CIVIL AIR PATROL

AEROSPACE EDUCATION

Introduction to Cybersecurity

INTRODUCTION

LEGACY CONTENT

Please be advised that this book is part of our original curriculum catalog.

- **Status**: This book has been moved to the new platform, Absorb, and has had all links updated, but has not yet undergone formal content revision.

- **Context**: While the core pedagogy remains sound, you may notice older formatting, standards, or references consistent with the most recent publication date (2019).

CONTRIBUTORS

First Edition: MAJ THOMAS A. OWENS, CAP

Editing:
- SUSAN MALLETT, CAP NHQ
- DR. JEFF MONTGOMERY, CAP NHQ

2019 Revision: MAJ DEREK RUSTVOLD, CAP DIRECTOR OF CYBER PROGRAMS, MAR

MODULE PURPOSE

This module provides an essential introduction to the evolving threats of cyberspace and offers practical activities to strengthen our collective digital defense. As technology integrates into every aspect of society, understanding cybersecurity is no longer just a technical skill, it is a necessity for every citizen. Developed by the Civil Air Patrol, this module is an educational resource designed to empower our members. By mastering these concepts, you will understand the real-world implications of cyber warfare and help build a more secure digital future for our communities and the nation. This module includes:

- The Cyber Landscape: An overview of modern threats and how to defend against them.
- Career Impact: Insight into the diverse world of cybersecurity careers and how they protect every major global industry.
- CyberPatriot Readiness: A technical primer for members preparing to compete in the National Youth Cyber Education Program, sponsored by the Air Force Association.

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 that the prefix "cyber-" is derived from the word *cybernetic*, which comes from a Greek word meaning pilot, rudder, steersman, or governor. Some early cybernetic applications will be reviewed in the **C**hronology 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 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, including capturing aircraft performance and avionics data.

Cybersecurity

Cybersecurity is the professional practice of identifying vulnerabilities and countering threats to the exploitation or disruption of computers, smartphones, 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.

WORD TO KNOW: PHISHING

By masquerading as a reputable source with an urgent or enticing request, an attacker lures the victim into giving sensitive information (usernames, passwords), similar to using bait to catch a fish.

MOTIVATION FOR ACTION

Government Attacks

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 released 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 offline 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.

WORD TO KNOW: CYBER ESPIONAGE

A type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage, or political reasons.

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 were traced to Jian, PRC. The People's Republic of China denied any involvement.

Business Attacks

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 it 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 April of 2011, Sony's PlayStation network was hacked, and user account information, including 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 hacked, 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 ... "

WORD TO KNOW: SPEAR-PHISHING

A highly targeted, personalized cyberattack that uses researched information to trick specific individuals or organizations into revealing sensitive data, clicking malicious links, or downloading malware.

On 1 August 2011, the arrested teenager was released on bail, and soon after, anonymous hackers penetrated the 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.

The year 2014 included a series of high-impact data breaches, including Sony Pictures, Apple iCloud, Heartbleed vulnerability and Cryptolocker ransomware. The Sony Pictures breach was potentially attributed to North Korea for political retaliation. The same year, several famous people had private photos exposed in the Apple iCloud security breach. Another high-profile security incident was the Heartbleed vulnerability associated with OpenSSL, an open source implementation of SSL and TLS protocols widely used for HTTPS, allowing data, including credentials, financial details, and personal information to be observed. Cryptolocker was a ransomware attack, encrypting data and requiring a sum of money from the victim for the decryption key. A rise in CryptoLocker variants, including Cryptowall, CryptoLocker V2, Cryptodefense, and ZeroLocker, with similar behavior, occurred and aimed at financial interests.

In June 2015, 21-25 million federal workers' records stored with the Office of Personnel Management (OPM) were disclosed. Besides Social Security Numbers and other sensitive information impacted by the breach, an estimated 5.6 million fingerprints were stolen. The concern of unique biometric data, such as fingerprints, being exposed is because those are unable to be changed. The OPM Office of the Inspector General (OIG) determined OPM failed to have an accurate inventory of hardware and software. Furthermore, the agency was unable to demonstrate a vulnerability scanning program, nor was multi-factor authentication required to access OPM systems.

In October 2016, hackers stole the personal information of approximately 57 million Uber riders and drivers in a mega data breach that occurred. Uber paid $100,000 to prevent the news from being disclosed and keep the information safe. Email addresses, phone numbers, and names belonging to riders and drivers, and some drivers' license numbers, were stolen as well. EternalBlue was leaked by the Shadow Brokers hacker group in April 2017, and was a component of the global WannaCry ransomware attack a month later. Following attacks such as NotPetya and Retefe banking trojan are believed to be related to the leak. Anti-Virus was unable to prevent the attack because it resides in memory instead of in a file.

Another catastrophic breach in 2017 was the Equifax disclosure, including 143 million customers, attributed to a vulnerability discovered in open source software. Full names, birth dates, Social Security numbers, and addresses were released in addition to approximately 200,000 credit card numbers and almost 200,000 other confidential documents containing PII. 2018 included some of the most noteworthy exposrues and data breaches in history. It was revealed that Facebook was selling information about its users, and Marriott Hotel demonstrated that security breaches can remain hidden for years before discovery.

The trend continued in 2019 when Capital One was breached resulted in the exposure of more than 100 million customers' information, including credit history, credit card limits, credit scores, balances, bank account numbers, home addresses, and Social Security numbers. First American Financial, a leading settlement and insurance provider, exposed 800 million records due to a flaw in the database design that existed for almost sixteen years. The public-facing website revealed private mortgage information, bank account numbers, tax records, and Social Security numbers.

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.

Intrusion Groups

Adversary tactics and techniques are based on observed behaviors aimed at the private sector, government, and cybersecurity product and service providers, which are organized into Intrusion Groups. MITRE ATT&CK is a knowledge base of attack characteristics, improving communication, and improving cybersecurity, including:

- Initial Access attempts to get on the network.
- Execution of malicious programs.
- Persistence by maintaining a foothold on the network.
- Privilege Escalation to gain higher-level permissions on systems.
- Defense Evasion to avoid detection.
- Credential Access steals user names and passwords.
- Discovery of the network and systems by the adversary.
- Lateral Movement through the network and systems.
- Collection of private information and data in the environment.
- Command and Control communication with malicious programs on the network.
- Exfiltration to steal private information and data.
- Impact of attempts to manipulate, interrupt, and destroy systems and information.

INTRODUCTION TO CRYPTOGRAPHY

Ciphers have been used throughout history for confidentiality with encryption and decryption. Two kinds of cryptosystems are used: symmetric systems use the same key as a shared secret to encrypt and decrypt information. Asymmetric systems use public that is shared and private key. Also called Public-Private Key encryption, this enables both confidentiality with encryption and authentication for the private key holder.

Activity 1: Codes, Ciphers and Encryption Awareness

OBJECTIVE

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

Pencil and paper (ideally graph paper).
Optional: A computer with a simple text editor set in a Courier font.
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.

Directions: 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.

Plaintext	Hint	Ciphertext
	rot-1	HAL Bnlotsdqr deehbdmskx rddj zmrvdqr.
	rot13	Tyvqref jvyy qrcneg ng qnja gb qryvire grnz puneyvr enatref gb gur evire oevqtr.
		Tpiewi hvmro qsvi Szepxmri.
		ahuahv ghsduwhg vduglv zlwk d iohhw dqg wkluwb-wkrxvdqg kruvhphq

If you are having trouble, remember that the letter "e" has the 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. Let's say the letter G had a high frequency in the cipher, and the language was expected to be English.

G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

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.

A B C D G H I J K L M N O P Q R S T U V W X Y Z A B
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

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 encription. Consider the following questions:

- Can you find an online computer program to count the letters (or characters) of any ciphertext?
- How might you use such a program?
- Can you recall (or find) any substitution ciphers used throughout history, business or fiction?
- Can you suggest any methods to overcome the limitations of substitution ciphers?

Activity 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

Pencil and paper (ideally graph paper).
Optional: A printout of President Jefferson's mapping matrix on the next page.
Optional: A 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
```

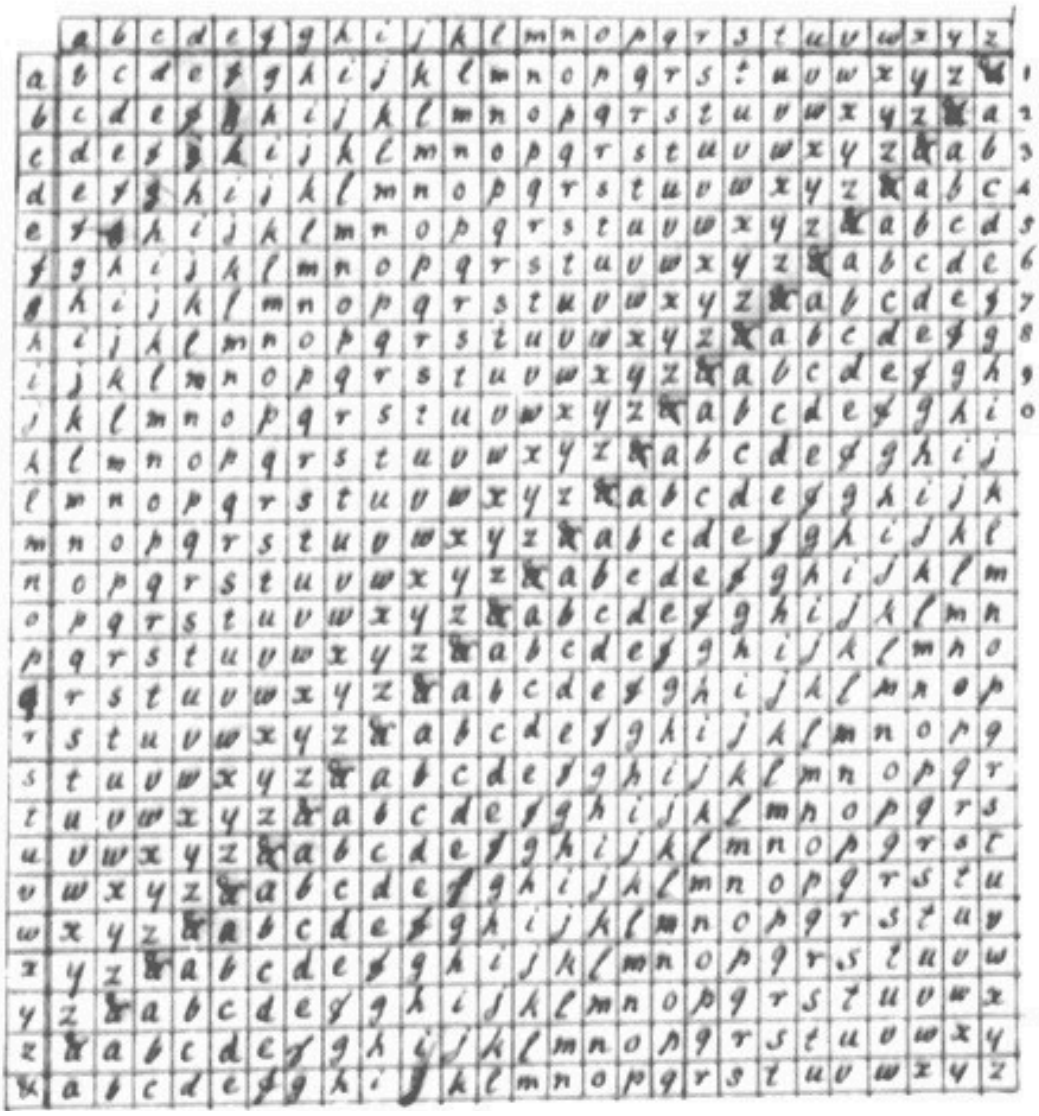
This cipher is based upon the Vigenère Cipher, which was widely used in Europe and considered unbreakable until the mid to late 1800s. Thomas Jefferson was a legendary US president who sought to raise the level of education for all Americans. We highly recommend a visit to Monticello in person or online, 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.

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. **efnbkebfjdwsulytdwsnmxfwbw&fxkp**
2. **ojnvjjnpfokifxrjuibnirjqgwkmnwg**
3. **tjddxgwlljqsbkytptuyfuggqdysnfh**
4. **dtehtsujfklvpxvpuusnqtduwhqpsw**

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.

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.



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.

Consider the following questions:

- Is there any evidence that Lewis humored Jefferson with an encrypted report from the field?
- Would the encryption be secure if a Wing AEO selected "aerospace" as a key? Why or why not?
- What would be the best way to generate an encryption key?
- Would you need a computer to generate an encryption key in this way? If so, why?
- In 1883, Auguste Kerckhoff proposed six design principles for military ciphers. What are they?
- Which "father of the computer" is first known to have broken a variant of the Vigenere Cipher?

Activity 3: The Kryptos Sculpture

OBJECTIVE

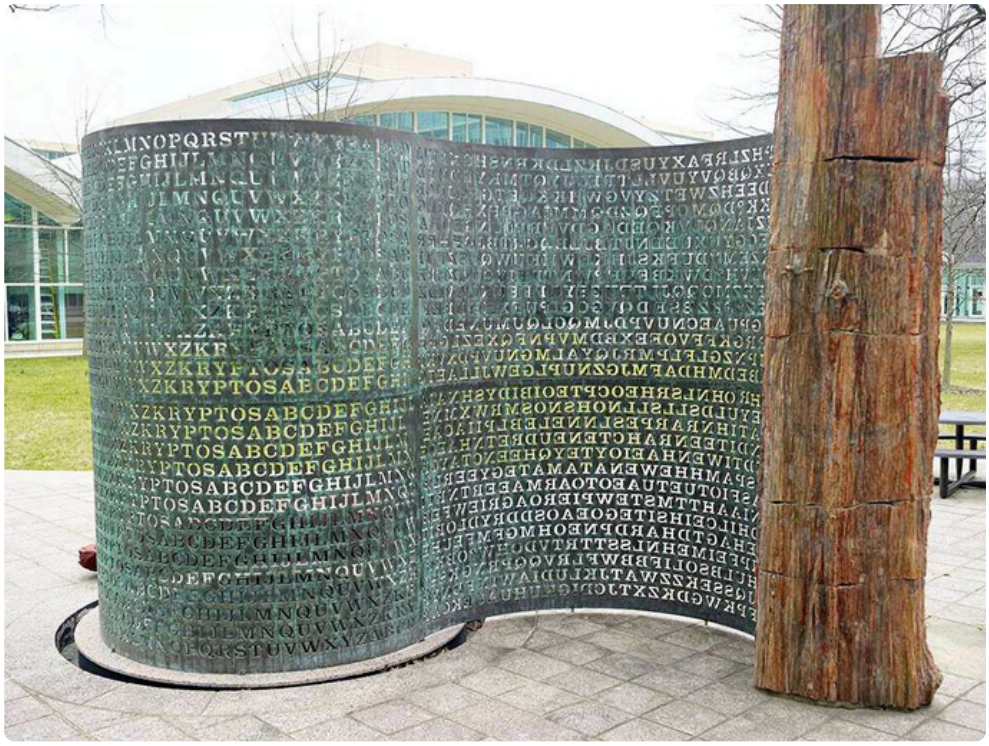
The objective of this activity is to introduce students to the challenge presented by Jim Sanborn's Kryptos sculpture and to use it as a motivational tool for recruiting and learning. In the real world, solutions to puzzles will not be provided in the back of a textbook. The clock ticks, waiting for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

MATERIALS

Computer with internet access, printer, and paper, and permission from the school principal or squadron commander to post approved images.

MISSION BRIEFING

Look up images of Jim Sanborn's Kryptos sculpture, located on the campus of the CIA headquarters in Langley, VA. Post an 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**.



1. Using online tools, find the Latitude and Longitude of Kryptos
2. Research and list online communities and groups working to complete the decryption process.
3. Research the cryptographer who instructed Mr. Sanborn in various methods of encryption.
4. 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.

Consider the following questions:

- How long did it take to break any one of the four sections?
- Who was the first person to publicly announce solving the first three sections?
- Name the analyst who likely first solved the three sections, but made no public announcement.
- Are there any other sculptures of this nature? If so, where are they?

Activity 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

Computer with internet access, and paper and pencil to write definitions and work through additional messages.

MISSION BRIEFING

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

Method	Method Definition	Codetext	Plaintext
CODE		Climb Mount Nitaka.	
MORSE		.-- .... .- - / .... .- - .... / --. --- -.. / .-- .-. --- ..- - -. .... - ..--..	
BACONIAN		IeXTEnd My haNd In wElComE To You	
RAILFENCE		caeinepeeootcgog aigafrrzlvlwntrwdo iet	
BFID		EesphO Promgt 9/Bkmvna ve bvwnqa nt Vwchderb	

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.

Consider the following questions:

- Name a trulyAmerican code used during World War II that used a non-English language.
- What were some of the code phrases broadcast prior to the Invasion of Normandy?
- What is the main advantage of Baconian Ciphertext?
- What is the cost paid for this advantage?

Activity 5: PGP Pretty Good Privacy and Gpg4win Software

OBJECTIVE

The purpose of this optional advanced activity is to demonstrate how students may use modern asymmetric encryption software (public and private keys) to secure the privacy of their documents and email messages. We also introduce the concept of a hash algorithm and a checksum 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

Computer with internet access, and a hard drive with sufficient space for a 40MB download.

MISSION BRIEFING

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 a while, 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 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.

UNIT PROFILE: ROOM 40 AND BLETCHLEY PARK

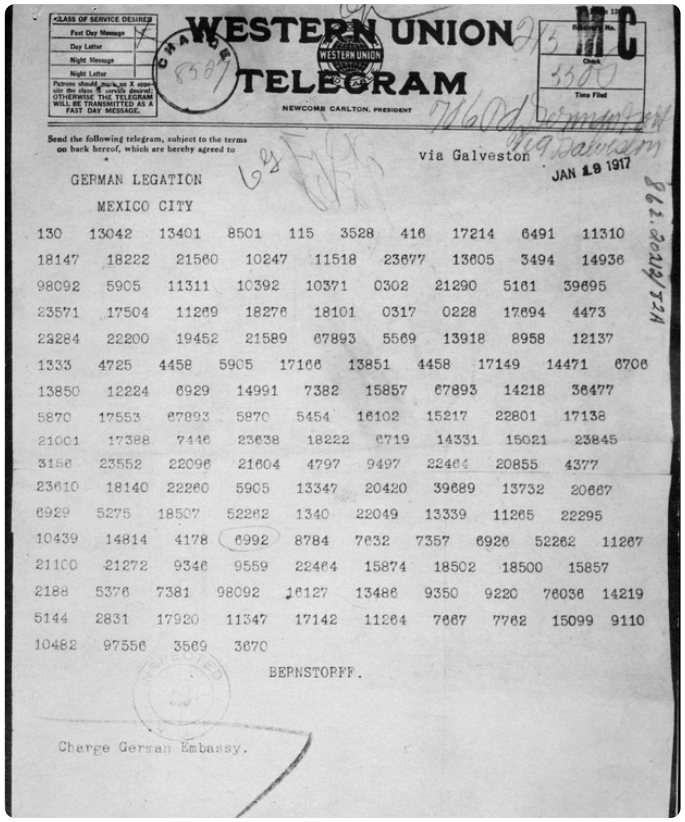
Room 40

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 (below), 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. The Russian capture of the German cruiser Magdeburg 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.



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM
NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

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.

DIGITAL EXTENSION

Learn more about the impact of Bletchley Park.
https://www.bletchleypark.org.uk/our-story/low-level-codes-and-ciphers/

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.

YOUTUBE VIDEO

Alan Turing | A Genius With A Complex Personal Life
https://youtu.be/MidJR581irA

INFORMATION ASSURANCE

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.

Summary of Threats, Attacks, and Motivation for CAP Action

Common Internet Threats include Malware, Phishing, Ransomware, Scams, and Fraud. Malicious Software is commonly referred to as Malware and describes software written to steal information, spy on users, and gain control of computers. Those are categorized by how they spread and what it does. Some categories are: Viruses/Worms, Trojan Horses, Zombies and Botnets, Keyloggers, Backdoors, Logic/Time Bombs, and Spyware. These threats and attacks continue to grow. As dependence on the Internet grows for commerce and all aspects of our daily lives. Cyber is frequently referred to as the 5th Domain after land, sea, air, and space. In the same way, systems operating in those other domains increasingly rely on cyber. As a leader in Aerospace Education, Civil Air Patrol must also include Cyber as aircraft, and spacecraft, that depend more and more on computer systems integrated into command, control, and navigation.

Summary of Threats, Attacks, and Motivation for CAP Action

Common Internet Threats include Malware, Phishing, Ransomware, Scams, and Fraud. Malicious Software is commonly referred to as Malware and describes software written to steal information, spy on users, and gain control of computers. Those are categorized by how they spread and what it does. Some categories are: Viruses/Worms, Trojan Horses, Zombies and Botnets, Keyloggers, Backdoors, Logic/Time Bombs, and Spyware. These threats and attacks continue to grow. As dependence on the Internet grows for commerce and all aspects of our daily lives. Cyber is frequently referred to as the 5th Domain after land, sea, air, and space. In the same way, systems operating in those other domains increasingly rely on cyber. As a leader in Aerospace Education, Civil Air Patrol must also include Cyber as aircraft, and spacecraft, that depend more and more on computer systems integrated into command, control, and navigation.

Social Media Safety, Privacy, and Web Browsing Best Practices

Cybersecurity begins with social media safety and privacy. These simple guidelines are tremendous aids to protecting yourself on the Internet.

- Only Accept or Follow People You've Met in Person
- Never Share or Post Your Location (Including App Geo-Tracking)
- Assume Your Digital Footprint is Permanent When Sharing
- Customize and Harden Security Settings
- Never Share Personally Identifiable Information (PII)
- Always Log Out When Finished

ACRONYM TO KNOW: PII

PII (Personally Identifiable Information) includes data that can identify a person, such as a social security number, student ID number, birthplace, birth date, or passwords.

Other best practices include:

- Using automatic updates.
- Using and regularly updating built-in safety features such as anti-virus, anti-phishing, pop-up blockers, and anti-spyware
- Using a third-party web browser such as Google Chrome, because Internet Explorer and other built-in web browsers are more frequently targeted and have more security flaws than third-party browsers.
- Chatting only with trusted, verified individuals to troubleshoot web, app, or other device issues.
- Assuming everything can be made public, via direct-sharing or through posted screenshots or recordings.
- Not using the “Save Password” or “Remember Me” functions, as those can be replayed when the browser is exploited.

The CIA-Triad and Five Pillars of Information Assurance

The CIA-Triad is a foundational cybersecurity model ensuring data privacy, accuracy, and accessibility. The Department of Defense (DoD) 5 Pillars of Information Assurance (IA) expand on this to include Authentication and Non-repudiation, ensuring authorized access and accountability in protecting information systems.

Confidentiality

Confidentiality ensures that sensitive information such as troop movements, aircraft designs, or encryption keys is accessible only to those with authorized clearance. The value of data is often tied directly to its secrecy; if an adversary intercepts a flight plan, the mission is compromised.

Integrity

Integrity ensures that information remains accurate, complete, and unaltered throughout its entire life cycle. If data is "adulterated" by unauthorized changes, false rumors, or "red herrings," it becomes unreliable. A pilot must trust that the coordinates in the navigation system are exactly what the dispatcher entered.

Availability

Availability ensures that authorized users have reliable and timely access to data and resources. An adversary doesn't need to steal your secrets to defeat you; if they can deny you access to your own radar data or communication links through a "denial-of-service," they have effectively neutralized your advantage.

Authentication

Authentication is the process of verifying the identity of a user, device, or system. In a secure network, it isn't enough to have the right password; we must prove that the person entering the network is exactly who they claim to be.

Non-Repudiation

Non-repudiation provides proof of the origin and delivery of data so that the sender cannot later deny having sent it, and the recipient cannot deny having received it. Think of it as a certified logbook: it creates an undeniable trail of accountability for every action taken within the system.

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 Organization extends the definition of cyberwar to include the 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, including:

1. Spoofing of user identity
2. Tampering
3. Repudiation
4. Information disclosure
5. Denial of Service (DoS)
6. Elevation of privilege

Countermeasures are procedures and devices that 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 countermeasures include: two-stage authentication, firewalls, and storage ofvital 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.

WORD TO KNOW: TWO-FACTOR AUTHORIZATION (2FA)

A secondary layer of security requiring both a known credential (password) and a physical verification (code or notification) to grant access, adding a critical layer of security against unauthorized access.

CYBER SITUATIONAL AWARENESS

"He who can handle the quickest rate of change survives." -Lt. Colonel John Boyd

John Boyd was a fighter pilot and military strategist responsible for developing an idea to achieve success in air-to-air combat. During the Korean Conflict, he observed air combat between North American F-86 Sabers and MiG-15s. John Boyd concluded "time is the dominant parameter," and the pilot most effective at completing the cycle beginning with observing and ending with action will win. He called this the OODA Loop:

1. Observe the collection of information provided by our senses.
2. Orient with the analysis of information to form the most correct perspective of the situation.
3. Decide the best course of action based on that perspective.
4. Act by performing the decision.

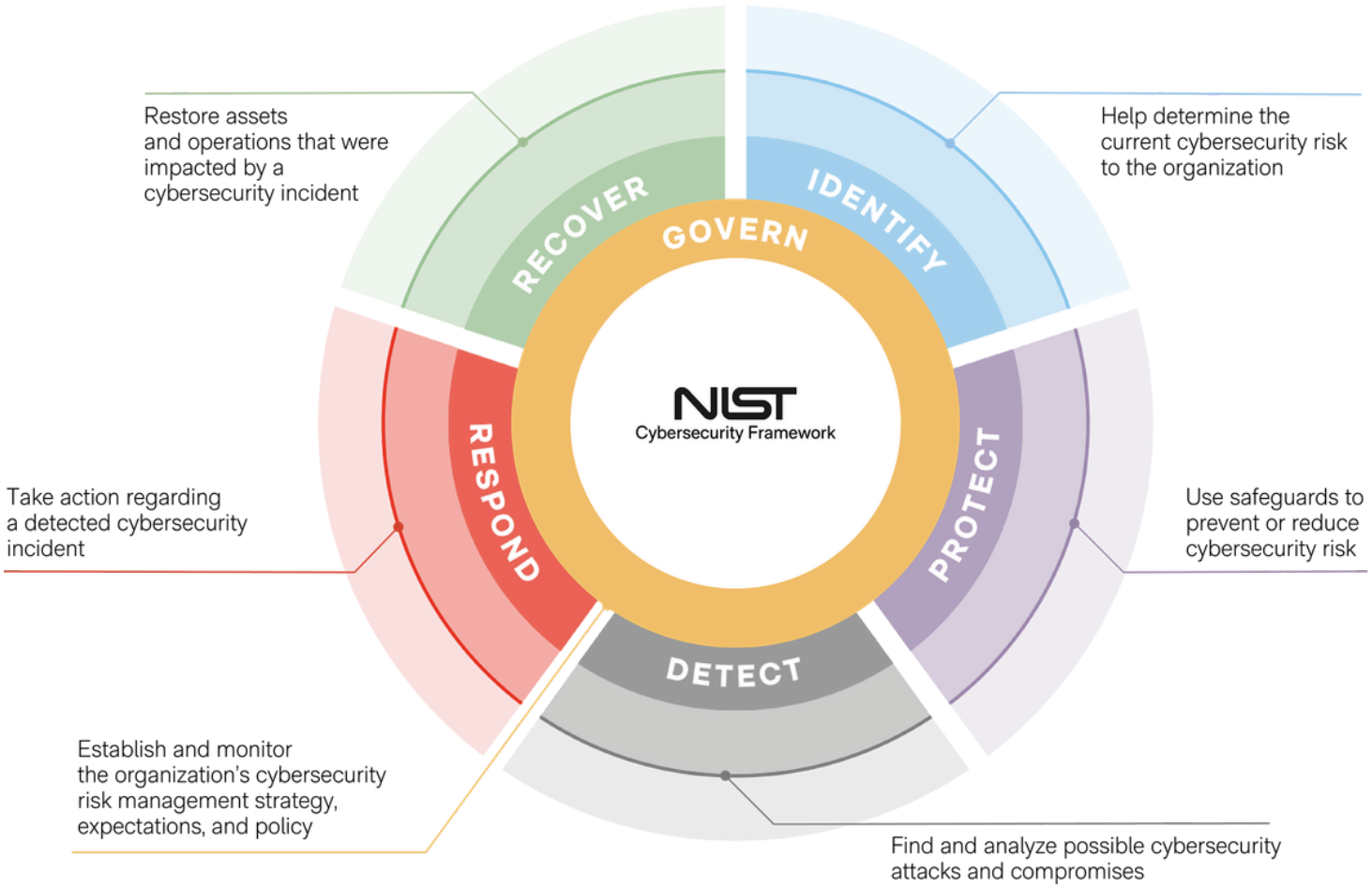
In the same way, cybersecurity requires being aware, understanding, and taking action. This is organized into Network Awareness, Threat Awareness, and Mission Awareness. All three areas must be observed to orient, decide, and effectively act.

Network Awareness includes discipline, hardware, and software inventory with correct configuration management. Running scheduled vulnerability scanning and auditing is used to identify potential areas of exploitation. Patch management and compliance reporting to measure and track risk, and plans to identify incidents for awareness throughout the organization.

Threat Awareness aims to monitor, identify, and track suspicious internal activities for potential security incidents. It requires being knowledgeable of external threats and often includes participating in community sharing of potential indicators of system compromise.

Mission Awareness defines a complete understanding of inter-dependencies and systems used to operate on the Internet. Assessing mission-impact for defense planning, risk and readiness assessments, incident response, triage, and forensic analysis to recover and learn from an incident.

The National Institute of Standards and Technology (NIST) published the Cybersecurity Framework with the goal of improving critical infrastructure cybersecurity. It includes Identify, Protect, Detect, Respond, and Recover from incidents (see next page).



Cyber Kill Chain

The Cyber Kill Chain, developed by Lockheed Martin, identifies all the steps an adversary must complete to be successful. Disrupting any link in the chain will neutralize the attacker. The seven links in the chain are:

1. Reconnaissance collecting publicly available information from websites and gathering emails.
2. Weaponization of information gathered during reconnaissance to combine an exploit with malware.
3. Delivery of the weaponized software through email, web, USB to the victim.
4. Exploitation by executing the weaponized software after delivery.
5. Installation of malware on the compromised system.
6. Command & Control (C2) with the malware to manipulate the compromised systems.
7. Actions on Objectives to accomplish intended goals such as exfiltration or ransomware.

Ethics

Ethics intends to promote a sense of fairness by creating rules of acceptable behavior and practices to help identify what is also unacceptable. A Code of Ethics aims to protect society, the common good, trust, and confidence by acting honorably, honestly, just, responsibly, and lawfully.

Behaving ethically is not always easy, but it is necessary. Often, courage is needed to see and say something, be willing to go against friends and peers, and stand up to bullies. Humility can also be required to admit when making a wrong decision and correct a mistake.

Do Not

- Do not use a computer to harm other people.
- Do not interfere with other people's computer work.
- Do not snoop around in other people's computer files.
- Do not use a computer to steal.
- Do not use a computer to bear false witness.
- Do not copy or use proprietary software for which you have not paid.
- Do not use other people's computer resources without authorization or proper compensation.
- Do not steal other people's intellectual property.

Do

- Do think about the social consequences of the program you are writing or the system you are designing.
- Do always use a computer in ways that ensure consideration and respect for your fellow humans.

Activity 1: Vulnerabilities and Basic Defense Skills

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

Computer with internet access.

MISSION BRIEFING

Weak passwords are one of the biggest vulnerabilities to protecting our systems through user authentication. Passwords such as birthdays, airplane names, or favorite sports 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. She found students using the passwords in the table below. Your assignment is to rate these passwords as weak, good, or strong. Then, input each password into the **password checker tool** for the system rating of the password and how long it would take to "crack" that password.

Password	Your Rating	System Rating	Estimated Time to "Crack"
&cat65Whz			
BlueKnight7			
7041992			
Mary$321			
$6gK3m5o#			

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 "0i2rlyr3g."

Make it Long

Longer passwords are stronger passwords. Consider using a passphrase. A passphrase is a type of password made up of 4 or more random words. They're tricky for cybercriminals to crack, but easy for you to remember.

Make it Unpredictable

The best passwords aren't predictable in any way. Avoid using patterns as they are easier for a person or password-guessing programs to figure out. Keep cybercriminals guessing by avoiding passwords with personal information, predictable substitutions (e.g., $ instead of S), and common references.

Make it Unique

Don't use the same password across multiple accounts. If one service suffers a data breach, then that puts any account with the same password at risk.

Conclusion: You can see from the scores generated that the minimum requirements for a password are that it be at least 8 characters in length and contain at least 3 of the following items: uppercase, lowercase, numbers, and symbols. Additional credit is given for the 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:

- Explain the trade-off between having a password that is easy to remember and having one that is difficult to crack.
- Brainstorm some additional strategies to generate a complex password that you can remember, but that also scores well on the meter.

Activity 2: Two-Stage Authentication

OBJECTIVE

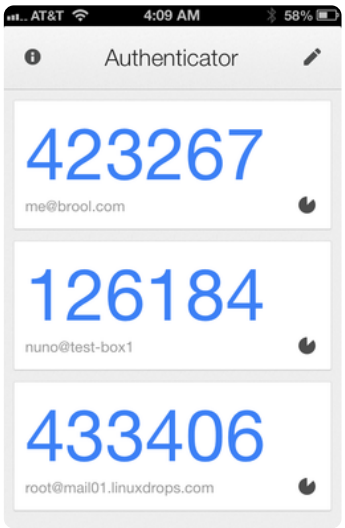
The objective of this activity is to allow the student to experience how professionals in DoD installations and subcontractors might be two-stage authenticated to gain access to critical or top-secret information. The technology emulates the RSA SecureID device with the modern smartphone that some may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

MATERIALS

Computer with internet access, a Gmail account, a smartphone that can run the Google Authentication App.

MISSION BRIEFING

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. Google has implemented a version of Two- Step Verification using Gmail and the user's cellphone. Follow the steps below:



1. Sign in to your Gmail account and choose My Account.
2. In the Personal Settings – Security Group,
3. Choose Using 2-step verification
4. Follow the directions so that you will be sent a code by whatever device you have available.

Conclusion: The installation process for this tool is not too difficult to work through. If you configure an icon on your handheld 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 teammates over electronic channels. You wouldn't want your account hacked during this competition period.

Questions for further consideration:

- Do you believe the second step is worth the effort? Why or why not?

Activity 3: 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

Cybersecurity Audit Checklist, computer with internet access, clipboard, pencil.

MISSION BRIEFING

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 on the next page.

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 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:

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

CIVIL AIR PATROL
AEROSPACE EDUCATION

CYBERSECURITY AUDIT CHECKLIST

VulClass	Vulnerability Description	List Findings and Location (Home, Squadron, School)
Physical	Lab walls are susceptible to penetration	
Physical	Unguarded/unmonitored access to lab	
Physical	Unlocked doors or windows	
Software	OS/SW lacks current updates/patches	
Software	High-risk domains not filtered/blocked.	
Software	No user authentication required.	
Software	Poorly written software installed: scripting, buffer overflows, crashes	
Software	Deliberate holes: vendor backdoors, spyware/keyloggers, trojan horses	
Network	Unencrypted network protocols	
Network	The wireless network reaches the parking lot and/or evidence of war-chalking	
Network	Connections to multiple networks	
Comms	Unnecessary protocols allowed	
Comms	No filtering between network segments	
Human	Poorly defined procedures: No Incident Response Plan, violations not logged.	
Human	Stolen credentials	

UNIT PROFILE: 688TH INFORMATION OPERATIONS WING

The 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 redesignated 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 redesignated 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: LT. GEN. ROBERT J. SKINNER

Lt. Gen. Robert J. Skinner is the Director of the Defense Information Systems Agency and the Commander of the Joint Force Headquarters- Department of Defense Information Network, Fort George G. Meade, Maryland.

As Director of the Defense Information Systems Agency, Lt. Gen. Skinner manages a global network and leads nearly 19,000 service members, civilians, and contractors who plan, develop, deliver, and operate joint, interoperable command and control capabilities and defend an enterprise infrastructure in more than 42 countries. This mission directly supports the President, Secretary of Defense, Joint Chiefs of Staff, combatant commanders, U.S. Department of Defense components, and other mission partners across the spectrum of competition, combat, and combat support operations.

As Commander of Joint Force Headquarters-Department of Defense Information Network, he is charged with leading unified action across DoD to secure, operate, and defend the DoDIN. He leads the establishment of DoDIN priorities and directs threat-informed actions through formal planning and future operational initiatives, as well as the command and control of daily unified network operations, cybersecurity actions, and defensive operations on the DoDIN.

Lt. Gen. Skinner was commissioned through Officer Training School (second-honor graduate) in 1989. He has served in various tactical and fixed communications assignments, plans, policy, and resource staff work. He has commanded at the squadron, group, wing, and Numbered Air Force levels and served on the staffs at a NAF, major command headquarters, Headquarters Air Force, and the Joint Staff. Before assuming his current position, Lt. Gen. Skinner was the Director of Command, Control, Communications, and Cyber at U.S. Indo-Pacific Command, Camp H.M. Smith, Hawaii.

Biography Source: USAF
https://www.af.mil/About-Us/Biographies/Display/Article/467179/robert-j-skinner/

CONCEPTS OF OPERATING SYSTEMS AND NETWORKING

Overview of Operating System Functions

An Operating System (OS) is the system software that acts as an intermediary between computer hardware and the user. It manages the computer's resources and provides a platform for application software to run.
Primary Functions of an OS

- **Resource Management**: The OS manages the Central Processing Unit (CPU). It uses "scheduling" to determine which applications receive processing power and for how long, ensuring the system remains responsive.

- **Memory Management:** It tracks every byte of Random Access Memory (RAM). The OS allocates memory to specific programs when they start and "deallocates" (reclaims) that memory when the program closes to prevent system slowdowns.

- **Storage and File Management**: The OS maintains a File System (like NTFS or APFS). It controls how data is organized, stored, and retrieved on hard drives or SSDs, including managing file permissions and directory structures.

- **Hardware Abstraction (Device Management**): The OS uses drivers to communicate with hardware peripherals (printers, keyboards, GPUs). This allows software developers to write one version of a program that works across many different hardware brands.

- **User Interface (UI)**: It provides the environment for human interaction, whether through a Graphical User Interface (GUI) using icons and windows or a Command Line Interface (CLI) using text-based input.

- **Security and Access Control**: The OS enforces authentication (logins) and authorization (permissions). It ensures that users and applications can only access the files and memory sectors they are permitted to use.

Disk Operating System

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 on a computer's hard drive. They may also close access to USB ports. Hackers and crackers must therefore resort to lesser-known command-line operations 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, including 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 Cyber Patriot. Other popular distributions include openSUSE, Debian GNU/Linux, Ubuntu, CentOS, and RedHat.

Virtualization

Hardware and platform virtualization has enabled the computing resources to be like a physical computer and operating system, inside a host machine, with software enabling the sharing of physical resources. Several virtualization options exist, including VMWare, Hyper-V, VirtualBox, and Parallels.

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 or Mac OS can download and install VMWare, along with the Fedora image, so that they may experiment with the Linux operating system and perform certain activities of the Cyber Patriot modules.

Cloud Computing

Cloud Computing emerged with the growth of the Internet to provide on-demand computer resources for infrastructure, platforms, and software. Generally, these existed in large data centers with multiple locations to provide services for as many people as possible. There are generally accepted to be three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

IaaS is the virtual or physical hardware foundation, including servers, storage, load balancers, and networking switches and routers. PaaS includes the web servers, databases, and database tools hosted on IaaS. SaaS encompasses applications such as search engines, web email, word processing, and social media.

Web Applications

Web Applications, or Web Apps, are part of a client-server program constructed using a variety of technologies such as PHP, ASP.NET, Java, and JavaScript. The **Open Web Application Security Project** (OWASP) is a non-profit charity devoted to improving web application security. It lists the Top Ten Most Critical Web Application Security Risks annually. The 2025 list showcased the following:

1. A01:2025 - Broken Access Control
2. A02:2025 - Security Misconfiguration
3. A03:2025 - Software Supply Chain Failures
4. A04:2025 - Cryptographic Failures
5. A05:2025 - Injection
6. A06:2025 - Insecure Design
7. A07:2025 - Authentication Failures
8. A08:2025 - Software or Data Integrity Failures
9. A09:2025 - Security Logging and Alerting Failures
10. A10:2025 - Mishandling of Exceptional Conditions

Web application architects and authors are encouraged to design their application to avoid those mistakes, and technical assessments are performed to locate, identify, and recommend fixing those design flaws.

Activity 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 into 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, erased, or their attributes modified.

MATERIALS

Computer running Microsoft Windows OS.

MISSION BRIEFING

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 in the lower left corner. In the Search programs and files text box, type **cmd** and press **Enter**.
2. A black command shell will appear. Typing **help** at the prompt gives you a list of available commands.

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

ACRONYM TO KNOW: FBO

An airport FBO (Fixed-Base Operator) is a private, specialized terminal and service provider located at an airport that acts as the primary support hub for general aviation, private jets, and charter flights.

The **COMP** command allows you to compare the contents of two files or sets of files for unauthorized changes. For this activity, bring up the black **cmdshell** and type each of the commands listed below at the prompt.

Command	Description	Application
osk	On-Screen Keyboard	If the computer is configured as a mouse-driven kiosk, Osk will get you an electronic keyboard.
explorer	Windows Explorer	
mrt		Periodically run as a good practice.
chkdsk		
taskmgr		
perfom	Windows Performance Monitor	
resmon	Resource Monitor	
shutdown	Unencrypted network protocols	
ping	Test “reachability” or determine IP.	
tracert	Determine domain name, routing	

Conclusion: This activity has demonstrated a tool to work around a computer that cannot boot to its Graphical User Interface or has had features disabled by administrators or malware. 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**."

Activity 2: Ping and Tracert Commands

OBJECTIVE

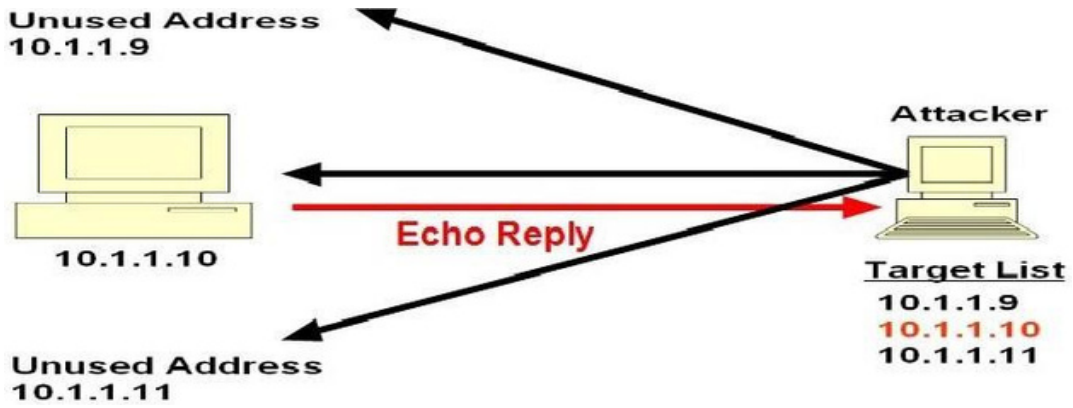
Hackers and penetration testers need to be successful to deliver their point regarding the urgency of the problem. Often, this means ignoring the most secure targets and looking for the weak links in the supply chain. If a DoD website or system is too secure, perhaps a DoD contractor is a more accessible 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.

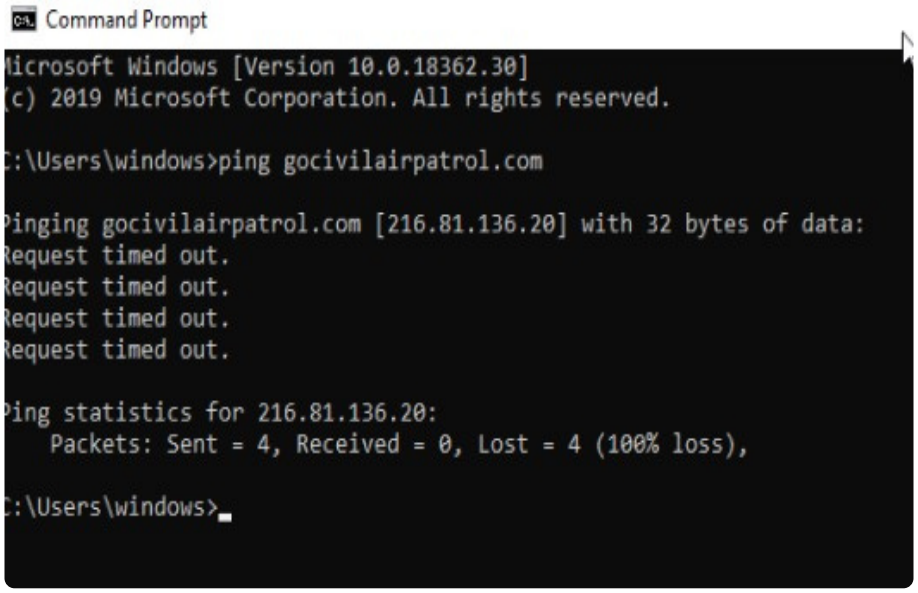
MATERIALS

Computer running Microsoft Windows OS or Unix/Linix, access to the internet.

MISSION BRIEFING

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 gocivilairpatrol.com from a **cmdshell**. We include an echo print below so that you may check your work. However, your results may vary.





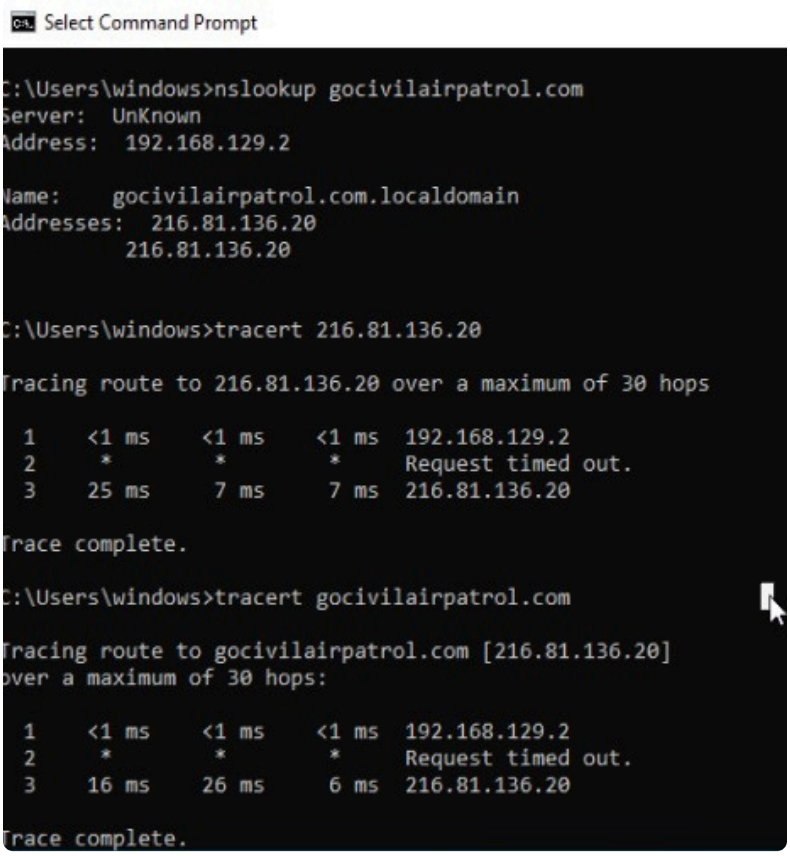
From the last command run, we received the IP Address of 216.81.136.20 Now run the ping command with the -a option to resolve a hostname. Remember, you can receive help on any of these commands by placing /? after the command.

For example, **C:\Users\Patriot\ping /?** will show all the switches for the ping command.

```
Usage:ping[-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-vTOS]
              [-r count] [-s count] [[-j host-list] | [-k host-list]]
              [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

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

Next, we will demonstrate the tracert command.



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 than what we see here.

Questions for further consideration:

- Research the Welchia worm. As a result of Welchia, how was the diagnostic usefulness of the ping command impaired?
- Research the nmap tool created by Gordon Lyon. What additional information can nmap determine, beyond simply whether a host is up or down?

Activity 3: Conduct a Whois Probe of a Website

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

Computer with internet access.

MISSION BRIEFING

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 is suspected of housing valuable data. A decision is then made to compile intelligence on the site in preparation for an attack. Once a cybersecurity expert has conducted their search, they will turn to researching the domain online for any reported weaknesses.

Your assignment is to emulate this approach as follows:

1. Go to the URL: **https://lookup.icann.org/en**
2. Enter any website URL on which you are curious, and choose Domain and hit Submit.

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:

- What are some ways you could openly determine which businesses supply goods and services to a US Defense Contractor?
- What is NAICS? What is the NAICS code for Engineering Services? For Drafting Services?
- How would you determine suppliers and subcontractors for Lockheed Martin or Boeing?

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)
- 688th Information Operations Wing (688 IOW)
- 689th Combat Communications Wing (689 CCW)
- 624th Operations Center (624 OC)

Mission Statement: The mission of the United States Air Force is to fly, fight and win - airpower anytime, anywhere.

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: BRIG. GEN. KEVIN B. WOOTON

Brig. Gen. Kevin B. Wooton is the Principal Deputy Director, Integrated Air, Space, Cyberspace, and ISR Operations, Headquarters Air Force Space Command, Peterson Air Force Base, Colo. The directorate is responsible for organizing, training, and equipping Air Force Space Command units for globally integrated space, cyberspace, and ISR operations and for assimilating capabilities into the operational level of war. Mission areas include missile warning, space control, spacelift and range operations, satellite command and control, nuclear event detection, airfield operations, offensive cyber operations, defensive cyber operations, DoD information network operations, and intelligence, surveillance, and reconnaissance. The directorate executes an annual operations and maintenance budget of $1 billion. Additionally, General Wooton acts on behalf of the Commander, Air Force Space Command, as the Air Force's Designated Approval Authority for systems connecting to the Air Force network and for the AFSPC's $11.4 billion space and cyberspace mission system portfolio.

Prior to his current assignment, General Wooton served as the Director, Communications and Information Directorate, Headquarters Air Force Space Command, Peterson AFB, Colo.

Biography Source: USAF
https://www.af.mil/About-Us/Biographies/Display/Article/108821/kevin-b-wooton/

EXPLORING CAREERS IN CYBERSECURITY

Getting the Education

The National Security Agency (NSA) has established Centers of Academic Excellence (CAE) to recognize cybersecurity curricula meeting an established standard for two types of study: Cyber Defense and Cyber Operations.

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. 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.

A Bachelor's degree in cybersecurity might include:

- Foundations of Cybersecurity
- Applied Cybersecurity Foundations I & II
- Accounting and Economic Aspects of Cybersecurity
- Human Actors and Cyber Attacks
- Introduction to Reverse Engineering
- Security Incident Handling and Management
- Digital Forensics
- Beyond Technology, the Policy Implications of Cyberspace
- Cyber Psychology
- Methods for Solving (and Not Solving) Puzzles

There is a unique balance of multi-disciplinary, including technical and non-technical topics such as system monitoring, incident responses, operating system and network basics, penetration testing, applied statistics, 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.

YOUTUBE VIDEO

Why Study Cybersecurity? | College Majors | College Degrees | Study Hall **https://youtu.be/QUTihHd2oO4**

DIGITAL EXTENSION

Explore the NSA's National Centers in Academic Excellence in Cybersecurity webpage to learn about current NCSA institutions. **https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/**

What Cybersecurity Jobs are In Demand?

Cybersecurity includes a multitude of roles and responsibilities encompassing a wide range of technical and non-technical skills. Defenders are responsible for ensuring security on a daily basis. Their scope of tasks can include vulnerability scanning, interpreting those scans, network monitoring for alerts, and incident response. Analysts will often investigate suspicious or anomalous events for malicious activity matching threat intelligence. Leaders tend to be highly experienced professionals qualified to set strategy and policy, train defenders and analysts, and conduct research & development.

Most cybersecurity jobs, especially with the U.S. Government, require a security clearance, including a background investigation. Personal Security Clearances (PCL) must be sponsored and can require U.S. Citizenship. A general search for "Cybersecurity jobs" will give you an understanding of the current demand level and various skills required.

Some roles to research further:

- Cybersecurity Analyst
- Filesystems Forensic Analyst
- Reverse Engineer
- Senior Cybersecurity Analyst
- Cybersecurity Mobile Security Analyst
- Cyber Intelligence 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

Interested in learning more about career pathways in cybersecurity roles? **CyberSeek.org** is a data-driven tool designed to provide detailed, actionable information about the cybersecurity job market in the United States. It is a collaborative project supported by several authoritative organizations, including:

- NIST (National Institute of Standards and Technology)
- CompTIA: The world's leading vendor-neutral IT certification body
- Lightcast (formerly Emsi Burning Glass): A premier labor market analytics firm.

Who is Hiring Cybersecurity-Related Jobs?

Cybersecurity is no longer a niche field for tech companies; it has become a fundamental requirement for any organization that handles data, money, or critical infrastructure. Below are some of the primary industries hiring cybersecurity professionals and the specific risks they are trying to mitigate:

1. **Financial Services (Banking, Insurance, Fintech)**
   - Financial institutions are high-value targets for theft and fraud. They handle massive amounts of personally identifiable information (PII) and liquid assets.
   - Focus: Transaction security, preventing business email compromise (BEC), and ensuring compliance with strict federal regulations (like GLBA or SOX).

2. **Healthcare (Hospitals, Pharmaceuticals, Biotech)**
   - Medical records are extremely valuable on the dark web because they contain permanent data (Social Security numbers, birth dates) that cannot be changed.
   - Focus: Protecting Patient Health Information (PHI) and ensuring the Availability of life-critical systems (like ventilators or surgery robots) against ransomware.

3. **Government and Defense (Public Sector)**
   - This sector manages national security data, classified intelligence, and public infrastructure.
   - Focus: Information Assurance (IA), protecting against Advanced Persistent Threats (APTs) from nation-states, and securing the supply chain for military hardware and software.

4. **Critical Infrastructure (Energy, Water, Transportation)**
   - These industries rely on Industrial Control Systems (ICS) and SCADA networks that bridge the gap between digital commands and physical machinery.
   - Focus: Prevent sabotage that could result in physical damage, such as grid blackouts or water supply contamination.

5. **Retail and E-commerce**
   - Retailers process millions of credit card transactions daily, making them targets for Point-of-Sale (PoS) malware and data breaches.
   - Focus: Securing the PCI DSS (Payment Card Industry Data Security Standard) pipeline and protecting customer databases from large-scale "credential stuffing" attacks.

6. **Technology and Managed Security Service Providers (MSSPs)**
   - As companies outsource their security, specialized firms (MSSPs) need large teams to monitor "Security Operations Centers" (SOCs) for multiple clients.
   - Focus: Threat hunting, incident response, and developing the security software (firewalls, antivirus) that other industries use.

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 **US Cyber Command** on 23 June 2009.

The Command has three main focus areas: Defending the DoDIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber attack.

The Command unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise. USCYBERCOM improves DoD's capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM is designing the cyber force structure, training requirements and certification standards that will enable the Services to build the cyber force required to execute our assigned missions. The command also works closely with interagency and international partners in executing these critical missions.

Mission Statement: "Direct, Synchronize, and Coordinate Cyberspace Planning and Operations - to Defend and Advance National Interests - in Collaboration with Domestic and International Partners."

PATRIOT BIO: BRIG. GEN. KEVIN B. WOOTON

General Keith B. Alexander, USA, served as the Director, National Security Agency (DIRNSA) beginning in 2005, and also as Commander USCYBERCOM beginning in 2010. Gen. Alexander gave the Keynote Presentation at BlackHat 2013, and then at DEF CON 20, he gave a session titled "Shared Values Shared Responsibility. He retired in March 2014.

The USCYBERCOM seal includes an MD5 Hash of its mission statement located on the inner gold band around the Eagle and Globe of its emblem. It reads "9ec4c12949a4f31474f299058ce2b22a."

Bonus Activity: MD5 Checksum (File Hash)

MISSION BRIEFING

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.

1. Using Notepad, copy the text from the Mission Statement above, without the quotes, into a text (.txt) file.
2. Open PowerShell and run the command on the text file you just created:
PS C:> Get-Filehash -path <path to file> -algorithm md5
3. Compare the MD5 hash with "9ec4c12949a4f31474f299058ce2b22a"
4. Verify that the hash matches that of the text of the file.
5. Change one letter of the Mission Statement text and process again to see the avalanche effect.
6. Write your own Mission Statement for your Cybersecurity Team and then hash it.

CONCLUSION

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.

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, including the Chronology, Biographies, and the Glossary.

A Cybersecurity Checklist For Future Exploration

- [ ] Visit the AFA Cyberpatriot website: **https://www.uscyberpatriot.org/**
- [ ] Visit the CIA SpyKids webpage: **https://www.cia.gov/spy-kids/**
- [ ] Create a Gmail News Alert (or other provider) to advise of cybersecurity issues as they happen.
- [ ] Explore cyber career profiles: **https://cyber.org/career-exploration/cyber-career-profiles**
- [ ] Create a Gmail News Alert (or other provider) to advise of cybersecurity issues as they happen.
- [ ] Stay up-to-date with cybersecurity training at cyber.org: **https://cyber.org/find-curricula**
- [ ] Learn coding with Scratch: **https://scratch.mit.edu/**

CIVIL AIR PATROL
AEROSPACE EDUCATION

KNOWLEDGE ASSESSMENT

This End of Module exam consists of 25 questions to test your comprehension of the urgency of the cyber threat, its vectors, and available countermeasures.

#	Question	Answer Choices
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 46b. Operation Aurora c. Cascade Mist 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

#	Question	Answer Choices
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	Which of the following are best practices for social media safety and privacy?	a. Only accept or follow friends you have met in real life b. Do not post your location c. Don't over-share d. all of the above
11	What is the OODA Loop?	a. Orient, Observe, Determine, Account b. Orbit, Organize, Decide, Announce c. Observe, Orient, Decide, Act d. none of the above
12	How many links are in the Cyber Kill Chain?	a. 3 b. 5 c. 7 d. 11
13	Ethics intends to promote a sense of fairness by creating rules of acceptable behavior and practices to help identify what is also unacceptable.	a. True b. False
14	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
15	Which of the following is a broken cryptographic hash function?	a. 7-Zip b. SHA-2 c. MD5 d. all of the above
16	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

#	Question	Answer Choices
17	The 21st Air Force is the USAF component of USCYBERCOM.	a. True b. False
18	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
19	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 Mist effect
20	What language was designed to retrieve information from relational databases?	a. C# b. TCP/IP c. SQL d. parsec
21	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
22	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, Cascade Mist Eligible Receiver d. Both a and b are correct
23	Crackers in Serbia attacked NATO systems in retaliation for NATO's intervention in Kosovo.	a. True b. False
24	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
25	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

CIVIL AIR PATROL
AEROSPACE EDUCATION

KNOWLEDGE ASSESSMENT ANSWER KEY

#	Answer
1	a
2	d
3	b
4	c
5	d
6	c
7	a
8	d
9	c
10	d
11	c
12	c
13	a
14	d
15	c

#	Answer
16	b
17	b
18	d
19	b
20	c
21	d
22	a
23	a
24	d
25	c

CIVIL AIR PATROL
AEROSPACE EDUCATION

ACTIVITY SOLUTIONS

Activity 1, Page 8

Plaintext	Hint	Ciphertext
IBM computers efficiently seek answers.	rot-1	HAL Bnlotsdqr deehbdmskx rddj zmrvdqr.
Gliders will depart at dawn to deliver Team Charlie Rangers to the river bridge.	rot13	Tyvqref jvyy qrcneg ng qnja gb qryvire grnz puneyvr enatref gb gur evire oevqtr.
please drink more Ovaltine.		Tpiewi hvmro qsvi Szepxmri.
xerxes departed sardis with a fleet and thirty-thousand horsemen.		ahuahv ghsduwhg vduglv zlwk d iohhw dqg wkluwb-wkrxvdqg kruvhphq

Activity 2, Page 10

Plaintext	Hint	Ciphertext
dawnspacecraftisarrivingatvesta		1efnbkebfjdwsulytdwsnmxfwbw&fxkp
new gru mm anf ir ebi rd air cr		ojnvjjnpfokifxrjuibnirjqgwkmnwg
af tfl ie s sem per vi gil an		tjddxgwlljqsbkytptuyfuggqdysnfh
sis mo tto fo rp atr io t		dtehtsujfklvpxvpuusnqtduwhqpsw

Activity 3, Page 13

No solution (yet).

CIVIL AIR PATROL
AEROSPACE EDUCATION

ACTIVITY SOLUTIONS

Activity 4, Page 14

Method	Method Definition	Codetext	Plaintext
CODE	When words or phrases have specific meanings, this is a code and not a cipher.	Climb Mount Nitaka.	Commence aerial attack on Pearl Harbor.
BACONIAN	A complex form of steganography or hidden writing in which two fonts are used.	I eXTEnd My haNd In wElComE To You	hello, _____.
RAILFENCE	When you rearrange your text in a "wave" sort of pattern (down, down, up, up, down, down, etc.), it is called a railfence.	caeinepeeootcgogaigaf rrzlvlwntrwdoiet	find railfence decoder online and advise

GLOSSARY OF TERMS

Term	Definition
7-Zip	A free, open-source file archiver used to compress and decompress data to save storage space or package multiple files together.
Active Content	Interactive web elements (like scripts or plugins) that provide functionality but can also be used to execute malicious code on a user's system.
AES	Advanced Encryption Standard. A widely used symmetric encryption algorithm that uses 128, 192, or 256-bit keys to protect sensitive data from sophisticated cryptographic attacks.
Algorithm	A finite, step-by-step set of instructions used to perform a specific task, solve a problem, or complete a computation.
Anonymizer	A tool or proxy server that hides a user's identifying information (like their IP address), making their internet activity difficult to trace.
ARP	Address Resolution Protocol. A communication protocol used to map an IP address to a physical MAC address on a local network.
ARP Attack	A technique (often called ARP Spoofing) where an attacker links their MAC address to a legitimate IP address to intercept, modify, or block network traffic.
Availability	A pillar of the CIA Triad ensuring that authorized users have reliable and timely access to data and system resources.
AVG Antivirus	A suite of security software designed to detect, block, and remove malware and other internet threats.
Backdoor	A method of bypassing normal authentication in a system. It can be installed by developers for troubleshooting or by attackers to maintain hidden access after a breach.
Bastion Host	A specialized, highly secured computer designed to withstand attacks. It usually sits on the edge of a network (like a DMZ) to act as a single point of contact for external traffic.
Biometrics	Authentication methods that use unique biological traits, such as fingerprints, facial recognition, or iris scans, to verify a user's identity.

GLOSSARY OF TERMS

Term	Definition
Black Hat	An unethical hacker who violates computer security for personal gain, malicious intent, or to cause disruption.
Black Hat Briefings	A world-renowned series of information security conferences that bring together corporate, government, and underground hacking communities to discuss the latest vulnerabilities.
Blacklist	A security filter that blocks traffic or access from specific, known-malicious addresses or entities while allowing everyone else by default.
Bluejacking	The act of sending unsolicited "spam" messages to discoverable Bluetooth-enabled devices.
Bluesnarfing	The unauthorized theft of data (such as contacts or photos) from a device via a Bluetooth connection.
Bluebugging	A severe exploit where an attacker takes full control of a Bluetooth-enabled device, allowing them to make calls, listen to conversations, or send messages.
Botnet	A network of "zombie" computers infected with malware and controlled as a group by a "bot herder" to perform massive tasks like DDoS attacks.
C4ISR	A military acronym for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance; the digital backbone of modern defense operations.
Cabir	Historically significant as the first worm developed to infect mobile phones via Bluetooth connections.
CAPTCHA	A challenge-response test used on websites to determine whether a user is a human or an automated bot.
CERT	Computer Emergency Response Team. An expert group that handles security incidents and provides research and education to protect network infrastructure.
Checksum	A unique string of characters (or hash) used to verify that a file has not been altered or corrupted during transmission or storage.
CIA Triad	The foundational model of cybersecurity consisting of Confidentiality, Integrity, and Availability.

GLOSSARY OF TERMS

Term	Definition
Cipher	An algorithm used to encrypt data by transforming readable text into an unreadable format through mathematical or systematic changes.
Cmdlet	Pronounced "command-let," these are specialized, lightweight commands used in the PowerShell environment to perform specific system management tasks.
CNCI	Comprehensive National Cybersecurity Initiative. A presidential directive aimed at coordinating federal efforts to protect U.S. government networks and critical infrastructure.
Code	Often confused with a cipher; a code replaces entire words or phrases with different meanings (e.g., the Navajo Code), whereas a cipher modifies individual characters.
Code Red	A historic 2001 worm that infected nearly 300,000 systems to launch a DDoS attack against the White House. It is a classic example of scheduled, automated malware.
Confidentiality	A pillar of the CIA Triad ensuring that sensitive information is accessible only to authorized users, protecting it from unauthorized disclosure or eavesdropping.
Computer Security	The proactive and reactive measures—including technologies, policies, and methods—used to protect information systems and devices from unauthorized access or damage.
Cookie	A small data file stored on a user's computer by a web browser that tracks site preferences and session information for future visits.
Cookie Scrubber	A privacy tool or browser setting used to delete cookies, preventing websites from tracking long-term user behavior or storing sensitive session data.
Countermeasure	Any action, device, or procedure used to reduce a vulnerability or thwart a specific threat to an information system.
Cracker	A term sometimes used to distinguish malicious actors who "break" systems for harm or profit from "hackers" who focus on technical skill and exploration.
Cross-Site Scripting (XSS)	A vulnerability where an attacker injects malicious scripts into a trusted website, which then executes in the victim's browser to steal data or hijack sessions.
Cryptography	The scientific study and practice of securing communication by transforming data to hide its meaning, prevent unauthorized use, or detect modifications.

GLOSSARY OF TERMS

Term	Definition
Cryptographic Hash Function	A mathematical algorithm that maps data of any size to a fixed-size string of characters. It is "deterministic," meaning the same input always produces the same "digest." Even a tiny change to the input completely changes the output.
Cyberbullying	The use of digital communication technologies to engage in deliberate, repeated, and hostile behavior intended to harm or harass others.
Cyber Espionage	The unauthorized use of computer networks to steal confidential information or intellectual property from governments or private organizations.
Cyber Terrorism	Premeditated, politically motivated attacks against information systems or data that result in violence, physical destruction, or extreme financial harm to non-combatant targets.
Cyberwarfare	State-sponsored actions designed to penetrate another nation's computers or networks to cause damage, disruption, or strategic disadvantage.
DEF CON	One of the world's oldest and largest annual hacker conventions. It serves as a major hub for security research, competitions, and networking between hackers and government agencies.
Defense-in-Depth	A layered security strategy that uses multiple independent security controls (firewalls, encryption, training, etc.) to protect assets; if one layer fails, others are in place to stop the attack.
DMZ	Demilitarized Zone. A subnetwork that sits between a private internal network and the public internet. it hosts external-facing services (like web or email servers) to keep the internal network isolated.
Denial of Service (DoS)	An attack that attempts to make a machine or network resource unavailable to its intended users by flooding it with traffic or crashing its services.
DES	Data Encryption Standard. A legacy encryption method from the 1970s. It is now considered insecure because its short 56-bit key can be easily broken by modern computers.
dig	Domain Information Groper. A powerful command-line tool used by network administrators to query Domain Name System (DNS) servers and troubleshoot name resolution issues.

GLOSSARY OF TERMS

Term	Definition
Digital Dirt	Also known as a negative "Digital Footprint"; the traces of online activity (posts, photos, comments) that could damage an individual's reputation or be exploited by others.
Disaster Recovery Plan (DRP)	A documented process for restoring critical IT systems and data following a major hardware failure, cyberattack, or natural disaster.
DDoS	Distributed Denial of Service. A DoS attack that uses a multitude of compromised systems (a botnet) to flood a target with traffic, forcing it to shut down.
DoD	United States Department of Defense. The federal department responsible for the nation's military forces and national security.
Dumpster Diving	A physical social engineering technique where attackers search through trash to find discarded passwords, sensitive documents, or hardware containing private data.
Elevation of Privilege	An attack stage where an intruder exploits a bug or configuration flaw to gain a higher level of access (such as Administrative or "Root" permissions) than they were originally granted.
Eligible Receiver	A landmark 1997 DoD exercise where an NSA "Red Team" successfully infiltrated military networks and civilian infrastructure using only publicly available software, proving the vulnerability of national systems.
Email Spoofing	The act of forging an email header so that the message appears to be from a legitimate or known sender. This is possible because the standard protocol for email (SMTP) does not inherently verify sender identity.
Encryption	The process of converting readable "plaintext" into unreadable "ciphertext" using a mathematical algorithm (cipher) and a secret key.
Enigma Machine	A famous electro-mechanical rotor machine used during WWII for encrypting secret messages. Its eventual decryption by Allied codebreakers provided a massive strategic advantage.
Ethical Hacking	Also known as penetration testing; the practice of authorized hacking to identify and fix security vulnerabilities before they can be exploited by malicious actors.

GLOSSARY OF TERMS

Term	Definition
Event Viewer	A Windows administrative tool that displays logs of system, application, and security events. It is essential for troubleshooting errors and auditing unauthorized access attempts.
Exploit	A specific piece of code, data, or command that takes advantage of a software or hardware vulnerability to cause unintended behavior, such as gaining unauthorized access.
Fedora	A popular, community-driven Linux distribution used as a platform for innovation and the testing of new open-source technologies.
Firewall	A network security device that monitors and filters incoming and outgoing traffic based on a defined set of rules. It acts as a barrier between a trusted internal network and untrusted external networks.
Footprinting	The initial phase of an attack where a hacker gathers as much information as possible about a target network (IP addresses, DNS records, employee info) to find potential entry points.
Forensics	The scientific process of collecting, preserving, and analyzing digital evidence to investigate a cybercrime or security breach.
GIAC	Global Information Assurance Certification. A leading certification body that validates the specific, hands-on technical skills of cybersecurity professionals.
GUI	Graphical User Interface. A visual way for users to interact with a computer using items like icons, menus, and windows, rather than typing text commands.
Hacker	Historically, a person with deep technical skill who enjoys exploring and modifying computer systems. In modern use, the term is often categorized into "White Hat" (ethical) and "Black Hat" (malicious).
Hainan Island Incident	A 2001 mid-air collision between a U.S. Navy EP-3 and a Chinese fighter jet. It serves as a key case study in the "Physical Security" domain regarding the risk of classified data compromise when hardware is captured.
Hardening	The process of securing a system by reducing its "attack surface." This involves removing unnecessary software, closing unused ports, and disabling unneeded services to minimize potential entry points for attackers.

GLOSSARY OF TERMS

Term	Definition
Honeypot	A decoy system or network designed to lure attackers. It is used to divert them from legitimate targets and to study their methods without risking real data.
IDS	Intrusion Detection System. A security tool that monitors network traffic or system activity for malicious behavior or policy violations, alerting administrators when threats are found.
Information Disclosure	A vulnerability where a system unintentionally reveals sensitive data (such as software versions or system paths) that an attacker can use to plan a more targeted strike.
Initialization Vector (IV)	A random or semi-random fixed-size input used in encryption to ensure that even if the same plaintext is encrypted twice with the same key, it produces different ciphertext.
Integrity	A pillar of the CIA Triad ensuring that data remains accurate and has not been altered or corrupted during storage or transmission.
IP Address	Internet Protocol Address. A unique numerical label assigned to each device on a network. It serves for host identification and location addressing (e.g., IPv4 "dotted-quad" format like 192.168.1.1).
ISTAR	A military framework standing for Intelligence, Surveillance, Target Acquisition, and Reconnaissance; used to manage and integrate information gathered from the field.
Jargon File	A historical glossary of hacker slang and culture originating from early technical institutions like MIT and Stanford.
Kernel	The core component of an operating system that manages the system's resources and the communication between hardware and software.
Keylogger	Software or hardware that records every keystroke made on a computer. It is often used by attackers to steal passwords, credit card numbers, and other sensitive data.

GLOSSARY OF TERMS

Term	Definition
Kludge	A "quick and dirty" workaround or inelegant solution to a problem. While functional, kludges often create long-term security vulnerabilities or system instability.
Kryptos Sculpture	A famous encrypted copper sculpture at CIA Headquarters. It serves as a symbolic landmark for the world of cryptology, with one of its four sections still unsolved.
Logic Bomb	Malicious code triggered by a specific event, such as a date (Time Bomb) or a specific user action. Unlike viruses, logic bombs often lie dormant until their conditions are met.
Macro Virus	A type of virus written in a macro language (often found in word processors or spreadsheets). It executes when the document is opened and can spread to other files.
Malware	Malicious Software. An umbrella term for any program designed to compromise the CIA triad—Confidentiality, Integrity, or Availability—of a system.
Man-in-the-Middle (MitM)	An attack where a third party secretly intercepts and potentially alters the communication between two authorized parties without their knowledge.
McAfee VirusScan	A widely used antivirus and security suite designed to detect and neutralize malware in home and enterprise environments.
MD5 Hash	Message Digest 5. A legacy cryptographic hash function. While still used for simple file integrity checks, it is no longer considered secure for digital signatures due to "collision" vulnerabilities.
MAC Address	Media Access Control Address. A unique "physical address" assigned to a network interface card (NIC) by the manufacturer. It identifies a specific device on a local network.
Moonlight Maze	A massive, two-year coordinated cyberespionage campaign discovered in 1998 targeting the Pentagon and NASA. It is one of the first widely recognized examples of an Advanced Persistent Threat (APT).
NIST	National Institute of Standards and Technology. A U.S. government agency that develops security standards and frameworks (like the NIST Cybersecurity Framework) used globally to protect infrastructure.

GLOSSARY OF TERMS

Term	Definition
NSA	National Security Agency. The U.S. intelligence agency responsible for global monitoring, collection, and processing of information (SIGINT) and the protection of U.S. government communications.
NCM	National Cryptologic Museum. A public museum affiliated with the NSA that preserves the history of American cryptology and intelligence.
NetWars	A popular suite of hands-on cybersecurity simulations and competitions used to train professionals in vulnerability assessment, ethical hacking, and incident response.
Nimda Worm	A highly aggressive 2001 worm that spread across the internet in just 22 minutes by using multiple "attack vectors" (email, web servers, and shared folders) simultaneously.
Nmap	Network Mapper. A powerful, open-source tool used for network discovery and security auditing. It "maps" a network by sending packets to hosts and analyzing the responses.
nslookup	A legacy command-line tool used to query DNS servers to find IP addresses associated with domain names. While still common, it is being replaced by the dig and host commands.
Patch	A software update designed to fix bugs, improve performance, or—most importantly—close security vulnerabilities. Timely patching is a core defense against malware.
Payload	The part of malware that performs the actual malicious action (e.g., deleting files, stealing data, or encrypting a drive) after the virus has successfully infected the system.
Penetration Testing	A simulated cyberattack against a system to check for exploitable vulnerabilities. Often referred to as "Pen Testing" or "Ethical Hacking."
PGP	Pretty Good Privacy. An encryption program used for signing, encrypting, and decrypting texts, emails, and files to increase the security of digital communications.
Pharming	A cyberattack that redirects a user from a legitimate website to a fake one by "poisoning" DNS entries or host files, even if the user types the correct URL.

GLOSSARY OF TERMS

Term	Definition
Phishing	A social engineering attack where an attacker sends fraudulent messages (often email) designed to trick a person into revealing sensitive information like passwords or credit card numbers.
Phreaking	A historical term for hacking into telecommunications systems, such as telephone networks, to make free calls or tap lines. It is considered the predecessor to modern computer hacking.
Ping Scan / Sweep	A network discovery technique that sends ICMP Echo Requests (pings) to a range of IP addresses to identify which hosts are active and "alive" on a network.
Ping of Death	A legacy DoS attack where an attacker sends a malformed or oversized ICMP packet to a target, causing the system to crash or freeze.
Ping Flood	A Denial of Service (DoS) attack that overwhelms a target by sending a massive volume of ICMP echo requests, saturating its bandwidth and processing power.
Port	A logical connection point used by programs to exchange data. Closing unnecessary ports is a key security practice to reduce the "attack surface" of a computer.
Pretexting	A social engineering tactic where an attacker creates a fabricated scenario (the "pretext") to establish trust with a victim, such as pretending to be a bank official or IT support.
Ransomware	A type of malware that encrypts a victim's files and demands a payment (ransom) in exchange for the decryption key.
RAT	Remote Access Trojan. Malware that grants an attacker full remote control over a victim's system. They can be used to steal data, record video/audio, or turn the system into a "zombie" for further attacks.
Repudiation	In a security context, the ability of a user to deny that they performed a specific action (such as sending a message or making a transaction) because there is no proof of their identity.
Road Apple	A physical social engineering bait, such as a USB drive or CD left in a public place. It relies on curiosity to trick a finder into plugging the infected media into their computer.

GLOSSARY OF TERMS

Term	Definition
Rootkit	A sophisticated type of malware designed to hide its presence while maintaining administrative (root-level) access to a system. It often subverts the OS to remain invisible to antivirus software.
Sabotage	Deliberate actions intended to weaken or destroy an organization or infrastructure through subversion or disruption of its digital or physical systems.
SACL	System Access Control List. A list of permissions attached to a file or object that specifies which users are allowed access and what specific actions (read, write, delete) they can perform.
SAIC	Science Applications International Corp. A major technology and engineering firm that provides technical support to the U.S. government and is a founding partner of CyberPatriot.
SANS Institute	A globally recognized organization that provides specialized cybersecurity training, research, and certifications (such as GIAC).
Scanning	The process of probing a network by sending packets to systems to identify open ports, active services, and potential vulnerabilities.
Scripting Language	Programming languages (like Python, JavaScript, or PowerShell) that are interpreted "on the fly" rather than compiled. They are frequently used by both admins and attackers to automate tasks.
Script Kiddie	A derogatory term for an unskilled attacker who uses pre-written scripts or automated tools developed by others to launch attacks, often without understanding how they work.
Shared Key Authentication	An authentication method used in early wireless protocols like WEP. It is now considered insecure and has been replaced by more robust standards like WPA3.
SMTP	Simple Mail Transfer Protocol. The standard protocol used for sending emails. Because the original design lacked built-in sender authentication, it is highly susceptible to email spoofing.
Smurf Attack	A type of DDoS attack where the attacker pings a network's broadcast address using a spoofed target IP. This causes every device on that network to reply to the victim, overwhelming their system.

GLOSSARY OF TERMS

Term	Definition
Sniffer	A tool used to capture and analyze network traffic. While used by admins for troubleshooting, attackers use sniffers to "listen" to unencrypted data (like passwords) sent over a network.
Sobig	A massive 2003 worm that notably disrupted CSX railway communications. It is a key historical example of how digital malware can have direct, physical consequences on transportation infrastructure.
Social Engineering	The "human hacking" aspect of security; the practice of manipulating or tricking people into giving up confidential information or performing actions that compromise security.
Spoofing	The act of disguising a communication from an unknown source as being from a known, trusted source (e.g., faking an email address, IP address, or website).
SQL Injection	A vulnerability where an attacker "injects" malicious database commands into a web form. If successful, it can bypass logins or allow the attacker to steal, delete, or modify database data.
SQL Slammer	A 2003 worm that exploited a known vulnerability to infect 75,000 systems in just 10 minutes. It serves as a classic lesson on the importance of timely patching.
SSH	Secure Shell. A protocol used to securely log into a remote computer. It provides strong encryption and is the standard alternative to the insecure Telnet protocol.
SSID	Service Set Identifier. The name of a wireless network. Security risks include using "default" names (like "Linksys") which can give attackers clues about the router's vulnerabilities.
Stenography	The practice of hiding a secret message within a non-secret file (such as an image or audio file) to avoid detection.
Streaming Media	Multimedia content delivered in real-time. In security, these streams are monitored for "Denial of Service" (DoS) vulnerabilities that could disrupt the availability of the content.
STRIDE	A threat-modeling framework used to identify security risks. It stands for: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, and **E**levation of Privilege.

GLOSSARY OF TERMS

Term	Definition
Stuxnet	A highly sophisticated worm discovered in 2010 designed to sabotage industrial control systems (PLCs). It is famous for being the first cyber-weapon used to cause physical damage to infrastructure.
Attack Surface	(Formerly "Surface of Vulnerability") The sum of all points in a system where an attacker can try to enter or extract data. Reducing the attack surface is a core goal of system hardening.
SYN Flood	A DoS attack that exploits the "TCP handshake" process by sending a constant stream of connection requests (SYN) but never completing the connection, eventually crashing the server.
Tampering	The unauthorized and intentional modification of data or software. A common countermeasure is using hashes to verify that a file has not been altered.
Threat	Any potential event or circumstance that could result in unauthorized access, destruction, or disruption of an information system or its data.
TLD	Top Level Domain. The last part of a web address (like .com, .gov, or .org). Malicious TLDs are often used in phishing or "typosquatting" attacks.
Tracert / Traceroute	A diagnostic tool used to show the path a packet takes across a network. It lists every router (hop) the data passes through between the source and the destination.
Trojan Horse	A type of malware that disguises itself as legitimate or useful software. Unlike a worm, a Trojan cannot replicate itself; it relies on a user to execute it.
TTX	Table Top Exercise. A simulated emergency drill where participants discuss their roles and responses to a hypothetical cyberattack scenario in an informal, classroom-style setting.
UDP	User Datagram Protocol. A "connectionless" protocol used for fast data transmission (like video streaming or gaming). Unlike TCP, it does not check if data arrived correctly, making it faster but less reliable.
Vector	The specific path or method an attacker uses to deliver malware or gain access to a system (e.g., an email attachment, a malicious link, or a vulnerable USB drive).

CIVIL AIR PATROL
AEROSPACE EDUCATION

GLOSSARY OF TERMS

Term	Definition
View Source	A browser feature that allows a user to see the underlying HTML/CSS code of a webpage. Attackers use it to find hidden vulnerabilities or clues about how a site processes data.
Virtualization	The process of running a "virtual" computer (Virtual Machine) inside a physical one. It allows users to run multiple operating systems (like Linux inside Windows) safely and in isolation.
Virus	A type of malware that "infects" legitimate files and requires human action (like opening an app) to spread. It replicates by attaching its code to other programs.
Vishing	Voice Phishing. A social engineering attack performed over the phone or VoIP where the attacker poses as a trusted official to steal personal information.
VoIP	Voice over IP. Technology that allows voice calls to be made over the internet rather than traditional phone lines.
War Dialing / Driving	War Dialing: Historically, calling many phone numbers to find modems. War Driving: Searching for available Wi-Fi networks by driving through an area with a high-gain antenna.
WEP	Wired Equivalent Privacy. An obsolete and highly insecure wireless security protocol. It can be cracked in minutes and should always be replaced with WPA2 or WPA3.
White Hat	An ethical hacker who uses their skills to find and fix security vulnerabilities with the owner's permission.
WiGLE	Wireless Geographic Logging Engine. A website and database that maps the location of wireless networks around the world based on data uploaded by users.
Windows PowerShell	A powerful task automation and configuration management framework from Microsoft. It includes a command-line shell and a scripting language used by admins to manage systems locally or remotely.
Worm	A type of malware that is self-replicating and self-propagating. Unlike a virus, a worm does not need to attach itself to an existing program or require human action to spread across a network.

GLOSSARY OF TERMS

Term	Definition
Zero-Day	A vulnerability or attack that is unknown to the software vendor or the public. Because there is no "Day 0" patch or antivirus signature available yet, these threats are extremely difficult to defend against.
Zeroization	The process of permanently erasing cryptographic keys or sensitive data from a device to prevent recovery, especially if the hardware is at risk of being captured or stolen.
Zombie	An infected computer that has been taken over by an attacker and is being used as part of a botnet to perform malicious tasks, such as launching a DDoS attack or sending spam.