quickly find opportunities to put it to work. This is your opportunity to show others how to keep a clean computer and how to protect from malware, phishing, cross-site scripting and other attack vectors.
Unit Profile:  USCYBERCOM

In response to various attacks, Secretary of Defense Robert M. Gates directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish USCYBERCOM on 23 June 2009.

Initial operational capability was attained on May 21, 2010. General Keith B. Alexander was promoted to General and took charge of U.S. Cyber Command in a ceremony at Fort Meade.

USCYBERCOM reached full operational capability on October 31, 2010.

Mission Statement:  "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

The MD5 Hash of their Mission Statement is located in the inner gold band around the Eagle and Globe of its emblem. It reads "9ec4c12949a4f31474f299058ce2b22a."

Bonus Activity: MD5 Checksum

A cryptographic hash function processes a block of data and returns a fixed-size bit string, called the (cryptographic) hash value. Even a small change to the data would result in a radical change to the computed hash value. This is called the avalanche effect. The original data block is called the "message," and the computed cryptographic hash is the “message digest” or simply “the digest.”

In this activity we will test and generate some MD5 hashes. Please follow these steps:

2. Using Notepad, copy the text from the Mission Statement above, without the quotes, into a .txt file.
3. Using CTRL+C, copy the hash string "9ec4c12949a4f31474f299058ce2b22a" without the quotes.
4. Run the MD5.exe program.
5. Paste the copied hash string into the top slot and browse for the Mission Statement text file.
6. Verify that the hash matches that for the text of the file.
7. Change one letter of the Mission Statement text and process again to see avalanche effect.
8. Write your own Mission Statement for your Cybersecurity Team and then hash it.

Patriot Bio:  GEN Keith B. Alexander

General Keith B. Alexander, USA, serves as the current Director, National Security Agency (DIRNSA) and Commander, USCYBERCOM. Listen to a podcast interview with General Alexander.

General Alexander was born in 1952 in Syracuse, NY. He attended West Point and graduated in 1974 with a Bachelor of Science degree. Additionally, Gen. Alexander holds dual Master of Science degrees in systems technology (electronic warfare) and physics from the Naval Postgraduate School. He also holds a Master of Science degree in national security from the National Defense University.
A number of projects have published MD5 rainbow tables online, that can be used to reverse many MD5 hashes into strings that collide with the original input, usually for the purposes of password cracking. A US-CERT vulnerability notification pronounced MD5 compromised, saying it "should be considered cryptographically broken and unsuitable for further use." Most U.S. government applications now require the SHA-2 family of hash functions, which were designed by the NSA.

**DOS**

DOS, an acronym for "Disk Operating System", refers to commercial operating systems that dominated the personal computer market in the 1980s and early 90s. PC-DOS and MS-DOS used a command-line interface in which executable programs were started by entering their filename at a command prompt. Internal or administrative commands, such as file compare or copy could be run with optional switches placed inline.

DOS also provided a limited form of **shell scripting**, through .BAT or “batch” files. These are text files that would store multiple commands to be run in an automated sequence.

**Windows and Mac OS**

Microsoft Windows and Mac OS gained popularity through their Graphical User Interfaces which greatly reduced the learning curve for certain software applications, like word processors and administrative tools. Instead of requiring users to place program options in a cryptic command-line, check-boxes and radio buttons could be presented to remind users of available choices.

To **harden** a system, administrators will often prevent the installation of unapproved software to a computer's hard drive. They may also close access to USB ports. Hackers and crackers must therefore resort to lesser know command-line operations in order to achieve their goals. They do this by getting access to a Command Shell through one or more creative ways. We'll explore this in a later activity.

**UNIX Operating System**

UNIX is a multitasking computer operating system originally developed in 1969 by a group of AT&T employees at Bell Labs, to include Ken Thompson and Dennis Ritchie. Unix and the C programming language were distributed to government and academic institutions.

This led to them being ported to a wider variety of machine families than any other operating system. As a result, Unix became synonymous with "open systems" and the OS grew as individuals wrote additional command-line tools and programs. In the early 1990s, MIT's X-Windows emerged to establish a GUI for the UNIX OS. Others soon followed.

One open version of a UNIX-like operating system is **Linux**, a kernel originally written in 1991 by Linus Torvalds. System tools and libraries from the GNU Project are the basis for the Free Software Foundation’s preferred name GNU/Linux. Linux “distributions” include Linux and large collections of compatible software. One of these, called **Fedora**, was chosen for Cyberpatriot III. Other popular distributions include openSUSE, Debian GNU/Linux, Ubuntu and RedHat.

**Virtualization and VMWare**

Users currently running a preferred or authorized operating system, can experiment with another through either dual-boot or **virtualization** products from VMware. VMware is a company headquartered in Palo Alto, CA providing desktop software that runs on Microsoft Windows, Linux, and Mac OS X. Users of Microsoft Windows 7 or Mac OS can download and install VMware along with the **Fedora image** so that they may experiment with the Linux operating system and work certain activities of the Cyber Patriot modules. This will be detailed later in **Activity Group Four**.
Activity Group Three: Basic Probing Skills

Activity 3.1: Command Shell Fun

Objective: Shell commands are tools, just like a screwdriver or the Cyber Patriot USB Flash Drive. The difference is that "these software tools" are built-in to most operating systems, whether Windows or Unix. The objective of this activity is to become more familiar with another path of access to various Windows functions and tools available through the old-style command-line interface. These commands are particularly helpful if something prevents you from loading and using the GUI or Graphical User Interface of your Operating System. These commands may be assembled into simple scripts known as .BAT or Batch Files so that large numbers of files can be conditionally moved, copied or erased or their attributes modified.

Materials You Will Need:
1. Computer running a version of Microsoft Windows
2. Curiosity to go online and explore .bat file programming. Be cautious!

Mission Brief:
To prevent the “accidental” installation of gaming and other software on public computers, “admins” or administrators often remove the icon allowing access to the web browser. At airport FBOs, computer keyboards may even be removed. A workaround to these situations is to bring up a Command Shell.

1. From your desktop, click the Windows Start Button to the lower left.
2. In the Search programs and files text box, type cmd and press enter.
A black command shell will appear. Typing `help` at the prompt gives you a list of available commands.

Unfortunately, only a few of these commands are of real interest to attackers and defenders. The `COMP` command allows you to compare content of two files or sets of files for unauthorized changes. Here’s a quick list of interesting shell commands that you could explore immediately. Bring up the black cmdshell and type each of the commands listed below at the prompt.

Example: `C:\Users\Patriot> osk` or, to get help `C:\Users\Patriot> shutdown /?`

Complete the table below with your findings.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>osk</td>
<td>On Screen Keyboard</td>
<td>If computer is configured as a mouse driven kiosk, osk will get you an electronic keyboard.</td>
</tr>
<tr>
<td>explorer</td>
<td>Windows Explorer</td>
<td></td>
</tr>
<tr>
<td>mrt</td>
<td></td>
<td>Periodically run as a good practice.</td>
</tr>
<tr>
<td>chkdsk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>taskmgr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>perfmon</td>
<td>Windows Performance Monitor</td>
<td></td>
</tr>
<tr>
<td>resmon</td>
<td>Resource Monitor</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ping</td>
<td>Test “reachability” or determine IP.</td>
<td></td>
</tr>
<tr>
<td>tracert</td>
<td>Determine domain name, routing</td>
<td></td>
</tr>
</tbody>
</table>

Next, consider searching for and reading about .BAT files or Batch Applications online. Be careful of running any of these that have programmed loops, however, as you may have difficulty shutting them down. This will give you a flavor of the common term "script kiddies."

**Conclusion:** This activity has demonstrated a tool to workaround a computer that cannot boot to its Graphical User Interface or has had features disabled by administrators or malware. More advanced cmdlets are available through Windows PowerShell, which we will address shortly.
Activity 3.2: ping and tracert commands

Objective: Hackers and penetration testers need to be successful, in order to deliver their point regarding the urgency of the problem. Often, this means ignoring the most secure targets and looking for the weak links in the supply chain. If a DoD website or system is too secure, perhaps a DoD contractor is a more accessible target. The objective of this activity and the one to follow is to demonstrate the methods by which hackers conduct initial probes of potential targets.

Materials You Will Need:
1. A computer running Microsoft Windows or a Unix/Linux variant
2. Access to the internet

Mission Brief:
Using the ping command, attackers could conduct a ping sweep against a range of IP addresses and functional systems may respond with an echo reply. An analogy has been drawn to the submariner's SONAR ping. This preliminary method could provide a list of potential targets.

A ping may also be used to determine the IP Address of a Host Website. So, at this time we ask you to ping capmembers.com from a cmdshell. We include an echo print below so that you may check your work. However, your results may vary.

C:\Users\Patriot>ping capmembers.com
Pinging capmembers.com [205.237.127.87] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 205.237.127.87:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

From the last command run, we receive the IP Address of 205.237.127.87!

Now run the ping command with the -a option to resolve a host name. Remember, you can receive help on any of these commands by placing /? after the command.
For example, `C:\Users\Patriot\ping /?` will show all the switches for the ping command.

[-r count] [-s count] [-j host-list] [-k host-list] 

Options:
- `-t` Ping the specified host until stopped.
  To see statistics and continue - type Control-Break;
  To stop - type Control-C.
- `-a` Resolve addresses to hostnames.
- `-n count` Number of echo requests to send.
- `-l size` Send buffer size.
- `-f` Set Don't Fragment flag in packet (IPv4-only).
- `-i TTL` Time To Live.
- `-v TOS` Type Of Service (IPv4-only. This setting has been deprecated 
  and has no effect on the type of service field in the IP Hea
- `-r count` Record route for count hops (IPv4-only).
- `-s count` Timestamp for count hops (IPv4-only).
- `-j host-list` Loose source route along host-list (IPv4-only).
- `-k host-list` Strict source route along host-list (IPv4-only).
- `-w timeout` Timeout in milliseconds to wait for each reply.
- `-R` Use routing header to test reverse route also (IPv6-only).
- `-S srcaddr` Source address to use.
- `-4` Force using IPv4.
- `-6` Force using IPv6.

`C:\Users\Patriot> ping -a 205.237.127.87`

Pinging 205-237-127-87.global-reach.com [205.237.127.87] with 32 bytes of 
data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 205.237.127.87:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Which would obviously lead some to research global-reach.com

Next, we will demonstrate the tracert command.

`C:\Users\Patriot> tracert capmembers.com OR`

`C:\Users\Patriot> tracert 205.237.127.87`

```
   1    1 ms  <1 ms  1 ms  lxx.lxx.x
   2    *    *    *     Request timed out.
   3    *    *    *     Request timed out.
   4    *    *    *     Request timed out.
   5    *    *    *     Request timed out.
   6    *    *    *     Request timed out.
   7    *    *    *     Request timed out.
   8    7 ms  8 ms  11 ms  vlan52.ebr2.Atlanta2.Level3.net [4.69.150.126]
   9    9 ms  6 ms  7 ms  ae-73-73.ebr3.Atlanta2.Level3.net [4.69.148.253]
```
This output confirms what we find in our research on the tracert or traceroute command. Many networks block, or de-prioritize the ICMP (Internet Control Message Protocol) time exceeded message that is required to determine round trip time.

A very good simulation for learning Traceroute Basics is available here and we recommend this over probes of domains not in your control.

Conclusion: This activity has introduced the topic of host discovery or ping scanning also known as ping sweep. Command tools like ping and tracert can be used by penetration testers to gather information about network infrastructure and IP ranges around a given host. On corporate intranets, these will likely generate much more information that what we see here.

Questions for Further Consideration or Research:
1. Research the Welchia worm.
2. As a result of Welchia, how was the diagnostic usefulness of the ping command impaired?
3. Research the nmap tool created by Gordon Lyon.
4. What additional information can nmap determine, beyond simply whether a host is up or down?
Activity 3.3: Conduct a Whois Probe of capmembers.com

Objective: Once a pingsweep or traceroute has identified the presence and domain of a working computer at an IP Address, the WhoIs probe may be used to learn more about who has registered that domain. This activity introduces one, not-so-automated method for obtaining this information.

Materials You Will Need:
1. A computer with internet access
2. A careful and respectful curiosity

Mission Brief:
A cracker might conduct a Whois Probe of a particular domain name, once it has been identified as either a threat to an agenda or if it was suspected of housing valuable data. A decision is then made to compile intelligence on the site in preparation for an attack.

Your assignment is to emulate this approach as follows:
1. Go to the URL listed in blue to the right: http://www.internic.net/whois.html
2. Enter any website URL on which you are curious, and choose Domain and hit Submit.

You will receive a return that looks something like this...

Whois Server Version 2.0

Domain Name: CAPMEMBERS.COM
Registrar: GODADDY.COM, INC.

Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
Name Server: NS1.CYPRUSWEB.COM
Name Server: NS2.CYPRUSWEB.COM

Status: clientDeleteProhibited
Status: clientRenewProhibited
Status: clientTransferProhibited
Next, the curious cybersecurity expert will turn to research godaddy.com and cyprusweb.com on the internet for any reported weaknesses, just as soon as they get past all the GODADDY advertisement videos on YouTube.

**Conclusion:** This activity demonstrated a method for determining which corporation, government or organization might be responsible for a newly discovered remote host at a given internet address. This information, in combination with knowledge of the tree structure of subcontractors working for larger organizations is often the basis for finding weak links in an information supply chain. Students will want to explore, by means of news articles, which entities support and supply others.

Although we demonstrated a WhoIs lookup using a simple internet service, the student will imagine the power of an automated report generated by a script that delivers the output of a ping sweep to a command line whois function.

**Questions for Further Consideration or Research:**
1. What are some ways you could openly determine which businesses supply goods and services to a US Defense Contractor?
2. What is NAICS? What is the NAICS code for Engineering Services? For Drafting Services?
3. How would you determine suppliers and sub-contractors for Lockheed Martin or Boeing?

**Activity 3.4: Viewing Page Source for Vulnerabilities**

**Objective:** Websites deliver marketing and technical support information to the clients and customers of the companies who construct them. In order to maintain the economic value of the information provided, these websites are often secured with user names and passwords. The objective of this activity is to demonstrate one common way that websites are probed for weaknesses and that their user databases may be penetrated or revealed.

**Materials You will Need:**
1. Computer with internet access.
2. A website that asks for a userid and password or other input from the user.
3. Additional curiosity to research “Page Source Hack”

**Mission Brief:**
Most of us already know that when viewing a given website, it is possible to “View source.” This means we can take a peak at the XHTML code that was generated to render the page. Many times, security professionals and crackers use this to gain insight into potential weaknesses for exploit.

Your assignment is to review how to look at the page source:
1. Right click on any part of the page that is not a video, image, link or menu option.
2. A pop-up menu of options will appear and **View source** will be an option approximately in the middle of this list.
3. Next, choose the View source option, to see a page displaying the color-coded XHTML code. These might be used to accept user input for a password, feedback, or some search criteria. Use CTRL-F to pop up a Find window and you can enter “form action” to see if anything is revealed. The image above shows one form action tag.

We are typically looking for FORM tags in the HTML code. These might be used to accept user input for a password, feedback, or some search criteria. Use CTRL-F to pop up a Find window and you can enter “form action” to see if anything is revealed. The image above shows one form action tag.

This is a typical approach to prepare for a SQL Injection Attack, or SQLIA. SQL is the relational database Structured Query Language that pulls certain fields (name, address, city, state) out of a database for certain filtered records, such as registered users of a website living in Alabama.

A hacker could bypass authentication by entering text such as ' or '1'='1, which would always check true. This could happen if the site programmer did not filter user input for this type of attack.

Conclusion: This activity described a method to probe a webpage seeking user input. Early websites that were run on free, open-source content management software were often penetrated or defaced following this initial approach. This activity should ready the user for the next, which details SQL Injection and Cross-site Scripting.

Questions for Further Consideration:
1. Which NASA departments had websites fall victim to SQL Injection Attacks?
2. What were the specifics of these penetrations?
Activity 3.5: Script Injection, Cross-site Scripting and SQL Injection Training

Objective: We understand that many students are learning from online video resources because they more cost effectively and quickly deliver the required information. They don't bog you down with overhead and you can see what you need to do in the motion of the video rather than read a long textual explanation. The objective of this activity is to encourage you to continue learning as much as you can about attack vectors and countermeasures by whatever medium most appeals to you.

Materials You Will Need:
1. Computer with internet access.
2. YouTube

Mission Brief:
Another type of code injection attack is known as cross-site scripting or XSS. This has become one of the most common methods of attack, in which private user data from a cookie is stolen. Please watch the following training videos, from Imperva, to learn more about these methods of attack.

1. Script Injection Demonstration
2. Cross-site Scripting Demonstration
3. Database Threats 101: SQL Injection Attacks
4. Passwords and Credit Card Numbers Hacked

Conclusion: Hopefully, you were able to visually and quickly learn exactly how weaknesses are exploited or countered without the loss of attention and immediate meaning from which prose can suffer. More importantly, you are seeing the related search terms needed to get more information at this faster pace. Keep going!

Questions for Future Consideration or Research:
1. What related videos on other attack vectors or cybersecurity techniques has YouTube revealed?
2. Can you create a Gmail alert to automatically advise you of any news on these techniques?

Activity 3.6: Windows PowerShell

Objective: The GUI or Graphical User Interface is perfectly fine for day to day operations with email, presentation software and spreadsheets. However, if you are looking to defend against attacks you will need to learn much more about the Operating System on which you are running. The objective of this activity is to introduce the student to a relatively new scripting tool that allows low level interaction with the various objects and methods of the Windows Operating System.

Materials You Will Need:
1. Computer with a Windows Operating System
2. Confirm installation of Windows PowerShell or Download it.
Mission Brief:

**DEF CON** (also written as **DEFCON** or **Defcon**) is one of the world’s largest annual hacker conventions, held in Las Vegas, NV. The first DEF CON took place in June 1993. At DEFCON18 in 2010, a presentation on **Windows PowerShell** demonstrated the power of the tool as a new attack vector, to deliver any “payload” a hacker chooses in both a bind and reverse type scenario and drop any executable.

Do not experiment too “aggressively” on any computer that you might need to use for work or school or home management. You could crash your machine. If you don’t already have it, download **Windows PowerShell** and acquire a reputable training book. We’ll provide a short introduction.

### 3.6.1. Start Windows PowerShell

Left click on the Windows Start logo at the bottom left of your computer screen and type “powershell” into the search box. A PS shell environment will “pop-up” and you can begin to experiment.

![Windows PowerShell](image)

### 3.6.2. Learn the Command Format

The standard command format in Windows PowerShell is verb-noun, with **parameters** specified following a `-`. Some simple, safe, commands you can type to get a feel for this scripting environment follow. Check off each command below as you either type it or use Get-Help to explore its format.

```
```
3.6.3 Learn A Few Aliases

No, we aren't talking about George Sand, Andy McNab or Mark Twain. Within PowerShell, an alias is another name assigned to a cmdlet, function, script, or executable file. Just about anything you can run from the PowerShell command prompt can have an alias assigned to it. We'll explain how this works, and why you'd even care about it, by first showing you some of the aliases built-in to PowerShell.

The alias for Get-Alias is, you guessed it... gal. Type that now and see what is returned.

```plaintext
PS C:\Users\Patriot> gal
```

Looking through the list, we find that gps is the standard alias for Get-Process and sort is an alias for Sort-Object, and more is an alias to call Out-Host -paging, so that one page of data will be released to the screen at a time, with a key press allowing "more" to be seen until the entire output is delivered.

The full command format of verb-noun reminds administrators and programmers of the structure of the system. Shortened aliases are used to speed typing and reduce workload, where appropriate.

3.6.4 Learn About Pipelines and Passing Data from Command to Command

Unix command shells, like Bourne Shell and C Shell, have previously allowed for command pipelines. This concept of a pipeline allowed for the output of one command to be piped as input to another command. Why would administrators, programmers or hackers wish to do that?

One part of the answer lies in being able to page-through, filter or sort the data immediately as it is returned from execution of the command. You aren't interested in ALL of the files, processes or users that a command execution returns. You just want the ones dealing with a certain object... or maybe just the ones that have been most recently active. You could string together a series of commands with applied filters and sorts into a script. You could then program this script to run at fixed intervals using the chron command to alert yourself to violations or intrusions.

We'll start slow. Lets just pipe the output of a few Windows PowerShell commands, that return long lists, to the Out-Host cmdlet. Please type each of the following commands and observe the results.

```plaintext
[ ] PS C:\Users\Patriot> Get-Process | Out-Host -paging
```

Of course, all of this can be manipulated interactively using the Out-Gridview cmdlet. Lets try it!

```plaintext
[ ] PS C:\Users\Patriot> Get-Process | Out-Gridview
```

Conclusion: We're hoping that you executed these commands and then decided to search for more on your own. There are many scripts available for Windows PowerShell that do some amazing things with the processes currently running in the background while you are reading this summary.

Questions for Future Consideration or Research:

1. Can you find any Windows PowerShell tutorials on YouTube?
Unit Profile: 24th Air Force

The Twenty-Fourth Air Force (24th AF) is the US Air Force component of US Cyber Command (USCYBERCOM). Over 14,000 airmen work for 24th AF, with many cyberspace specialists distributed throughout other units and organizations. Units under this Numbered Air Force include:

67th Network Warfare Wing (67 NWW) - Lackland AFB, Texas
688th Information Operations Wing (688 IOW) - Lackland AFB, Texas
689th Combat Communications Wing (689 CCW) - Robins AFB, Georgia
624th Operations Center (624 OC) - Lackland AFB, Texas

The current mission of the United States Air Force is

“To fly, fight and win… in air, space and cyberspace.”


Unit Profile: 67th Network Warfare Wing

The 67NWW is charged with executing Air Force Space Command’s global mission of information operations. As USAF’s largest operational wing, it has people or equipment on every continent save for Antarctica.

The wing is composed of five intelligence groups, 35 squadrons and detachments and more than 8,000 people serving in 100 locations around the world to provide information to help shape global events.

Mission Statement: “To conduct Information Operations. The wing directs planning of multi-source electronic combat services, information warfare and communications security. It assists the Air Force components in the development of airpower concepts, conducting exercises and employment of AFISRA forces in contingencies, low-intensity conflict, counterdrug activities and special operations.”

Patriot Bio: Col Kevin B. Wooton

Col. Kevin B. Wooton commands the 67th Network Warfare Wing.

As part of Operation Enduring Freedom, Col Wooton deployed to Kandahar Afghanistan, as Director of Intelligence, Task Force-South.

Sample of Qualifications:
1985 B.S. Geophysics, University of Utah, Salt Lake City, Utah.
1993 Squadron Officer School, Maxwell AFB, Alabama.
1995 M.S. Administration, Central Michigan University.
1998 Air Command & Staff College, Dist Grad, Maxwell AFB.
2005 National Security Affairs Fellow, Hoover Institution.
2010 National Security Management Course, Syracuse University.
Exploring Careers in Cybersecurity

On 4 December 2009, the Department of Homeland Security uploaded a YouTube video message from Philip Reitinger, Director of the National Cybersecurity Center. He announced the Department's authority to expedite hiring of up to 1,000 cybersecurity experts over the next 3 years.

“The Department seeks your expertise in Cyber Incident Response, Cyber Risk and Strategic Analysis, Vulnerability Detection and Assessment, Intelligence and Investigation, and in Networks and Systems Engineering.”

Getting the Education

The University of Texas San Antonio created the Institute for Cyber Security in 2007. UTSA currently offers Bachelor's and Master's degrees in Infrastructure Assurance. In response to the 2009 DHS announcement above, the University of Maryland created the Maryland Cybersecurity Center and three degree programs at the University of Maryland University College to provide practical and theoretical training. The bachelor’s degree in cybersecurity requires 120 credits, including 33 credits of coursework in the major, and students can take many of the courses online.

Two master's degrees are available in a cybersecurity technical track and in cybersecurity policy, each of which would require six online courses. Students must also complete internship programs.

These are career targeted programs that differ from Computer Science or Engineering majors.

UMD's Cybersecurity Club participates in cybersecurity competitions and hosts technical speakers.

A sample of some required courses to earn a Bachelor's Degree in Cybersecurity might include:

- EDCP 100: Principles and Strategies of Successful Learning
- LIBS 150: Information Literacy and Research Methods
- MATH 106: Finite Mathematics
- IFSM 201: Introduction to Computer-Based Systems
- CMIS 102: Introduction to Problem Solving and Algorithm Design
- PHIL 140: Contemporary Moral Issues
- CCJS 100: Introduction to Criminal Justice
- CSIA 301: Information Systems Architecture
- IFSM 304: Ethics in the Information Age
- CSIA 412: Senior System Managers and Security
- CSIA 413: System Administrators and Information Security
- CMIT 320: Network Security
- CCJS 421: Computer Forensics
- CSIA 457: Cyber Crime and Cyber Terrorism

You can see the unique balance of topics in math, programming, security, forensics and ethics. Individuals with degrees in mathematics, computer science and electrical engineering would also be candidates for higher level and niche positions in cybersecurity requiring the design of algorithms and hardware for detection and countermeasures.
What Cybersecurity Jobs are In Demand?

A search of usajobs.gov, monster.com, CareerBuilder.com, or dice.com for “Cybersecurity” would quickly give you an understanding of the current demand level and various skills required.

We list the various job titles first and explore a few descriptions in another section to follow.

Cybersecurity Analyst
Senior Cybersecurity Analyst
Cybersecurity Mobile Security Analyst
Cyberintelligence Analyst
Defense INTEL Officer For Cyber Issues
Cybersecurity Programmer
Encryption Engineer
Cybersecurity Software Engineering Researcher
Computer Systems Engineer – Identify Management
Cyber Systems Engineer
Senior Cyber Forensics Engineer
Senior Project Manager – Cybersecurity
Project Engineer – Cybersecurity
Academic Director – Cybersecurity

Who is Hiring Cybersecurity Related Jobs?

Northrop Grumman
Lockheed Martin
Raytheon
IBM
BAE Systems
Battelle
Booz Allen Hamilton
General Electric
CyberCoders Engineering
Johns Hopkins Applied Physics Laboratory
ManTech International
University of Illinois, National Center for Supercomputing Applications
National Protection and Programs Directorate

What Specific Knowledge and Skills are Required?

The answer depends on the role and employer, however a solid list of entry-level buzz words follows:

UNIX OS to include BSD or Linux. TCP/IP, Shell scripting, C/C++/C#, python, PERL, Ruby, HTML, PHP, Relational Databases and SQL (Structured Query Language).
Routing, firewall functionality, host/network intrusion detection systems, encryption, load balancing.
GIAC Certified Intrusion Analysis (GCIA) or GIAC Certified Incident Handler (GCIH).
## Career Profile: Cybersecurity Analyst

<table>
<thead>
<tr>
<th>Position Title</th>
<th>Cyber Security Analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Washington DC</td>
</tr>
<tr>
<td>Clearance Reqd</td>
<td>Yes - Not Required to Start</td>
</tr>
<tr>
<td>Clearance Type</td>
<td>None</td>
</tr>
</tbody>
</table>

### Daily Responsibilities

SRA is actively seeking talented IT security professionals at mid and senior career levels to join our growing cyber security and privacy team. Team members support our clients by:

- analyzing security programs;
- developing security policies and procedures;
- participating in the security authorization process;
- preparing risk assessment reports;
- developing system security plans, risk mitigation plans, contingency plans, and disaster recovery plans;
- supporting security tests and evaluations (ST&Es);
- creating Plans of Action and Milestones (POA&Ms);
- conducting FISMA self-assessments;
- conducting system security assessments; and
- providing security documentation support.

### Required: Years of experience (min)

6-9

### Required: Degree

Bachelors

### Required: Basic Qualifications

Successful candidates will possess a mix of the following knowledge, skills, and abilities:

- familiarity with **FISMA**, **FIPS**, the **NIST 800** series, OMB A-130, and other information security-related federal guidelines;
- Bachelor's or Master's degree in a related discipline; and
- an active government security clearance, or the ability to obtain one.
### Career Profile: Cybersecurity Programmer

<table>
<thead>
<tr>
<th>Position Title</th>
<th>Cybersecurity Programmer 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Costa Mesa, California</td>
</tr>
<tr>
<td>Clearance Reqd</td>
<td>Yes – Not Required to Start</td>
</tr>
<tr>
<td>Clearance Type</td>
<td>None</td>
</tr>
</tbody>
</table>

#### Daily Responsibilities
- Establish and execute an R&D agenda in Cyber Operations to assist in building an external and internal programmatic funding base
- Conceive innovative ideas for Cyber R&D programs
- Lead a team of programmers in C#, Java, C/C++ and other software development
- Oversee and contribute to the full life-cycle modeling, documenting and maintaining of developed software applications and systems
- Conduct research into and develop novel digital communications platforms and networks
- Develop XML-based solutions via web services and Service-Oriented Architectures
- Debug, analyze, and modify software written by others
- **Reverse engineer** and analyze programs at the assembly code level
- Write project proposals and pre-proposal documents
- Utilize sound task management and effective communication skills in initiating, planning, executing, and monitoring task activities involving multidisciplinary teams
- Monitor task progress, manage critical path activities and ensure adherence to key task performance indicators

#### Required: Years of experience (min)
Minimum of 8 years experience in Computer Science, Computer Engineering, or related technical area.

#### Required: Degree
Bachelor’s degree in Computer Science, Computer Engineering, or related.

#### Required: Basic Qualifications
- Proficient in C#, Java and C/C++ and scripting languages
- Proficient in network operations and programming network applications
- Proficient in XML technologies/programming, web services and Service-Oriented Architecture
- Proficient in database programming including **MySQL** and MS SQL Server
- Advanced knowledge of networking protocols and applications at all layers of the network stack
- Sole US Citizenship with the ability to obtain and maintain government security clearances.
- Exceptional communication skills.
Activity Group Four: Preparation for Cyber Patriot

Activity 4.1: Introduction to Cyber Cup and Cyber Patriot

Watch the promotional videos on Cyber Patriot III and the San Diego Cyber Cup Challenge.

Competing teams will download a virtual computer image target with pre-configured vulnerabilities which they must quickly find, close and lock down. This process is known as hardening.

Activity 4.2: CyberNEXS Training Environment Brief

Review the CyberNEXS brochure while watching the SAIC video on the capabilities of the Cyber Network Exercise System. You can find this video on SAIC's Media Download page.

CyberNEXS addresses the present short falls in Cyber Security training. It is designed to reinforce book learning with practical opportunities in a safe, self-contained environment that emulates the standard enterprise. CyberNEXS also quantifies and trends performance of the team and individual with real-time feedback. Scores are based on how well critical services are maintained, how well the system is hardened, and how well the team communicates status and resource requirements.

Activity 4.3: Review the Presentation and Video for Windows Security Tips

1. Windows Security Tips Presentation
2. Video of Windows Security Tips

Activity 4.4: Review the Presentation and Video for Unix Security Tips

1. Unix Security Tips Presentation
2. Video of Unix Security Tips

Activity 4.5: Learn About VMWare

Cyber Patriot makes extensive use of VMware Player, a free virtualization product that allows you to “run a computer within your computer”. You and your team will be downloading or receiving VMware images for Cyber Patriot training and competitions. Any time you download a Cyber Patriot image it is extremely important that you verify you have a “clean” download. You may do this by matching the checksum of the file you downloaded with the checksum displayed on the web page where you downloaded the Cyber Patriot image.

A checksum is a mathematical calculation based on the data contained in a file – matching checksums allows you to determine if a file has been corrupted or modified from its original state. If the checksum of the file you downloaded does not match the checksum displayed on the web page where you downloaded the file you must download the image again. While the file may seem “okay”, if the checksums do not match a variety of unexpected errors could occur.
Activity 4.6: Validating Windows Computer System Capability for Installation of VMWare

In addition to having an OS (Operating System) that runs VMware Player, your computer will require:
. 2 Gigabytes of RAM,
. 15 Gigabytes of hard drive space,
. a Screen Resolution of 1280 x 1024, and
. a Network connection with at least 256Kbps down & 64kbps up to the internet.

You may verify your Windows system memory with a right click of My Computer or Computer as shown in the image below.

Next we will need you to verify the size of your hard drive and remaining free space. You can do this by right clicking on the letter for the hard drive on which you will install the software.

Activity 4.7: Download and Install 7-Zip and MD5

7-Zip is an open-source file archiving tool distributed under the GNU Lesser General Public License. You will use it to unpack some of the large virtual system images we are about to download.

1. Go to the 7-Zip Download Page
2. Click on the "Download" link for the 7-zip executable to download 7-zip.
3. Once the "File Download" window appears, click the "Run" button.
4. Once the download is complete, the 7-zip setup window will appear. Click "Install".
5. Click "Finish" when the installation is complete.

WinMD5Free is a tiny and fast utility to compute MD5 Hash Values for files and message strings. You will need it to verify your successful, accurate download of several large files.

1. Go to [http://www.winmd5.com](http://www.winmd5.com) and click the "WinMD5 Freeware Download" link.
2. We will save this file to the "Desktop" by clicking the "Save" button.
3. After WinMD5free has finished downloading, right click on it and select "7-zip> Extract Here".
4. The "WinMD5free" icon should appear on your desktop.

Details for this installation pair are also available from [SAIC's CyberNEXS Game Instructions](http://www.winmd5.com).

**Activity 4.8: Download and Install VMWare Player**

Go to SAIC's [detailed guide for downloading and installing VMWare](http://www.winmd5.com) and follow those instructions.

**Activity 4.9: Download and Install Fedora Core Image**

**Fedora Core 12 Virtual Machine**: (MD5 Hash of A204524A33A5B7D2DD33D58417F0069F)

This Linux-based virtual system should be downloaded for the "Using MD5 to Verify Downloads" and "Introduction to VMWare" Cyber Patriot activities. This virtual machine is also used in labs associated with many of the Cyber Patriot modules. You will need to download and install a copy of the VMWare Player software before you can use this image.

Once you have downloaded the Fedora Core image as a zip file, you will want to verify the “message digest” or checksum using MD5. Double-click “WinMD5Free” to launch the checksum program.

The “A204524A33A5B7D2DD33D58417F0069F” is the value to be placed in the lower field if you wish to verify the FC12 zip file. You can paste the value as copied from the website. If the two checksums match, you have a good copy and may proceed. Otherwise, you will need to download again.

Next, we strongly recommend you use 7-Zip to decompress this image and all other zip files. Finally, visit the [Modules Section of the Preparation Page](http://www.winmd5.com) to download and read each of the Five Cyber Patriot Modules. Work through the examples and practice Linux using the [One-Page-Reference](http://www.winmd5.com).
Unit Profile: 688th Information Operations Wing

The 688th Information Operations Wing is located at Lackland AFB, San Antonio, Texas.

It was originally activated on 1 July 1953 as the 6901st Special Communications Center. On 1 July 1975, it was re-designated as the Air Force Electronic Warfare Center (AFEWC). The AFEWC's electronic combat and technical expertise contributed to Operation DESERT STORM and associated command and control warfare (C2W) successes.

The success in exploiting enemy information systems during Operation DESERT STORM led to the strategies and tactics of C2W being expanded to the entire information spectrum as information warfare (IW). In response, the unit was re-designated as the Air Force Information Operations Wing (AFIOC) on 10 September 1993 and contained technical skills from the former AFEWC and Air Force Cryptologic Support Center's Securities Directorate (AFCSC/SR).

The 688th team is presently comprised of more than 1200 military and civilian members skilled in the areas of engineering installation, weaponeering, operations research, intelligence, communications and computer applications. The 688th is composed of two groups: the 318th Information Operations Group (IOG) at Lackland AFB and the 38th Cyberspace Engineering Group (CEG) at Tinker AFB.

Mission Statement: “Deliver proven Information Operations and Engineering Infrastructure capabilities integrated across air, space and cyberspace domains.”

Patriot Bio: Col Robert J. Skinner

Colonel Robert J. Skinner is Commander, 688th Information Operations Wing, Lackland AFB, TX.

In this capacity, he leads 1,200 professionals in developing, training, exercising and testing information operations tactics, techniques and procedures for:

1. Analyzing and mitigating U.S. cyberspace vulnerabilities;
2. Integrating emerging information dominance capabilities in support of Air Force and Joint DOD war-fighters; and
3. Engineering, deploying and delivering survivable and resilient cyber infrastructure, for both in-garrison and deployed units.

Sample of Qualifications:
1989 Bachelor of Science Computer Science, Summa Cum Laude, Park College, Parkville, MO.
1990 Basic Communications Officer Training, Honor Graduate, Keesler AFB, MS.
1993 Master of Science in computer science, Honors, Oklahoma City University, OK.
1995 Squadron Officer School, Distinguished Graduate, Maxwell AFB, AL.
1996 Software Engineering Certification, Air Force Institute of Technology, Dayton, OH.
1998 Advanced Communications Officer Training, Gen. Paschal Award winner, Keesler AFB, MS.
2000 Command & General Staff College, AFCEA Writing Award Winner, Fort Leavenworth, KS.
2003 Air War College, correspondence, Air University, Maxwell Air Force Base, AL.
2006 Industrial College of the Armed Forces (Information Strategies Concentration)
Conclusion and Next Steps

The realities of the world have changed dramatically since the 1947 creation of the US Air Force and they continue to change rapidly. With these changes in mind, Air Force leaders released a new mission statement in 2008 with revisions in 2009 that defined the future direction of the service.

The new USAF mission statement became “to fly, fight and win... in air, space and cyberspace.”

In this Cybersecurity module, we’ve come to see that a secure “cyberspace” includes network security, data transmission and the sharing of corporate and military secrets. As we have seen throughout history, this process is vital to our national security and well-being.

We’ve learned that many American Airmen are dedicated to cyberspace with efforts to secure networks from penetration, as well as devising countermeasures. The Air Force is a natural leader in the cyber world and previous leaders thought it wise to recognize this fact.

We’ve introduced the concepts and specific strategies in Information Assurance and Cyber Warfare and have provided opportunities for future learning.

Before you continue on to the End of Module Exam, we recommend that you review the various sections of this document to include the Chronology, Biographies and the Glossary.

A Cybersecurity Checklist for Future Exploration

[ ] Watch the AMAZING video lessons at CyberSecurityVcast and from ImpervaChannel.

[ ] Visit the Air Force Association’s YouTube page and the US Cyber Patriot Home Page.
[ ] Visit the US Computer Emergency Readiness Team and their Tips Page.

[ ] If you are inclined, visit the CIA’s website of games and codes. Yes, a kids page really exists.

[ ] Create a Gmail News Alert (or other provider) to advise of cybersecurity issues as they happen. Good search terms include: hacking, cyber-espionage, phishing, cyber-spy, cyber-crime.

[ ] Join the Air Force Association’s new Cyberville Game on Facebook.
[ ] Contribute findings and system hardening tips to the CAP Cybersecurity Group.

[ ] Create and carry your Captain Cyber Patriot USB Flash Drive wherever you go, with the exception of DoD installations where Flash Drives are not welcome. Use the tools you have placed there to help others maintain a secure computing environment.

[ ] Explore Tutorials for Encryption and Codebreaking on YouTube and on the web.
[ ] Explore Tutorials for Windows Power Shell at Microsoft TechNet, YouTube and elsewhere.

[ ] Learn HTML. Consider creating or maintaining and securing a squadron website.
[ ] Learn SQL. SQL is important for database applications like SIMS and eServices.

[ ] Learn the TCP/IP stack.

[ ] Consider more serious training to achieve a Global Information Assurance Certification.
Activity Group Five: End of Module Exam

This End of Module exam consists of 26 questions to test your comprehension of the urgency of the cyber threat, its vectors, and available countermeasures.

1. Who are most likely to launch successful cyber terrorist attacks against classified networks and critical infrastructure?
   a. Nation-states
   b. Russian hackers
   c. Chinese hackers
   d. al Qaeda

2. Which country's military hacked into computers in the office of US Secretary of Defense Robert Gates?
   a. Iran
   b. Russia
   c. North Korea
   d. China

3. Israel believes that cyber warfare is the best tool for controlling the aggression of which of its Middle-eastern neighbors?
   a. Iraq
   b. Iran
   c. Syria
   d. Saudi Arabia

4. Which of the options below is a more common type of attack used on Web sites?
   a. Denial of Service
   b. Session Hijacking
   c. Cross-site scripting
   d. HTML code injection

5. To “Deliver proven Information Operations and Engineering Infrastructure capabilities integrated across air, space and cyberspace domains” is the mission of which unit?
   a. 24th Air Force
   b. US CYBERCOM
   c. 67th Network Warfare Wing
   d. 688th Information Operations Wing

6. The Zimmerman telegram was a coded message from ________ to ________ during ________.
   a. Yamamoto; Hitler; World War II
   b. Germany; Japan; World War II
   c. Germany; Mexico; World War I
   d. Japan; Germany; World War II
7. In the late 1990s, a “red team” of penetration specialists from the NSA was challenged to infiltrate Pentagon systems using only publicly available computer equipment and software. It became known that this team infiltrated and took control of the Pacific command center computers, as well as power grids and 911 systems in nine major U.S. Cities. What was the name of this operation?

a. Eligible Receiver  
b. Operation Aurora  
c. Titan Rain  
d. Moonlight Maze

8. A DoD contractor requires employees to provide both user-name and password combined with a fingerprint scan to access its computer system. What method of security is this?

a. Intensive Verification  
b. Two-stage Verification  
c. Biometric Authentication  
d. Both b and c

9. What are the three basic components of information security?

a. Cooperation, Investigation, Assiduity  
b. Confidentiality, Invulnerability, Accessibility  
c. Confidentiality, Integrity, Availability  
d. Confidentiality, Invulnerability, Accessibility

10. Given a range of new IP addresses, which method would potential attackers implement to determine if an operating computer was present at one of those addresses?

a. NOC-ACK Scan  
b. ARP Scan  
c. Tracert Review  
d. Ping Sweep

11. Which of the following is a broken cryptographic hash function?

a. 7-Zip  
b. SHA-2  
c. MD5  
d. all of the above

12. Which wing is composed of “five intelligence groups, 35 squadrons and detachments, and more than 8,000 people serving in 100 locations around the world to help shape global events?”

a. 688th Information Operations Wing  
b. 67th Network Warfare Wing  
c. 66th Special Operations Wing  
d. 67th Intelligence, Surveillance and Reconnaissance Wing

13. The 21st Air Force is the USAF component of USCYBERCOM.

a. True  
b. False
14. Which of the following are valid Linux-distributions?

a. openSUSE, Debian GNU/Linux
b. Ubuntu, RedHat, Fedora
c. VMWare, RedHat, Debian
d. Both a and b
e. a, b and c

15. A covert agent changes a single coordinate number in a long message data stream. When the file is verified through a cryptographic hash function, the message digest is radically different from the original. Crypt-analysts call this phenomenon the _______.

a. snowball effect
b. avalanche effect
c. domino effect
d. cascade effect

16. Who created the Institute for Cybersecurity in 2007?

a. University of San Diego
b. University of Maryland
c. University of Texas San Antonio
d. Massachusetts Institute of Technology

17. What language was designed to retrieve information from relational databases?

a. C#
   b. TCP/IP
   c. SQL
   d. parsec

18. What do Cybersecurity Analysts call the path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a malicious payload?

a. Trojan
   b. Vulnerability channel
   c. Backdoor
   d. Attack vector

19. STRIDE is an acronym of the six threat categories to include _________________________.

a. Spoofing, Tampering, Denial of Service, and Elevation of Privilege
b. Spear-phishing, Repudiation, Information Disclosure, and Elevation of Privilege
c. STUXNET, Titan Rain, Eligible Receiver
d. Both a and b are correct

20. Crackers in Serbia attacked NATO systems in retaliation for NATO’s intervention in Kosovo.

a. True
   b. False
21. When a user-supplied field is not strongly typed or is not checked for type constraints, a cracker could devise a string to enter into the prompt that would authenticate or reveal user information. This type of attack against the database and its natural language is called ________________.

a. SQL Injection  
b. Perl Insertion  
c. Cross-scripting  
d. Denial of Service

22. GIAC is the Global Information Assurance Certification. The organization offers certifications to include ____________.

a. GCIH: Certified Incident Handler  
b. GCIA: Certified Intrusion Analyst  
c. Both a and b  
d. None of the above

23. When students use a Mac computer to run a simulation of a specific Linux Operating System, this is called ________.

a. Virtualization  
b. Artificial Reality  
c. Open Software Rendering  
d. Phishing

24. The process by which vulnerabilities in a networked computer system are methodically identified, closed and locked down is known as _____________.

a. Defending  
b. Securing  
c. Rendering  
d. Hardening

25. A ________ is a type of malware that gains administrative-level control over a computer system without being detected. It can change how the operating system functions and even render Anti-Virus software ineffective.

a. Trojan  
b. Rootkit  
c. Worm  
d. Fisk

26. Name the Cyberweapon that was designed to target industrial software and equipment, to include Siemens programmable logic controllers.

a. Titan Rain  
b. Aurora  
c. Stuxnet  
d. Shady RAT
Appendix A: Motivational Chronology of Cyber Warfare

600 BCE: Hebrew scholars employ a simple mono-alphabetic substitution code known as an Atbash Cipher. In this cipher, the letters of an alphabet are simply reversed, a for z, b for y, and so on.

480 BCE: Demaratus, a Greek living in Persia, becomes aware that Xerxes is moving his armies to attack Greece. In those days, wooden tablets are covered with wax and used for writing. Demaratus writes a warning message directly on a wooden tablet and then covers it with wax, allowing this key information to be smuggled out of Persia to Greece. Herodotus later documents this and other examples of Greek steganography, or concealed writing.

60 BCE: Julius Caesar, according to Suetonius, employs a shift cipher to protect messages of military significance.

1803: US President Thomas Jefferson asks Meriwether Lewis to send frequent dispatches from the field and to “put anything into cipher which might cause harm if betrayed.”

Dec 1812: A coded letter from Joseph Bonaparte to Napoleon is intercepted. Sir George Scovell eventually breaks the Great Paris Code, and Wellington uses the intel to defeat the French at Vittoria on June 21, 1813.

Jan 1917: A coded telegram is sent from Arthur Zimmermann, Foreign Secretary of the German Empire, to the German ambassador in Washington, D.C., Johann von Bernstorff. It is then forwarded to the German ambassador in Mexico. The telegram is intercepted and decoded by British cryptographers of Room 40 to reveal a proposal for Mexico to make war against the United States.

Feb 1918: Arthur Scherbius, a German electrical engineer, applies for a patent for a cipher machine based on rotating wired wheels, now commonly called a rotor machine. One of the commercial models, called Enigma, would be adopted by the German Navy in 1926.

1940: The US Army Signals Intelligence Service (SIS) breaks Japan's PURPLE machine cipher.

Apr 1943: Admiral Yamamoto, who designed the attack at Pearl Harbor, is killed by US forces who know his itinerary from decoded messages.

Dec 1946: Meredith Gardner makes the first break into the VENONA code, revealing the existence of Soviet espionage at the Los Alamos National Laboratory.

1972: The infamous phreak, John Draper, becomes known as Captain Crunch when he discovers that he can fool AT&T's network with the tone from a plastic whistle distributed in the breakfast cereal.

1997: The US DoD initiates an internal exercise known as Eligible Receiver. A "red team" of hackers from the National Security Agency (NSA) are authorized to infiltrate Pentagon systems using only publicly available computer equipment and hacking software. Although some details are still classified, it becomes known that the red team infiltrated and took control of the Pacific command center computers, as well as power grids and 911 systems in nine major U.S. cities.
March 1998: Moonlight Maze begins. This is a pattern of computer system probes at the Pentagon, NASA, United States Department of Energy, private universities, and research labs that continue for nearly two years. Invaders systematically maraud through tens of thousands of files, to include maps of military installations, troop configurations, and military hardware designs. The US DoD trace the trail back to a mainframe computer in the former Soviet Union but Russia denies any involvement. Moonlight Maze is still being actively investigated by U.S. intelligence.

March 1999: Crackers in Serbia attack NATO systems in retaliation for NATO's intervention in Kosovo.

May 1999: NATO accidentally bombs the Chinese embassy in Belgrade, spawning a wave of cyber attacks from China against US government web sites.

2000: FBI Agent Michael Schuler lures two suspected Russian cyber criminals to the US in an elaborate ruse. The FBI captures their usernames and passwords with a keylogger that was covertly installed on a US machine that both used to access their computers in Russia. The FBI then uses these credentials to hack into the suspects' computers in Russia in order to obtain evidence to prosecute them.

April 2001: A Shenyang J-8 interceptor jet of the People's Republic of China collides with a EP-3E ARIES II Signals Intelligence Aircraft operated by the US Navy. This results in the death of the J-8 pilot and forcing the EP-3 to land on Hainan Island.

2003: Crackers begin a series of assaults on US government computer systems that lasts for years. The government code names the attacks Titan Rain and eventually traces them to China.

Jan 2008: Senior CIA analyst Tom Donahue publicly states at a conference that attackers have targeted power-grid computers worldwide, causing at least one widespread outage.

2008: The Pentagon reports some 360 million attempts to break into its network, up from just 6 million in 2006. That includes a reportedly successful attempt to hack into the $300 billion Joint Strike Fighter project and copy data about the aircraft's design and electronics systems.

2009: POTUS declares America's digital infrastructure to be a "strategic national asset."

June 2009: Secretary of Defense directs the Commander of US Strategic Command (USSTRATCOM) to establish USCYBERCOM.

July 2009: Michael Coppola wins SANS Institute NetWars competition, by ignoring the main targets and taking control of the game's scorekeeping algorithm. At the end of the game, his score is three times higher than everyone else's. Some might view this young man as a cheater or, worse, a cybercriminal in training. Alan Paller sees him as the future of America's national security.


"USCYBERCOM plans, coordinates, integrates, synchronize, and conducts activities to: direct the operations and defense of specified Department of Defense information networks; and prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace, and deny the same to our adversaries."
**July 2010:** Michael Hayden, former Deputy Director of national intelligence challenges thousands of attendees at the 2010 Black Hat Conference to help devise ways to “reshape the internet's security architecture,” explaining, "You guys made the cyberworld look like the north German plain."

**2010:** The FBI reveals that the Russian foreign intelligence service uses customized steganography software for embedding encrypted text messages inside image files for communications with agents stationed abroad.

**19 July 2010:** The People’s Liberation Army unveils its first department dedicated to tackling cyber war threats and protecting information security.

**Dec 2010:** Iran's covert uranium enrichment plant at Natanz may have lost 1,000 centrifuges due to damage caused by the **Stuxnet** cyber weapon, according to a report by the Institute for Science and International Security. Stuxnet attacks industrial hardware, such as programmable logic controllers.

**Feb 2011:** McAfee reports that several multinational oil companies were victims of cyber espionage by Chinese hackers who downloaded sensitive data from their corporate networks, including the companies’ crown jewels – “bid data” detailing oil discoveries worldwide. **Spear-phishing** attacks were used, wherein an email looks as if it comes directly from one’s boss or coworker. Links in the email typically connect to an infected site or open an infected attachment that installs a secret backdoor on the machine.

**Apr 2011:** Researchers at George Mason University's Mercatus Center author a paper entitled “Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy.” They contend that various hacker activities, and the resulting media hype, are actually designed to create a “cyber-industrial complex” to ramp up cybersecurity interests.

**Apr 2011:** Sony Corp. announces that hackers obtained personal data, and possibly credit card information, from tens of millions of people who had registered for PlayStation Network, the company’s online game and movie service, as well as Qriocity, its on-demand digital music service.

**Apr 2011:** The US Justice Department Inspector General reports that many of the FBI's field agents assigned to an elite cyber investigative unit lack the required skills to investigate cases of cyber espionage and other computerized attacks on the US.

**Jun 2011:** Google reveals that a computer **phishing** scam originating in China was directed at an unknown number of White House staff officials. The intended victims ranged across different functions in the White House and were not limited to those working on national security, economic policy, or trade areas that would be of particular interest to the Chinese government.

**13 Jun 2011:** The e-mails and passwords of a number of users of senate.gov, the website of the United States Senate, are hacked and released. **LulzSec** stated, "This is a small, just-for-kicks release of some internal data from senate.gov — is this an act of war, gentlemen? Problem?"

**15 Jun 2011:** The website of the Central Intelligence Agency is shutdown for several hours in a **Denial of Service Attack** launched by LulzSec.

**1 Aug 2011:** The suspected leader of LulzSec, believed responsible for the Sony Playstation Network hack in April, is released on bail.
1 Aug 2011: Anonymous hackers attack FBI contractor ManTech International. Documents belonging to NATO, the US Army, the US Department of Homeland Security, the US State Department, and US Department of Justice are said to have been compromised.

Appendix B: Glossary of Terms, Threats, and Countermeasures

In recognizing the need for a place to get quick explanations while working this module or the CyberPatriot program, the following Glossary of Terms is provided for quick reference. If working online, each term is hyperlinked to its definition. This is by no means a comprehensive list and readers should look to find the current Jargon File online for additional terms.

7-Zip: A free open source file archiver distributed under the GNU Lesser General Public License and noted for its "excellent compression ratio."

Active Content: Interactive web content that could carry malicious code.

ActiveX Control: Microsoft Windows software component used to create and distribute small applications through Internet Explorer. Because ActiveX controls can be used to perform a wide variety of functions, including downloading and running programs, vulnerabilities in them may be exploited by malware. In addition, cybercriminals may also develop their own ActiveX controls, which can damage a computer if a user visits a webpage hosting such a malicious control.

AES: Advanced Encryption Standard, which replaces the weaker DES (Data Encryption Standard developed by the National Institute of Standards and Technology). AES is similar to DES in principle but uses much longer keys (128, 192 or 256 bits) and is specifically designed to resist the most sophisticated cryptographic attacks, using methods such as timing analysis and power analysis. It's very low memory requirements are particularly suited for embedded applications, such as smart cards.


Anonymizer: A tool that acts to make certain internet activity is untraceable. This is implemented as a proxy server computer that accesses the internet on the user's behalf, thereby hiding the client computer's identifying information.

ARP: Address Resolution Protocol, which is a telecommunications protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.

ARP Attack: A technique used to attack a local-area network that makes use of the Address Resolution Protocol. ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, and stop the traffic altogether. The attacker will associate his MAC address with the IP address of another host (such as the default gateway). Any traffic meant for that IP address would be sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (interception) or modify the data before forwarding it (man-in-the-middle attack). The attacker could also launch a denial-of-service attack against a victim by associating a nonexistent MAC address to the IP address of the victim's default gateway.

Availability: Assurance that the data is available when needed. A lack of availability occurs if any network failure or DoS attack prevents an authorized user to gain access to a file stored in a Server.

AVG Antivirus: AVG is a family of anti-virus and internet security software, developed by AVG Technologies, a privately-held Czech company formerly known as Grisoft. The product has been certified by ICSA labs. In one review at PCWorld.com, the AVG 7.5 product received a 77/100. It did a "fine job" in disinfection tests, but ranked last of the ten products tested in proactive protection using one-month-old signature files.
Backdoor: A tool installed during development or after a compromise to give easier access to a system by circumventing any security mechanisms that are in place. A backdoor trojan is a type of trojan that provides attackers with remote unauthorized access and control of infected computers. Bots are a subcategory of backdoor trojans (see Botnet).

Bastion Host: A bastion host is usually a highly-exposed device that has been hardened or locked down in anticipation of vulnerabilities because it resides within the DMZ or Demilitarized Zone.

Biometrics: The practice of using human biological patterns for authentication. These could include eye retina scans, fingerprint scans, and voice-pattern recognition.

Black Hat: Borrowing from the flavor of the western movie, a black hat is a villain or bad guy and in our context refers to a computer security hacker that breaks into networks or computers or creates computer viruses.

Black Hat Briefings: A computer security conference that brings together a variety of people interested in information security. Representatives of federal agencies and corporations attend along with hackers.

Blacklist: A way to filter internet traffic so that all traffic is allowed except for that from selected servers.

Bluejacking: Sending unsolicited messages to Bluetooth devices. This is basically Bluetooth-based spam, but the possibility exists that this practice will evolve into Trojan Horse-style takeovers of Bluetooth assets. The Cabir worm has spread across mobile phones using Bluetooth.

Bluesnarfing: Unauthorized access of information from a wireless device through a Bluetooth connection (contact lists, pictures, data, etc.). The flaw that allowed this exploit has since been patched in current Bluetooth devices, and Bluesnarfing should no longer pose any real threat.

Bluebugging: Unauthorized control of Bluetooth assets. This more recent development may pose the greatest threat, as the technique is refined and improved.

Botnet: A network consisting of thousands of machines that have been infected with Trojan Horse viruses and are now controlled by criminals.

C4ISR: A term used by the US military that means Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

Cabir worm: One of the malicious software; usually referred as malware.

CAPTCHA: A software tool used on web sites to differentiate humans and internet bots.

CERT: Originally the Computer Emergency Response Team, CERT is a program tasked with protecting internet resources through a combination of analysis, education, and coordination activities. Various portions of the CERT program are managed by Carnegie-Mellon University and the Department of Homeland Security.

Checksum: A checksum or hash sum is a fixed-size data string computed from an arbitrary block of digital data for the purpose of detecting accidental errors that may have been introduced during its transmission or storage. If the checksum of the file you downloaded does not match the checksum displayed on the web page where you downloaded the file you must download the image again. While the file may seem “okay,” if the checksums do not match, a variety of unexpected errors could occur.
**CIA Triad:** The three components of information security: **Confidentiality, Integrity, and Availability.**

**Cipher:** An algorithm, or method, for converting text to an unreadable form. In the Caesar Cipher, letters were simply shifted two alphabetical positions, so “this” would become “vjku.”

**cmdlet:** Specialized commands in the PowerShell environment that implement specific functions.

**CNCl:** **Comprehensive National Cybersecurity Initiative.**

**Code:** The words code and cipher are often confused. A code is implemented when a word or phrase is used to mean something completely different. A cipher encrypts the letters of a message to a different set of characters. Choctaw Code and Navajo Code were actually different languages.

**Code Red:** A worm with multiple variants that first appeared in July 2001 and ultimately affected nearly 300,000 computers in the US. From days 1-19 of the month the worm would propagate; from days 20-27 it would launch a denial of service attack against the White House web site using thousands of pings; and from day 27 through the end of the month the worm would “sleep,” dormant in the computer. Richard Clarke, the president's adviser for cyberspace security, worked with the nation’s internet providers to thwart the attack by blocking traffic to the White House site.

**Confidentiality:** Assurance that information is shared only among authorized persons. Breaches of Confidentiality can occur when data is disclosed in any way. Examples include watching the content of a document or eavesdropping on a conference call.

**Computer Security:** Any proactive or reactive steps to protect smartphones, computers, company servers, IP phones, or set-top boxes from spam, viruses, worms, trojan horses, malware, and intrusion. It is defined as methods and technologies for deterring, protection, detection, response, recovery, and extended functionality in information systems.

**Cookie:** Information, usually in a file, about someone's internet activities, such as the date of the last visit to a web site, and preferences, etc., that will be sent back to the web site of origin on the next visit.

**Cookie Scrubber:** A tool for removing cookies which contain a user's sensitive authentication and web-surfing history information.

**Countermeasure:** An action taken to offset another one and to prevent an undesirable outcome in the process.

**Cracker:** The media uses the terms cracker and hacker interchangeably, they are not the same and this has become a point of contention. Hackers see themselves as technically-skilled individuals who build things and overcome limitations; crackers are viewed as those who break things.

**Cross-site scripting:** A vulnerability of dynamic web content where a malicious user may embed code into a web site that may cross over to a victim's computer.

**Cryptography:** The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Cryptographic hash function: A deterministic procedure, or finite list of well-defined instructions, that takes an arbitrary block of data and returns a fixed-size bit string, called the (cryptographic) hash value. Any accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest, or, simply, digest. Examples include MD-5, MD-6, SHA-1 and SHA-2.

Cyber bullying: The use of information or communication technologies to engage in or support deliberate, repeated, and hostile behavior by an individual or group, with intent to harm others.

Cyber espionage: The use of software tools to obtain secret or private government or business information.

CyberNEXS: SAIC's new cyber-training, competition, and certification product for the protection of critical data assets. SAIC (Science Applications International Corporation) is a leader in cybersecurity training and provides the competition engine for the Air Force Association (AFA) National High School Cyber Defense Competition called CyberPatriot.

Cyber terrorism: Any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. A cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the US Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.

Cyberwarfare: In his May 2010 book Cyber War, Richard A. Clarke defines cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

DEF CON: One of the world's largest annual hacker conventions, held every year in Las Vegas, Nevada. Federal law enforcement agents from the FBI, DoD, US Postal Inspection Service, and other agencies regularly attend DEF CON.

Defense-in-Depth: Defense-in-Depth is a security strategy in which multiple layers of protection are placed throughout the organizational assets. In a network environment, Defense-in-Depth involves the placement of multiple network defense components and segmenting the network properly to deter, prevent, detect, and respond to network attacks. These components include routers, firewalls, IDSs, DMZs, bastion hosts, antivirus software, and much more.

Demilitarized Zone: A term appropriated from the Korean War in which a neutral zone is established. In our CyberPatriot context, a DMZ is a machine or group of machines sitting between the internal network and the external environment (usually, the internet). DMZs should contain only those devices and services that require external access, such as e-mail or web services. The DMZ should not include any machines or services that contain information that is crucial or of extreme value or volatility.

Denial of Service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations. Time-critical may be milliseconds or hours, depending upon the service provided.

DES: Data Encryption Standard developed by the National Institute of Standards and Technology. While this may have been a secure method back in 1976, current computers are powerful enough to brute-force attack the relatively short key.
**dig**: Domain Information Groper (dig) is a network administration command-line tool for querying Domain Name System (DNS) name servers for any desired DNS records. This is a modern replacement to **nslookup**.

**Digital Dirt**: Traces left behind of an individual's internet activity that could reflect poorly or be used against the individual.

**Disaster Recovery Plan (DRP)**: A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

**Distributed Denial of Service (DDoS)**: A denial of service technique that uses numerous hosts to perform the attack. A multitude of compromised systems attack a single target. Valid users cannot access the targeted system as the flood of incoming messages forces it to shut down.

**DMZ**: See Demilitarized Zone.

**DoD**: US Department of Defense.

**DoS**: See Denial of Service and Distributed Denial of Service attacks.

**Dumpster Diving**: Obtaining passwords, corporate directories, program code, or designs by searching through discarded media. The most famous case of dumpster diving is actually a quote accredited to Bill Gates: “No, the best way to prepare is to write programs and to study great programs that other people have written. In my case, I went to the garbage cans at the Computer Science Center and I fished out listings of their operating system. You’ve got to be willing to read other people's code; then write your own; then have other people review your code.”

**Elevation of Privilege**: Elevation of privilege is not a class of attack, as much as it is the process of any attack. Virtually all attacks attempt to do something the attacker is not privileged to do. The bad guy wants to somehow leverage whatever limited privilege he has and turn it into higher (“elevated”) privilege.

**Eligible Receiver**: US Department of Defense Exercise conducted in 1997 in which a "red team" of hackers from the National Security Agency is authorized to infiltrate Pentagon systems using publicly available computer equipment and hacking software. Although some details are still classified, it became known that the red team took control of the Pacific command center computers, as well as power grids and 911 systems in nine major U.S. cities.

**Email Spoofing**: A type of spoofing using email in which the sender's address and other elements of the e-mail header, such as Return-Rath and Reply-To fields, are altered to make the e-mail appear as if it originated from a different source. Core SMTP (Simple Mail Transfer Protocol) doesn't provide any authentication, thus, it is easy to impersonate and forge emails.

**Encryption**: The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

**Enigma Machine**: Various electro-mechanical rotor machines that were used for the encryption and decryption of secret messages, notably those of the German Wolfpack submarines during World War II. The first model appeared at the end of WW I and was designed by Arthur Scherbius, a German engineer.
**Ethical hacking:** Also known as penetration testing, this is when a computer and network expert attacks a security system on behalf of its owners seeking vulnerabilities that a malicious hacker could exploit.

**Event Viewer:** Microsoft has featured event logging in its high-end operating system since the release of Windows NT in 1993. Event Viewer is an operating system component that lets admins and users view events that have taken place, such as a failure to start a component or complete an action. The system defines three log sources: System, Application, and Security.

**Exploit:** A piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch, or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

**Fedora:** Linux-based operating system that provides users with access to the latest software, in a stable, secure, and easy-to-manage package. Because of its predominance, the word "Fedora" is often used interchangeably to mean both the operating system and the Fedora Project, a partnership of free software community members from around the globe.

**Firewall:** A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass. A firewall is a logical device, not a physical barrier. If an attacker can physically connect to your network, the firewall is ineffective.

**Fisking:** A term that describes the logical point-by-point criticism of an online statement, essay, or blog entry. This differs from flaming in that it completely avoids any irrational or personal attacks on the writer. It is named after British Journalist Robert Fisk.

**Flaming:** Also known as bashing, is hostile and insulting interactions between Internet users.

**Footprinting:** In the planning and probing phase of a hacker attack, footprinting is the practice of gathering useful information about computer systems and networks. Techniques include DNS queries, network enumeration, network queries, operating system identification, organizational queries, ping sweeps, point of contact queries, port scanning, registrar queries (WHOIS queries). Some programs used for footprinting are Sam Spade, nslookup, traceroute, Nmap, and neotrace.

**Forensics:** The use of mathematics, computer science, and other technology to investigate crimes.

**GIAC:** Global Information Assurance Certification.

**Global Information Assurance Certification:** A certification organization founded in 1999 to validate the real-world skills of IT security professionals. GIAC currently offers certifications for over 20 job-specific responsibilities that reflect the current practice of information security. GIAC is unique in measuring specific knowledge areas instead of general purpose information security knowledge.

**GUI:** Graphical User Interface. Many command-line tools were updated to GUI for ease of use.

**Hacker:** A hacker is a person intensely interested in the detailed workings of any computer system. Most often, they are programmers who obtain advanced knowledge of operating systems and programming languages. They learn various holes within those systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never intentionally damage data. This differs greatly from a **cracker**, who has a malicious intent.
Hainan Island Incident: In 2003, the US Navy acknowledged that “Compromise by the People’s Republic of China of undestroyed classified material... is highly probable and cannot be ruled out.”

Hardening: The process of securing a system by reducing its **surface of vulnerability**. Single purpose systems tend to be less vulnerable than multipurpose ones. To reduce available vectors of attack, administrators work to remove unnecessary software, logins, and services.

There are various methods of hardening Unix and Linux systems. This may involve, among other measures, applying a patch to the kernel, such as Exec Shield or PaX; closing open network ports; and setting up intrusion-detection systems, firewalls, and intrusion-prevention systems. There are also hardening scripts and tools like Bastille Linux, JASS, and Apache/PHP Hardener that can deactivate unneeded features in configuration files or perform various other protective measures.

Honeypot: A trap used to divert, detect, and characterize would-be attackers of a computer system.

IDS: Intrusion Detection System. An IDS is a system used to detect several types of malicious behaviors, including attacks against vulnerable services, data-driven attacks on applications, unauthorized logins, and access to sensitive files.

Information Disclosure: Information disclosure enables an attacker to gain valuable information about a system. Thus users should always consider what information they are revealing and whether it can be used by a malicious user.

Initialization Vector (IV): A vector used in defining the starting point of an encryption process within a cryptographic algorithm.

Integrity: Electronic signals are said to have integrity when there is no corruption of information between one domain and another, such as from a disk drive to a computer display. Such integrity is a fundamental principle of **information assurance**. Corrupted information is untrustworthy, yet uncorrupted information is of value.

Internet Protocol (IP): The method or protocol by which data is sent from one computer to another on the internet.

IP Address: A unique number known as an Internet Protocol (IP) address is assigned to every device connected to the public internet. IP addresses consist of four numbers separated by periods, called a ‘dotted-quad,” and look something like 127.0.0.1. An IP address can often be used to identify the region, country, or general location from which a computer is connecting to the internet. Computer operating systems provide various diagnostic tools to examine their network interface and address configuration. Windows provides the command-line interface tools ipconfig and netsh and users of Unix-like systems can use ifconfig, netstat, route, lanstat, ifstat, or iproute2 utilities to accomplish the task.

ISTAR: Intelligence (information gathering), surveillance, target acquisition, and reconnaissance. It describes methods of observing the enemy and one's area of operations.

Jargon File: A glossary of hacker slang originally from professional technical sources, such as the MIT AI Lab, Stanford AI Lab (SAIL), and ARPANET teams to include Carnegie Mellon University and Worcester Polytechnic Institute. Source: [http://www.catb.org/jargon/html/go01.html](http://www.catb.org/jargon/html/go01.html).
Kernel: The essential center of a computer operating system, the core that provides basic services for all other parts of the operating system; a synonym is nucleus. Kernel is a term used more frequently in Unix and some other operating systems than in IBM mainframe systems.

Keylogger: A device or software that records keystrokes entered by a user, usually to secretly monitor and/or maliciously use this information. There are software keyloggers, hardware keyloggers, and wireless keyboard “sniffer” keyloggers, among others. An on-screen keyboard would be an effective countermeasure against hardware keyloggers. An anti-spyware application that can only disable hook-based keyloggers will be ineffective against kernel-based keyloggers.

Kludge: A kludge (or kluge) is a workaround, a clumsy or inelegant, yet effective, solution to a problem, typically using parts that are cobbled together. This term is diversely used in fields such as computer science and aerospace engineering.

Kryptos Sculpture: A copper wave sculpture of encrypted messages located at CIA headquarters in Langley, VA. Of the four sections, three have been solved, with the fourth remaining one of the most famous unsolved codes in the world.

Logic Bomb: Programming code, inserted intentionally or unintentionally, that is designed to execute (explode) under certain logical circumstances, such as the lapse of a certain amount of time (also called a time bomb), or a certain user logging in after a date has passed.

Macro-virus: A virus that attaches itself to documents and uses the macro-programming capabilities of the document’s application to execute and propagate.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

Man-in-the-Middle Attack: In a man-in-the-middle attack, the attacker accesses the communication session between authorized parties, and observes it. Think of it as digital wiretapping. By using a sniffer, the attacker can gather information to conduct a man-in-the-middle attack. This type of attack will normally only affect the confidentiality and integrity of information.

Maraud: To rove and raid in search of plunder. To raid or pillage for spoils.

McAfee VirusScan: McAfee VirusScan is an antivirus program created and maintained by McAfee Inc, formerly known as Network Associates. McAfee markets VirusScan to home and home-office users; McAfee also develops VirusScan Enterprise for use in corporate environments. McAfee also produces a similar product for Mac OS X under the name of VirusScan for Mac.

MD5 Hash: Message Digest Algorithm 5 is a cryptographic hash function that has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. However, it has been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property.

Media Access Control address: A numeric code assigned to every network interface device by its manufacturer. The MAC address is tantamount to any particular machine’s “fingerprint” or “physical address,” because it is based on the specific hardware, and is not assigned dynamically.
Moonlight Maze: US officials accidentally discovered a pattern of computer-system probes at the Pentagon, NASA, United States Department of Energy, private universities, and research labs that began in March 1998 and continued for nearly two years. According to sources, the invaders were systematically marauding through tens of thousands of files to include maps of military installations, troop configurations, and military hardware designs. The US Department of Defense traced the trail back to a mainframe computer in the former Soviet Union, but Russia denied any involvement. Moonlight Maze is still being actively investigated by US intelligence.

Mountain View: A town in California that was the repeated target of cyber attacks. Many of the largest technology companies in the world are headquartered in the city, including the Fortune 1000 companies Google, Symantec, and Intuit. Pilots will take note that Moffett Airfield, associated with NASA Ames Research Center, is also nearby.

National Institute of Standards and Technology (NIST): An agency of the US Department of Commerce that develops and promotes measurements, standards, and technology.

National Security Agency (NSA): The cryptologic organization of the United States. The core missions of the agency, according to nsa.gov, are to protect national security systems and to produce foreign signals intelligence (SIGINT) information to our nation’s policy-makers and military.

NCM: The National Cryptologic Museum is an American museum of cryptologic history that is affiliated with the National Security Agency. It is the first public museum in the US Intelligence Community, and located two blocks from the NSA headquarters at Fort George G. Meade, MD.

NetWars: A computer and network security challenge -- an adventure across the internet, sponsored by SANS Institute. It is one of the key competitions in the US Cyber Challenge. NetWars comes in two forms: Tournament and Continuous. NetWars Tournament is a six-hour challenge played over two days at a SANS national conference. You don't have to win to earn bragging rights. If you do well and play fair, you will receive recognition. NetWars Continuous allows each participant to build their skills over a four-month period, conquering challenges throughout that timeframe.

Nimda Worm: The Nimda worm was released on September 18, 2001. Multiple propagation vectors allowed Nimda to become the internet's most widespread virus/worm within 22 minutes.

Nmap: Network Mapper is a security scanning program used to discover hosts and services on a computer network, thereby "mapping" the network. To achieve this, Nmap sends specially-crafted packets to the target host and then analyzes the responses. Example: nmap –n –sP localhost GUI versions of this tool include NmapFE, Zenmap, and XNmap.

nslookup: A command-line tool available to network administrators on many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. The command syntax is: nslookup [-option] [name | -] [server] The nslookup utility is considered obsolete, with modern alternatives being host and dig programs.

Patch: A patch is a software update to fix a security flaw. Patches may be released on a regular basis or irregular basis, depending on the vendor and support team. (Microsoft usually releases its patches on Tuesday – “Patch Tuesday.”)

Payload: The eventual effect of a software virus that has been delivered to a user's computer.

Penetration testing: Penetration testing is used to test the external perimeter security of a network or facility. See “Ethical hacking.”
**PGP**: Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication for data communication. PGP encryption employs a serial combination of hashing, data compression, symmetric-key cryptography, and, finally, public-key cryptography. Each step uses one of several supported algorithms.

**Pharming**: Redirecting users from legitimate web sites to fraudulent web sites.

**Phishing**: Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

**Phreaking**: A slang term coined to describe a subculture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks.

**Ping Scan**: A ping scan looks for machines that are responding to ICMP Echo Requests (“pings”).

**Ping Sweep**: An attack that sends ICMP echo requests (“pings”) to a range of IP addresses with the goal of finding hosts that can be probed for vulnerabilities.

**Ping of Death**: An attack that sends an improperly-large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

**Ping Flood**: Ping may also be used in DoS attacks, in which a vast number of ICMP echo request packets are sent to the target, overwhelming its capability to process all other traffic. For this to work, the attacker must have a significantly higher bandwidth than the target.

**Port**: Unnecessary ports can create problems for your system, and such systems are more prone to hacker attacks. Hackers always search for open ports on a system and if they manage to find one, they can get into your system and do anything they want. They can even prevent your access on to your system. As a good security practice, you should check if you have kept any ports open accidentally, and take appropriate action to close them.

**Portal**: An introductory web page for a given topic that combines definitions of terms, recent events, images, videos, learning activities, and various categories that further describe the subject. Some people think of portals as information dashboards on their topic of interest. Wikipedia provides a portal on Computer Security, and Microsoft provides a [Malware Protection Center](https://aka.ms/securitycenter).

**Pretexting**: The process in social engineering of providing a reason (a pretext) to be communicating with the person to be tricked. Example: Posing as a help desk employee or phone repair person.

**RAT**: Remote Access Trojans provide a "backdoor" into systems through which a hacker may exercise remote control, to include running malicious code if so desired. Hackers can even use these hijacked systems, called zombies, to launch attacks on others. Some examples of RATs include Sysbug, Back Orifice, and Lamer's Death. **Operation Shady RAT** was exposed in August of 2011.

**Repudiation**: The refusal, especially by public authorities, to acknowledge a contract or debt.

**Road apple**: An infected item that has been deliberately left for someone to pick up. For example, a CD-ROM left in a parking lot with a label reading “Executive Compensation” or “Physics 301 Exam” which in reality contains a Trojan Horse. The term is slang for a piece of horse manure on the road.

**Rootkit**: A rootkit is a type of malware that is designed to gain administrative-level control over a
computer system without being detected. Rootkits can change how the operating system functions and, in some cases, can tamper with the anti-virus program and render it ineffective.

**Sabotage:** Sabotage is a deliberate action aimed at weakening another entity through subversion, obstruction, disruption, or destruction. One who engages in sabotage is called a saboteur.

**SAACL:** System Access Control List. An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file has an ACL that contains (Alice, delete), this would give Alice permission to delete the file.

**SAIC:** Science Applications International Corp is a scientific, engineering, and technology applications company that uses its "deep domain knowledge" to solve problems of vital importance to the nation and the world. SAIC is a founding partner of the Air Force Association's [CyberPatriot](#) program.

**SANS Institute:** The largest source for information security training and certification in the world. From their website, [www.sans.org/about/sans.php](http://www.sans.org/about/sans.php), it also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security.

**Scanning:** The practice of sending packet requests to another system for the purpose of gaining intelligence in preparation for an attack.

**Scripting Language:** Most scripting languages use no compiler to pretranslate the code into faster native machine language. They are, instead, being interpreted on the fly by the application itself. PHP, JavaScript, Ruby, Perl, Python, Tcl, and VBA are all scripting languages.

**Script Kiddies:** The lowest form of cracker; script kiddies do mischief with scripts and rootkits written by others, often without understanding the exploit they are using. As they have negligible technical expertise, they rely on easy-to-operate, pre-configured, and automated tools to conduct disruptive activities against networked systems.

**Shared Key Authentication:** This is the process a computer uses to gain full access to a wireless network using the Wired Equivalent Privacy (WEP) protocol. A computer authenticated using SKA has access to encrypted and unencrypted WEP traffic.

**SMTP:** Simple Mail Transfer Protocol. An internet standard for e-mail transmission across Internet Protocol (IP) networks. SMTP is specified for outgoing mail transport and uses TCP port 25. The original SMTP specification did not include a facility for authentication of senders, and so email spoofing attacks became common.

**Smurf:** The Smurf attack works by spoofing the target address and sending a ping to the broadcast address for a remote network resulting in a large amount of ping replies being sent to the target.

**Sniffer:** A program that monitors and analyzes network traffic and is used legitimately or illegitimately to capture data transmitted on a network. While a router reads the routing information of every packet passed to it, determining whether it is intended for a destination within the router's own network, a sniffer may be able to read the data inside the packet, as well as source and destination addresses.

**Sobig:** A computer worm that infected millions of internet-connected, Microsoft Windows computers
in August 2003. CSX passenger and freight trains in the Washington, D.C. area were stopped after CSX’s telecommunications network was overtaken by the Sobig.F variant. The Sobig.F worm deactivated itself on September 10, 2003. Microsoft announced a reward of $250,000 for information leading to the arrest of Sobig’s creator. To date, the perpetrator has not been caught. The Sobig.F variant was programmed to contact 20 IP addresses on UDP port 8998 on August 26, 2003.

**Social Engineering:** An attempt to trick someone into revealing information, such as a password, that can be used to attack systems or networks.

**Spoofing:** Describes a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Webpage spoofing and email spoofing are two current sub-categories.

**SQL Injection:** SQL Insertion Attacks, or SQLIA, exploit a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thus executed. A cracker could enter ' OR 1=1 – into a Username field. As 1 has and will always equal 1, the authentication routine becomes validated and the cracker gains access.

**SQL Slammer:** A computer worm that caused a denial of service on some internet hosts and dramatically slowed down general Internet traffic on January 25, 2003. Spreading rapidly, it infected most of its 75,000 victims within ten minutes. The worm exploited a buffer overflow bug in Microsoft’s flagship SQL Server and Desktop Engine database products, but a patch for this had been released six months earlier in MS02-039. Other names include W32.SQLExp.Worm, DDOS.SQLP1434.A, the Sapphire Worm, SQL_HEL, W32/SQLSlammer, and Helkern.

**SSH:** Secure Shell is a Unix application and associated security protocol used to gain secure access to a remote computer by establishing an encrypted connection. SSH protects users from malicious hacking attacks such as IP spoofing, IP source routing, and DNS spoofing.

**SSID:** Service Set Identifier. This is the name assigned to a wireless network. The associated risk lies in SSID broadcasting, or "beaconing," in which the access point effectively shouts “here I am,” so that it can be found by computers with wireless cards. Manufacturers typically provide a default SSID, such as Linksys. Using default SSIDs poses a security risk even if the AP is not broadcasting, because default names are widely known.

**Steganography:** A term introduced by the Greeks, which literally translates as "hidden writing." In conversations, you will often hear this abbreviated simply as "steg."

**Streaming Media:** Streaming media is multimedia that is constantly received by and presented to an end-user while being delivered by a streaming provider. Although virus attacks should be impossible with streaming media, denial of service attacks are a possible threat.

**STRIDE:** An acronym for the six threats to cyber security. These are: 1. Spoofing of user identity; 2. Tampering; 3. Repudiation; 4. Information disclosure; 5. Denial of Service (DoS); and 6. Elevation of privilege.

**Stuxnet Worm:** Stuxnet is a Windows computer worm discovered in July 2010 that targets industrial software and equipment. It is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit. Experts on Iran and computer security are convinced that Stuxnet was meant "to sabotage the uranium enrichment facility at Natanz where the centrifuge operational capacity has dropped over the past year by 30 percent."
Surface of Vulnerability: The vulnerability of people and places to environmental and social forces.

SYN Flood: A SYN flood is a form of Denial of Service attack in which an attacker sends a continuous succession of SYN requests to a target's system. This flooding causes servers to quit responding to requests to open new connections with clients, so no other users can connect to that server while it is under the effects of the SYN flood.

Tampering: Describes an intentional modification of products in a way that would make them harmful to the consumer. One countermeasure for tampering is to check the hash code for the download.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Titan Rain: A series of coordinated attacks on American computer systems since 2003, "most likely the result of Chinese military hackers attempting to gather information on US Systems." Titan Rain hackers gained access to many US computer networks, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA.

Top Level Domain (TLD): The names at the top of the Domain Name System (DNS) hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "net" in "www.example.net". The administrator for a TLD controls what second-level names are recognized in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognized by the DNS. Commonly used TLDs include .com, .net, .edu, .tv, .jp, .de, and others.

Traceroute: Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. Traceroute outputs the list of traversed routers in simple text format, together with timing information. On Microsoft Windows operating systems it is named Tracert.

Trojan Horse: A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

TTX: Abbreviation for Table Top Exercise.

User Datagram Protocol (UDP): A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to TCP, and, together with IP, is sometimes referred to as UDP/IP.

Vector: The method(s) that a virus, worm, or other malicious code use to propagate themselves or infect new computers. Common vectors include email, scripts, open network shares, and compromised websites.

View Source: A common technique to explore the source HTML of a web page for attack via SQL Injection methods.

Virtualization: The creation of a virtual (rather than actual) version of something, such as an operating system. If you are running Windows 7, you can use a virtualization software package like VMWare to run a version of the UNIX operating system.
**Virus**: A malicious, self-replicating program that runs and spreads by modifying other programs or files. Some viruses are a serious threat, deleting or deliberately changing files as they spread. Other viruses do something that appears harmless, such as playing music. Viruses are dangerous because they multiply, and can consume all available computer memory in an instant, causing a breakdown.

**Vishing**: A social engineering technique in which the attacker has the victim contact the attacker via a phone number (often using a VoIP connection), in order to lend a veneer of respectability and credibility to the scam.

**VoIP**: Voice over IP is a technology that allows you to make telephone calls using a high speed internet connection.

**War chalking**: War chalking is marking areas, usually on sidewalks with chalk, where wireless signals can be accessed.

**War dialing**: War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

**War driving**: War driving is the process of traveling around looking for wireless access point signals that can be used to get network access.

**WEP**: Wired Equivalent Privacy is a weak security algorithm for IEEE 802.11 wireless networks. Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favor of newer standards such as WPA2, an acronym for Wi-Fi Protected Access 2.

**White Hat**: A white hat is a hacker who leverages skills in computer and network security to benefit others. This could be by testing a client’s cyber defenses after receiving appropriate authorization. The white hat will inform the client of any weakness findings and might suggest countermeasures to address them, whereas the black hat will exploit the weaknesses he finds for personal benefit.

**WIGLE**: The Wireless Geographic Logging Engine makes maps of wireless networks.

**Windows Powershell**: Microsoft’s task automation framework. It consists of a command-line shell and associated scripting language built on top of, and integrated with the .NET Framework. PowerShell provides full access to COM and WMI. This tool enables administrators to perform administrative tasks on both local and remote Windows systems.

**Worm**: A self-replicating, self-propagating, and self-contained program that uses networking mechanisms to spread itself. Famous worms include Morris, Melissa, Code Red, Sobig, Stuxnet, and Daprosy.

**Zero-day threat**: A Zero-day virus is a previously-unknown computer virus or other malware for which specific antivirus software signatures are not yet available.

**Zeroization**: A practice of erasing keys or other sensitive data from a cryptographic system so as to prevent their disclosure in the case of capture. When encryption was performed by mechanical devices, all the machine’s settings would be changed to some fixed, meaningless value, such as zero.

**Zombie**: A program or infected computer commandeered to attack other machines on a network.

**Zombie Machine**: A computer that an attacker has taken control of using malware.
Appendix C: Toolbox of Promotional Resources

The biggest issue at this time is simply getting the news out that we have a serious problem.

Cyber Patriot IV Recruiting Poster
Patrol Your Security Perimeters
For more ideas, visit [http://www.selinc.com/cybersecurity/posters/University of California at Santa Cruz](http://www.selinc.com/cybersecurity/posters/University of California at Santa Cruz).

For more ideas, visit [http://its.ucsc.edu/security_awareness/posters.php](http://its.ucsc.edu/security_awareness/posters.php).

Go ahead and use whatever you find, OR create your own posters, and maybe add an encrypted message to see who among you is sufficiently skilled to crack it.
Articles of Interest to be Shared and Posted

Operation Shady RAT

McAfee’s White Paper on Operation Shady RAT

CyberWar: Sabotaging the System
http://www.cbsnews.com/video/watch/?id=6578069n

Warflighting in Cyber Space by GEN Keith B. Alexander

FBI Raid at Georgia Tech

Lockheed Martin HOW Cyber Security Video
http://www.youtube.com/watch?v=fhjFsWGcUm4

Hackers Take $1 Billion Per Year as Banks Blame Customers for Crime
Appendix D: Toolbox of Technical Resources

Cybersecurity Podcasts and VPodcasts
(If you wish to learn the advanced material via quality video presentations, this is the collection.)

  CyberSecurityVCast
  Security Now   also on TWiT Channel
  Imperva Channel
  Black Hat 2010: Hardening Windows Applications
  Animated Explanation of TCP/IP
  Network Security Podcast
  AFA's Cyber Patriot Channel

Cybersecurity Portals
  Wikipedia Portal on Computer Security
  NIST Computer Security
  US-CERT Tips
  Microsoft Malware Protection Center
  McAfee Security Advice Center
  USA Today Cybersecurity Education

Younger Audience Cybersecurity
  NSA Kids
  CIA Kids Page

Training Sites
  HackThisSite   with YouTube Video Solutions   and Wikipedia Site Description
  OSI School
  W3Schools

Encryption and Cryptology
  Rumkin Cipher Tools
  Cryptool Online
Software

GnuPG: A free software implementation of PGP, Pretty Good Privacy.

ZoneAlarm Pro

AVG Anti-virus

scanlogd a port scan detection tool
Appendix E. Solutions to Module Activities

It is never traditional, in this field of endeavor, to provide ready solutions to puzzle problems in a convenient place. As an example, no solution for Kryptos has been provided. In general, it is fairly obvious that you have a correct solution to a cipher when the plaintext you generate makes some logical sense or when you gain access via a password.

At this stage of training, however, some confirmation of your effort might encourage you to continue.

Activity 1.1: Solution to Caesar's Character Transposition Ciphers

The entire purpose of this exercise is to recall the Era of the Secret Decoder rings and demonstrate, that shift ciphers are easily broken and do not qualify as encryption.

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Hint</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAL bnlotsdqr deehbhdsksx rddj zmrvdqr.</td>
<td>rot-1</td>
<td>IBM computers efficiently seek answers.</td>
</tr>
</tbody>
</table>

In this case, there were two hints. The obvious “hint” indicated that the ciphertext would be generated by simply backing up (-1) one letter for each letter in the plaintext. The reference to HAL is another hint from the film 2001: A Space Odyssey. Most of us would rather not decode any of these by hand. Readers on their game will search online for RotN decoders and leverage computers and java code to do the work quickly.

```
tyvqref jvyy qrcneg ng qnja gb qryvire grnz puneyvr enatref gb gur evire oevqtr. | rot13 | Gliders will depart at dawn to deliver team charlie rangers to the river bridge. |
```

In this problem, each ciphertext letter was to be advanced forward 13 characters. The plaintext message honors General “Hap” Arnold who created the American Glider Program on 25 February 1941. The Waco CG-4A glider went into operation in July 1943 during the Allied Invasion of Sicily and on 6 June 1944 for the Invasion of Normandy.

```
tpiewi hvmro qsvi Szepxmri. None please drink more Ovaltine. |
```

In this case, no hint was provided. We do know, however, that the letter “e” is the most commonly used letter in the English language. So, our options without a computer are to create a histogram of letter counts. For each letter present, we count the number of times it is repeated. A:0 B:0 I:4 M:2 S:2 V:2 The letter “i” is most frequent and thus might represent the letter e. The letter “e” is 4 characters backward from the letter “i” or 22 characters forward. Thus Rot-4 and Rot22 result in the same shift. The plaintext is a reference to the Little Orphan Annie Secret Decoder Ring, comically presented in the 1983 movie “A Christmas Story.”

```
ahuahv ghduwhg vdulg zlw k Iohw dqg wkluwb-wkrxvdqg kruvhphq. | None | xerxes departed sardis with a fleet and thirty-thousand horsemen. |
```

The plaintext phrase is derived in the same way as the others, and commemorates the coded message that was sent to Greece to warn of the attack.
Activity 1.2: Solution to President Jefferson’s Cipher Problems

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Keyphrase</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>efnbkebfjdwulytdswnmxfbw&amp;fxkp</td>
<td>aerospace</td>
<td>dawnspacecraftisarrivingatvesta</td>
</tr>
</tbody>
</table>

Place the keyphrase on top of the ciphertext, repeating its characters as often as required to have a pair of letters for entry into Jefferson’s handwritten table. Use the top letter to enter the table at the top row and move down to the ciphertext letter in the table, move outward to the leftmost column to find the plaintext character. Note our use of the **courier font** to allow the characters to line up. This is a key tactic in playing with ciphers.

\[
\text{aerospaceaerospaceaerospaceaero} \\
\text{efnbkebfjdwulytdswnmxfbw&fxkp} \\
\text{dawnspacecraftisarrivingatvesta}
\]

Note that this cipher prevents the frequency of the letter “e” from being used to break the encryption.

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Keyphrase</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>ojnvjjnpfokifrjuibnirjqgwmnumwg</td>
<td>aerospace</td>
<td>newgrummanfirebirdaircraftflies</td>
</tr>
<tr>
<td>tjdxdgjlljqsbyptuyfuggqdysefnf</td>
<td>aerospace</td>
<td>sempervigilansismottoforpatriot</td>
</tr>
</tbody>
</table>

Activity 1.3: Location of the Kryptos Sculpture

A little digging should reveal the coordinates for this structure to be N38° 57′ 8.12", W77° 8′ 44.78" or 38.952255, -77.145773 or as UTM 18S 314060 4313668.

Activity 1.4: More Codes and Ciphers

**Code:** When words or phrases have specific meanings, this is a code and not a cipher.

codetext: Climb Mount Nitaka.
plaintext: Commence aerial attack on Pearl Harbor.

**Baconian:** A complex form of steganography or hidden writing in which two fonts are used.

ciphertext: I eXTEnd My haNd In wElComE To You
plaintext: hello (You’ll have to research this for yourself.)

**Railfence:** When you rearrange your text in a “wave” sort of pattern (down, down, up, up, down, down, etc.), it is called a railfence.

ciphertext: caeinepeeoootcgogafrzvlwntwdoiet
plaintext: find railfence decoder online and advise

Activity 5.0: Solutions to End of Module Exam