This type of trojan gives attackers remote control over a computer:



a.

A backdoor trojan



b.

An exploit trojan



c.

A trojan banker



d.

A Trojan downloader

Question **2**

Correct

2.0 points out of 2.0

Flag question

Question text

This type of trojan can download and install new and additional versions or malicious software on your computer.



a.

A backdoor trojan



b.

An exploit trojan



c.

A trojan banker



d.

A trojan downloader

Question **3**

Correct

2.0 points out of 2.0

Flag question

Question text

This type of trojan is designed to steal your account data for online banking systems, e-payments, and credit cards.



a.

A backdoor trojan



b.

An exploit trojan



c.

A trojan banker



d.

A trojan downloader

Question **4**

Incorrect

0.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_\_ is the act of using the telephone in an attempt to scam the user into surrendering personal identifiable information (PII) that will be used for identity theft.



a.

Smishing



b.

Whaling



c.

Vishing



d.

Phishing

Question **5**

Incorrect

0.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_\_ refers to unauthorized personal devices that are not vetted through the organization's IT Department.



a.

Bots



b.

Black box devices



c.

White box devices



d.

Shadow devices

Question **6**

Correct

2.0 points out of 2.0

Flag question

Question text

This type of trojan contains data/code that can take advantage of a vulnerability on a system.



a.

A backdoor trojan



b.

An exploit trojan



c.

A trojan banker



d.

A trojan downloader

Question **7**

Incorrect

0.0 points out of 2.0

Flag question

Question text

This type of attack promises something for something else. This is a trick used to gain a user's login credentials or even personal identifiable information.



a.

Vishing



b.

Phishing



c.

Watering hole



d.

Quid Pro Quo

Question **8**

Correct

2.0 points out of 2.0

Flag question

Question text

A \_\_\_\_ scan determines if a target contains software or hardware weaknesses that are susceptible to a threat.



a.

Rogue



b.

Resource



c.

Threat



d.

Vulnerability

Question **9**

Partially correct

1.0 points out of 2.0

Flag question

Question text

Tools for Rogue Process and Device detection include? Select all that apply.



a.

PSExec



b.

FireEye Redline



c.

Didier Stevens Authenticode



d.

Microsoft Sigcheck

Question **10**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_\_ is computing infrastructure created and managed over the Internet. Instead of significant capital investments, organizations can choose to pay reoccurring fees for infrastructure provided over the Internet.



a.

IaaS



b.

BYOD



c.

PaaS



d.

SaaS

Question **11**

Partially correct

1.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_ are infected systems used for distributed denial of service attacks. Choose all that apply.



a.

Rogue Access Points



b.

Bots



c.

Zombies



d.

DNS Servers

Question **12**

Correct

2.0 points out of 2.0

Flag question

Question text

A \_\_\_\_\_\_ is a computer program that can make copies of itself.



a.

A self-garbling virus



b.

A trojan horse



c.

A worm



d.

A malicious payload

Question **13**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_\_ is programming code that appears to be something else. They often masquerade as freeware.



a.

Virus



b.

Trojan



c.

Spyware



d.

Adware

Question **14**

Correct

2.0 points out of 2.0

Flag question

Question text

A computer virus written in the same macro language used for software programs is known as?



a.

A stealth virus



b.

A macro virus



c.

A boot sector virus



d.

A self-garbling virus

Question **15**

Correct

2.0 points out of 2.0

Flag question

Question text

A type of virus that infects the boot sector of the Master Boot Record (MBR) or hard disk instead of the MBR is known as?



a.

A multipartite virus



b.

A macro virus



c.

A polymorphic virus



d.

A boot sector virus

Question **16**

Complete

6.0 points out of 6.0

Flag question

Question text

Compare and Contrast the similarities and differences between crypto and locker ransomware.

Answer text

Crypto ransomeware requires a decryption key and encrypts the files on said computer - leaving users unable to do complete simple tasks like opening their documents. The aim of crypto ransomeware is to infected the files on a system, and take advantage of vulnerabilities on the system as well. Locker ransomeware will completely block a users access to their device, sometimes locker ransomeware will ask for payment for a type of software or compensation which will allow a user in for a fee of a sort.

Question **17**

Complete

6.0 points out of 6.0

Flag question

Question text

What are the differences between adware and spyware?

Answer text

Adware will often display itself as an advertisement whereas, spyware will watch a systems activity. Adware operates in a visible fashion to a user and spyware operates in the depths of the system behind the scenes. Also, most of the time adware will not pose as much of a threat as spyware whereas, spyware is categorized as more malicious.

Question **18**

Complete

6.0 points out of 6.0

Flag question

Question text

Compare and contrast spear phishing, clone phishing, and whaling.

Answer text

Clone phishing attacks through attachments and links which the user clicks on or downloads. Spear Phishing will use something that looks like a familiar application or tool to prompt you into surrendering your password without thinking that you could be logging into a scam, and this is in order to gather the users login information. Whaling will target the head of the leader of an operation in order to gain complete and sudden access to the most useful information in the chain of command.

Question **19**

Complete

6.0 points out of 6.0

Flag question

Question text

Discuss convergence and the differences between IT and OT

Answer text

Information technology relates to all of the information in a system. Operational technology is focused on system control, direct interactions with software, and hardware. A convergence of the two systems allow for a merged environment and will result in real time decision making. The system itself becomes more complex when there is a convergence between IT and OT.

Question text

Identify the different roles and HIDS and NIDS would perform.

Answer text

HIDS are installed on intersection points, with these being servers or routers and NIDS are installed on all host machines. HIDS are useful at examining specific host based actions - applications, logs, and which files are being utilized. NIDS analyze a workflow between computers and networks to search for suspicious behavior or activities. A corporate network would ideally feature an usage of both HIDS and NIDS for the reason that they are both able to provide security and together they can optimize safety in a way that even some firewalls are not capable of doing.

\_\_\_\_\_\_ is when the behavior of malware is studied to determine any patterns, intent, or purpose behind the malware.



a.

Static Analysis



b.

Malware Analysis



c.

Dynamic Analysis



d.

Vulnerability Analysis

Question **2**

Correct

2.0 points out of 2.0

Flag question

Question text

In a \_\_\_\_\_\_ attack, a nefarious actor exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake.



a.

DoS



b.

DDoS



c.

Smurf



d.

TCP SYN Flood Attack

Question **3**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_\_\_ offers the ability to both scan and delete registry keys containing embedded null characters.



a.

PsLogList



b.

DiskMon



c.

VMMap



d.

RegDelNull

Question **4**

Incorrect

0.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_ is the area of the internet that we use daily.



a.

Deep Web



b.

Dark Web



c.

World Wide Web



d.

Surface Web

Question **5**

Partially correct

1.3 points out of 2.0

Flag question

Question text

The phases of incident response include? Select all that apply.



a.

Eradication



b.

Containment



c.

Response



d.

Isolation

Question **6**

Correct

2.0 points out of 2.0

Flag question

Question text

A \_\_\_\_\_ attack forces a system to crash by causing both fragmentation and length offset fields in IP packets to overlap each other on the attacked host.



a.

Teardrop



b.

Worm



c.

Polymorphic virus



d.

MitM

Question **7**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_\_ provides the ability to check both group and user permissions regarding data, registry keys, Window services, directories and more.



a.

AccessChk



b.

DiskMon



c.

TCPView



d.

LogonSessions

Question **8**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_ makes a computer user execute undesired or malicious actions on a web application that the user is already authenticated to.



a.

CSXS



b.

CSRF



c.

XSS



d.

CRSF

Question **9**

Incorrect

0.0 points out of 2.0

Flag question

Question text

During an \_\_\_\_\_ attack, the attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client



a.

Session Hijacking



b.

Teardrop



c.

Replay



d.

Smurf

Question **10**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_ is when an attacker injects a payload with malicious JavaScript into a website's database.



a.

CSXS



b.

CSRF



c.

XSS



d.

CRSF

Question **11**

Incorrect

0.0 points out of 2.0

Flag question

Question text

A \_\_\_\_\_\_ attack involves using IP spoofing and the Internet Control Message Protocol (ICMP) to saturate a specific target network with traffic.



a.

TCP SynFlood



b.

Smurf



c.

Ping of Death



d.

DoS

Question **12**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_ may only be accessed via special tools, such as the onion router, and is often used by law enforcement and hackers.



a.

Deep Web



b.

Dark Web



c.

World Wide Web



d.

Surface Web

Question **13**

Correct

2.0 points out of 2.0

Flag question

Question text

\_\_\_\_\_\_ is when an attacker or ethical hacker initiates phases of the attack with some knowledge of the target(s).



a.

Grey Box Testing



b.

Purple Box Testing



c.

White Box Testing



d.

Black Box Testing

Question **14**

Incorrect

0.0 points out of 2.0

Flag question

Question text

A \_\_\_\_\_\_ attack is when an attacker is intercepting or hijacking sessions between a client and server.



a.

TCP SYN Flood



b.

MitM



c.

Session hijacking



d.

Replay

Question **15**

Correct

2.0 points out of 2.0

Flag question

Question text

 \_\_\_\_ refers to specific areas of the Word Wide Web that are not visible to the majority of people surfing the web.



a.

Deep Web



b.

Dark Web



c.

World Wide Web



d.

Surface Web

Question **16**

Complete

6.0 points out of 6.0

Flag question

Question text

Compare and Contrast base, temporal, and environmental scores including all sub scores.

Answer text

The base score is heavily relied upon by corporations. The base score is made up by exploitation metrics and impact metrics. The temporal score measures vulnerability and can either increase or decrease the base score based upon multiple factors. Temporal score consists of remediation levels, report confidences, and exploit code maturity. The environmental score also refines the base score based on its own environment. Environmental score includes categories such as collateral damage potential, target distribution, integrity requirements, availability, and confidence.  Scoring is ranked from 0 being the lowest and 10 being critical.

Question **17**

Complete

0.0 points out of 6.0

Flag question

Question text

Choose 2 tools you learned about for malware analysis. Identify pros and cons of each.

Answer text

Question **18**

Complete

0.0 points out of 6.0

Flag question

Question text

Identify and describe the seven steps involved in the creation of an organizational incident response plan.

Answer text

Question **19**

Complete

6.0 points out of 6.0

Flag question

Question text

Identify and discuss 3 types of APTs.

Answer text

Infiltration is where the hacker will infiltrate the system and use malicious uploads or social engineering attacks to gain access to the targets network. Infiltration can also include DDOS attacks which can weaken a security system to make it easier to breach. Another type of infiltration can include backdoor breaches which is a type of malware that will grant access to the hacker. There are many APTs that can be utilized however, these are just a few.

Complete

2.0 points out of 6.0

Flag question

Question text

Describe each of the 5 attack phases.

Answer text

1. Reconnaissance is where a hacker uses some type of informations to get intel on their intended target. This can be social media, company sites or other sources where data is stored or shared by the target

2. Incursion takes place after the hacker has already gotten inside of the targets network. During incursion the hacker will attack vulnerable systems with malware. Then APT will use various methods such as spear phishing, theft, utilizing downloads or even social engineering.

3. Discovery is where the hacker essentially lays low and creates a plan of attack in order to avoid detection. The hacker will use methods to get inside of the backdoor of the targets system. The hacker may use an APT to allow themself access to normally restricted areas of the targets system.

4. Capture, which is where the hacker has captured data from the target over a timeframe and now they will install APT malware. This is where the hacker essentially has caught the target and now will acquire the sensitive information needed/wanted on the target.

5. Exfiltration is when the APT will patiently wait for an opportunity to send the acquired information from their target to their control center. The control center will then provide an analysis on the information and sometimes even further exploit their target through various methods.

Week 1

# Malware and Attack Vector

**Content Author:** Dr. Michael J. Simko

Graphical user interface

Description automatically generated with medium confidence

|  |  |
| --- | --- |
| (transcript included in lecture to the right of this video) | **Malware** Malware is a generic term (MALicious softWARE) increasingly being used to describe any form of malicious software such as:   * Viruses * Trojans * Malicious active content * Change in checksum * Unexpected disk access * Change in file time stamp * Decrease in hard drive space * Random system activities and messages * Latency |

|  |  |
| --- | --- |
| (transcript included in lecture to the right of this video) | **Viruses** Macro Virus: a computer virus written in the same macro language used for software programs. (Examples: Microsoft Excel or Word).  Boot Sector Virus: a type of virus that infects the boot sector of the Master Boot Record (MBR) or hard disk instead of the MBR.  Stealth Virus: a hidden computer virus that attacks operating system processes and averts typical anti-virus or anti-malware scans. (Often hidden in files, partitions and boot sectors).  Polymorphic Virus: a complicated computer virus that affects data types and functions. It is self encrypted and duplicates itself by creating usable, slightly modified copies of itself.  Multipartite Virus: a computer virus that infects and spreads in multiple ways. (multiple steps to accomplish its goal).  Self Garbling Virus: a type of computer virus that will attempt to hide from an antivirus program by garbling its own code. This is all in attempt to trick the antivirus scanner and stay hidden. |

## Ransomware

Ransomware is a type of malicious software that prevents the availability of data until a ransom is paid. There are two types of generic Ransomware, Crypto ransomware and Locker ransomware.

|  |  |
| --- | --- |
| Crypto ransomware Crypto ransomware encrypts the user's files or prevents access to them. The files are retrieved upon making an attacker's demand in payment usually requested in bitcoin. Once the ransomed is paid, there is no guarantee the data will be returned. It's risky and there's a 50/50 chance the attacker will actually return your files. | Locker ransomware Locker ransomware locks out the physically computer, typically the MBR, preventing the machine from actually booting until a payment is made. Once the payment is made, the attacker will provide an unlock key that actually unlocks the system. Once again, there's a 50/50 chance of the attacker returning your files. |

**The best defense in these cases is to back up your data!**

[Malware Part 3 - Worms Transcript](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week01/mp4-FA22-MalwareAndAttackVectors/Part3Transcript.html)

## Trojans

|  |  |
| --- | --- |
| A low angle view of a building  Description automatically generated with low confidence  Image by [13smok](https://pixabay.com/users/13smok-5135280/?utm_source=link-attribution&utm_medium=referral&utm_campaign=image&utm_content=3108969) from [Pixabay](https://pixabay.com/?utm_source=link-attribution&utm_medium=referral&utm_campaign=image&utm_content=3108969) | A Trojan Horse is an apparently useful and innocent program (typically appears legitimate) containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.  A few examples of Trojan Horses are:   * Backdoor Trojan: gives attackers remote control over your computer * Exploit Trojan: contains data/code that take advantage of a vulnerability on your system * Trojan Banker: designed to steal your account data for online banking systems, e-payments and credit cards * Trojan Downloader: downloads and installs new and additional versions or malicious software on your computer * Trojan FakeAV: These are programs that simulate activity of a real antivirus software. They claim they will remove viruses or threats through extorting your money. But really it's just a trick to gain access to your banking information. |

## Backdoor

  
Image by [Gerd Altmann](https://pixabay.com/users/geralt-9301/?utm_source=link-attribution&utm_medium=referral&utm_campaign=image&utm_content=7057560) from [Pixabay](https://pixabay.com/?utm_source=link-attribution&utm_medium=referral&utm_campaign=image&utm_content=7057560)

A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, product or embedded device. It is an "undocumented portal or access" to your machine without your awareness/consent. It can also be referred to as intentional faults put into code to give someone access outside of the normal security model.

[Malware Part 4 - Rootkits Transcript](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week01/mp4-FA22-MalwareAndAttackVectors/Part4Transcript.html)

## Keylogger

|  |  |
| --- | --- |
|  | A keylogger, also known as a keystroke logger or a system monitor, is a type of surveillance technology used to monitor and records the keystrokes of a select victim.  Keyloggers can be used to capture usernames and passwords as you type them into various websites such as bank account websites, mortgage or bill websites.  Keyloggers aren't always used for malicious intent. Some parental controls offer the ability to keylog conversations and will send messages to assist parents with monitoring their children's activities. |

Shape

Description automatically generated with low confidence

**REMEMBER**

|  |
| --- |
| It is illegal to install the keylogger on a device you don't own as it's a clear invasion of privacy on the system if it is not owned by yourself or your organization. |

Some examples of free keyloggers are: [KidLogger](https://kidlogger.net/" \t "_blank), Actual [Keylogger](https://en.wikipedia.org/wiki/Keystroke_logging) and [Revealer Keylogger Free](https://www.logixoft.com/en-us/index).

[Malware Part 5 - Adware/Spyware Transcript](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week01/mp4-FA22-MalwareAndAttackVectors/Part5Transcript.html)

## Buffer Overflow

|  |  |
| --- | --- |
| (transcript included in lecture to the right of this video) | A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer (fixed block of memory), overruns the buffer's boundary and overwrites adjacent memory locations.  Exploiting a buffer overflow allows an attacker to control or crash process or to modify its internal variables.  Most operating systems have introduced runtime protection to make it more difficult for buffer overflow attacks to succeed. |

## Zero-Day

A Zero-Day exploit is an attack that exploits a previously unknown security vulnerability. It's sometimes referred to as an attack that takes advantage of a vulnerability the same day it becomes known. An example of a zero-day attack would be Stuxnet, which you will be learning about in additional required resources.

As we complete this lecture you should now have a better understanding of malware and various attack factors. Knowing basic information about various attacks will contribute to your ability to identify them in action.

Text

Description automatically generated

You should now be aware of many different attacks, but how exactly do you identify an attack in progress?

This lecture will discuss indicators that help you do just that.

Have you ever heard of unauthorized devices being detected or mysteriously showing up on a network? Commonly, we refer to these devices as rogue devices. Rogue processes are similar in nature. A rogue process may be any untrusted or suspicious process running on an actual host or system. A host system can be no other than a Windows 10/11 system, MAC, or even a server. Utilizing host-based security systems (HBSS's) can help identify rogue devices and processes on our networks and systems, in addition to the several tools identified at the end of the lecture.

## What is a Rogue Device?

A rogue device is not always intentionally malicious. For example, a piece of hardware popping up on scanners as an unknown device could be just an employee connecting a personally owned device to the company owned internet. This device may or may not be authorized by the organization but digging into more detail will provide clarification. It is highly recommended to implement rogue device detection software on company networks to be safe rather than sorry. It is always a good assumption and practice to treat all unknown devices as malicious in nature, engaging right away in company incident response procedures. This will at least flag the device and prompt further investigation.

Rogue Devices serve several purposes. A few examples are:

* To harvest credit card or payment information
* To acquire usernames and passwords
* To damage a company's network
* For network activity monitoring
* To hurt a company's reputation

## Examples of Rogue Devices & Processes

Let's discuss some actual examples of rogue devices you may come across in your ventures as a cybersecurity architect.

* **Bots or zombies**are infected systems used for distributed denial of service attacks. A computer serving as a bot on your company's network would be classified as a rogue device, as it is malicious and no longer performing its original intent as a workstation.
* An **access point**can be overtaken and used as a rogue access point. In this case, the attacker may have the intent of performing man-in-the-middle or client mis-association. Client mis-association is when an attacker sets up a rogue access point outside of a building and lures victims into connecting to it.
* A **sniffer**or any device spying on or analyzing traffic is yet another example of a rogue device. Unless this device is configured for packet analysis by the organization; an unauthorized device sniffing or scanning your network is probably not a good thing.

## Rogue Device Connection

Rogue devices may connect to a network using multiple avenues and mediums. Some common examples of how a rogue device may gain access to your network are:

|  |  |
| --- | --- |
| **Via Third Party Vendors** | Your company's network may be for the most part secure, but that doesn't mean all vendors or business partners your company does business with are. Hold third party vendors accountable for security implementation, standards and requirements. Rogue devices on their network could expose your customer personal identifiable information or agency trade secrets. |
| **Shadow IT** | Shadow devices or shadow IT refers to unauthorized personal devices that are not vetted through the organization's IT Department. What does this mean? It means that these devices are not authorized and probably not being patched. The organization's IT and cybersecurity departments ensure compliance on company owned assets (in a perfect world), but an unpatched rogue device serves as a vulnerability with multiple avenues for attack. |
| **No monitoring or rogue device detection software** | How would we know there is a rogue device if we are not looking for one? Lacking network visibility can lead to compromise of company systems and theft of data. |

## Rogue Device Detection

There are some basic strategies for identifying rogue devices. As we already discussed, lack of monitoring can lead to serious danger and high risk for the organization. The following primary actions should be implemented through various means to ensure risk is lowered to an optimal level:

|  |
| --- |
| 1. **Instantaneous Alerts** - Automated network discovery tools can assist in identifying devices as they populate the network. Notifications or alerts can be sent to the appropriate personnel monitoring the network in order to take hasty and appropriate action based on the alert. |
| 1. **Consistent Scanning** - Daily or weekly scans will help identify unknown IP addresses, vulnerabilities and devices that may not be authorized on the network. Nessus is a great tool for this and can be configured to run automated scans for enforcing consistency. |
| 1. **Continuous Monitoring** - As we learned in previous lectures, continuous monitoring is a must. You never know when devices may break, require updates or patching or be due for replacement if you are not staying engaged and actively monitoring all aspects, systems and technology within the enterprise's infrastructure and operations. |

## Rogue Process Detection

While the intent of malware is usually to remain unnoticed, identifying rogue processes early will help save time, money, resources and productivity for any organization. A few best practices exist for identifying a rogue process:

|  |
| --- |
| Monitor event Identification "Event ID 4688" for the creation of new processes. The information gathered from the event may help determine whether the process is rogue or not. The log also includes useful information such as the path of the process (executable), data and time stamps associated with the program starting, the creator and name of the process and who actually launched it. |
| Use the [**National Software Reference Library**](https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl) (NSRL) to verify processes or programs are legitimate. |
| **Verified code is signed.** Official software usually includes a signature (signed code) from the vendor or publisher to confirm the legitimacy of the software. Unsigned code can be a red flag that either malware has been incorporated into a previously legitimate piece of software or processes should not be trusted. |

## Tools for Rogue Processes and Device Detection

|  |  |
| --- | --- |
| [**Microsoft Sigcheck**](https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck)  Sigcheck is a SysInternals tool that provides file version, certificate chains, digital signature info, time stamp data and more. | [**PSExec**](https://docs.microsoft.com/en-us/sysinternals/downloads/psexec)  PSExec is another SysInternal tool providing the ability to execute processes remotely. This would most likely be a tool an attacker uses to access a system. Keep a lookout for the PSEXESVC process in the System Event Log (Event ID 7045). |
| [**FireEye Redline**](https://www.fireeye.com/services/freeware/redline.html)  This is an endpoint security tool providing file and memory analysis capabilities. It possesses the ability to audit and harvest all running processes for analysis. | [**Didier Stevens Authenticode Tools**](https://blog.didierstevens.com/programs/authenticode-tools/)  Similar to Sysinternals, this tool has the ability to verify signatures in PE files or authenticate code. |

WEEK 2

# Lecture: Threat Analysis

**Content Author:** Dr. Michael J. Simko

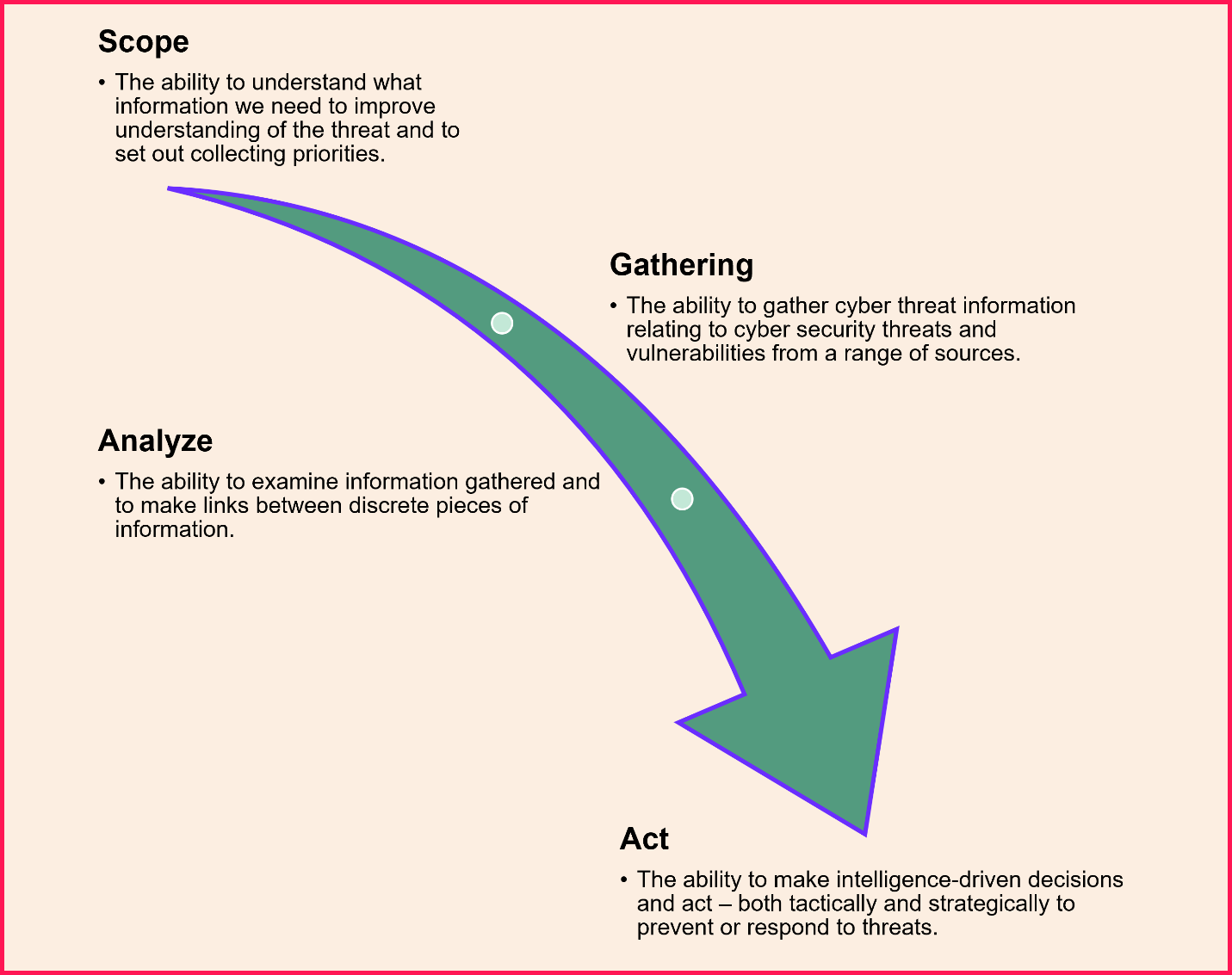
We are familiar with the general meaning of the word "threat," however, how does a threat pertain with the realm of cybersecurity? A threat is anything that can hinder an organization's ability to maintain confidentiality, integrity and availability of systems or data. We understand by now that some information technology systems may possess vulnerabilities, which if not patched increase the risk of exploitation. The vulnerabilities, impact or probability of exploitation occurring and threat in itself are utilized in a formula for calculating risk. The formula consists of multiplying organizational risk by vulnerabilities to determine the level of threat. Taking this into account, we will explore various means for threat analysis.

Let's talk about how threat analysis actually works. There are generally four primary phases to the process:

1. The **scope** or the ability to comprehend the threat.
2. **Gathering** information pertaining to the threat.
3. **Analyzing** or connecting links between the info.
4. Taking **action** on the threat.

**Figure 1**

Threat Analysis Phases



[Threat Analysis Phases Image Adapted from Source](https://resources.infosecinstitute.com/topic/cyber-threat-analysis/)

[Image Description for Threat Analysis Phases](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week02/FA22-ThreatAnalysis/ImageDescriptionFigure1.html)

Threats can be sorted into either human or non-human examples. When a threat is identified, you must analyze the **impact** the threat would have on the organization, the **likelihood** of the threat occurring, and the whether the threat is **cost effective** to mitigate.

Common examples of threats include:

|  |  |
| --- | --- |
| **Human Threats:** | Technicians, backup operations, electricians, hackers, theft, accidents, IT personnel lacking training, non-technical staff and more. |
|  | |
| **Non-Human threats:** | Viruses/malware, HVAC, electrical, fires, water and more. |

When assessing threats, it is best to develop a quantitative method for scaling various threats and the impact they may have on the organization. This way threats can be organized in a way that clearly states the severity and associated cost to mitigate the threat(s).

## Threat Modeling

Threat modeling is the process in which you would specifically identify threats and countermeasures to mitigate threats. An example of threat modeling would be making a list of all information systems on a network, identifying their purpose or function, listing threats pertaining to each and then associating each piece of equipment with a potential threat level. Furthermore, an example you may deal with on the job would be identifying critical infrastructure and facilities. We would want to pay more attention to a datacenter housing enterprise circuits, servers and hardware than a computer lab with 12 computers in a conference room.

## The Threat Matrix

A threat matrix is used to categorize threat attributes into metrics. For example, a threat matrix would rank threats by severity using a numerical value. Furthermore, refer to the chart below for a visual example of a threat matrix. On a ten-point scale, 1 being the lowest and 10 being the highest risk, you can see how each threat or vulnerabilities stacks up as compared to another in this scenario.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Vulnerabilities**  **Threats** | **Firewalls** | **Databases** | **Application Architecture** | **Physical Security** | **Insecure Wireless** | **Internet-based service (live VPNs)** | **Total Score** |
| **Intrusion (Hacking, Password Attacks)** | 9 | 3 | 9 | 9 | 9 | 3 | **42** |
| **Insider Attacks** | 3 | 3 | 3 | 9 | 3 | 1 | **22** |
| **DDoS** | 9 | 0 | 9 | 1 | 3 | 3 | **25** |
| **Theft of Hardware** | 1 | 1 | 1 | 9 | 3 | 1 | **16** |

[Threat Matrix Adapted from Source](https://resources.infosecinstitute.com/topic/cyber-threat-analysis/)

While threats are commonly associated with risk and software vulnerabilities, threats also correlate to the specific people behind attacks. Staying situationally aware of current events, current attacks, current trends and those responsible is necessary to stay ahead of the curve. While several hackers carry out their will due to a desire of financial gain, others are simply trying to prove a point, showcase skill or state a cause. There are regions on the World Wide Web that provide opportunity for those straying away from ethical behavior. You should understand the purposes behind these areas, why they exist and what the repercussions are for those who choose to use them. There is a thin line between a white, grey and black hatter.

**Disclaimer:**

This lecture discusses places on the web that are dangerous to visit. This discussion is for educational purposes only and Walsh College does not take responsibility for your actions or encourage partaking in any illegal activity on Dark Web. If you choose to, you do so at your own risk.

## Threat Landscape

The term threat landscape is commonly used in cybersecurity to describe both attacks that could occur and attacks that have occurred pertaining to a specific geographic location, population or even industry.

## Script Kiddies

Years ago, hackers were referred to as skilled individuals who understood how computers and software worked down to the binary level. These hackers knew how to manipulate these systems and code to carry out whatever actions they wished. While hackers with the same talent and motives exist today, there is a newer, more common breed known as script kiddies. In a sense, script kiddies have been around for years, but due to all of the advancements in open source software and the availability of hacking tool suites; script kiddies are the new trend of hacker. Rather than writing their own code, a script kiddie utilizes existing computer code, tools or scripts that are readily available. The mentality is why create your own code if someone has already done it for you? A few examples of hacker suites are:

|  |  |
| --- | --- |
| A person sitting in a chair  Description automatically generated with low confidence | * **BackTrack** is Linux based software (one of the originals) that has been used for penetration testing and digital forensics. * **Kali Linux**, maintained by Offensive Security Ltd., is another Debian based distribution for pen testing, forensics and security analysis. It is one of the best and most commonly used to this day. * **BackBox** is a Ubuntu based distro used for pen testing and security. * **Parrot Security OS** was developed by Frozenbox Network and provides encryption, anonymity and a cloud friendly environment. * **BlackArch**, provided by the ArchLinux distribution is yet another tool available for pen testing and security assessment. |

## Hacktivism & Hacktivists

Commonly used to voice free speech or defend a specific cause, hacktivism uses technology to promote political beliefs or demand social change. Hacktivists are those who actually carry out nefarious or unauthorized actions to support a cause through use of technology. An example of a Hacktivist group is Anonymous.

## Anonymous

Anonymous is "a loose band of people who share the same kind of ideals and wish to be a force for chaotic good," as described by Coldblood, a spokesperson for the group (NBC, 2013). This group is said to have formed around 2003, originating from a website message board known as 4chan. Anonymous has been responsible for targeting several governments (Iran, Zimbabwe and Australia), several churches and financial organizations such as MasterCard and Paypal.

Logo, icon

Description automatically generated with medium confidence

## Surface Web

Surface web is the area of the internet that we use daily. It is the most common area of the web utilized by the public. This is where our search engines such as Google perform searches, as well as where we shop, conduct research, collaborate on social media, etc.

## Deep Web

The deep web refers to specific areas of the Word Wide Web that are not visible to the majority of people surfing the web. While anyone can visit the Deep Web legally, there are places on Deep Web that may not be legal to visit based off your place of residence. Think of Deep Web as a large archive. It is a place where knowledge is endless, however, the content is not visible through means of a normal search engine, such as Google or Yahoo (commonly referred to as the surface web). Not to be confused with Deep Web, there is a small portion of the web referred to as the Dark Web.

## Dark Web

The Dark Web is a zone on the web where many illegal activities occur. Dark web is used both by hackers and law enforcement for various purposes. Dark web may only be accessed via special tools, such as the onion router.

## The Onion Router (TOR)

In the previous lecture on investigation techniques, we discussed search engines that grant the opportunity to search web content anonymously. The Onion Router or TOR is a web browser capable of doing the same. When using TOR, it is recommended to utilize a virtual private network (VPN). You can never be too safe when navigating uncharted terrain. Onion routing is a term used to describe browsing the internet in privacy. Orbot is the TOR equivalent application for android devices or mobile phones.

|  |  |
| --- | --- |
| [View more information on TOR](https://www.torproject.org/)  [TOR logo](https://www.torproject.org/) | [View more information on Orbot](https://guardianproject.info/apps/orbot/)  [Orbot logo](https://guardianproject.info/apps/orbot/) |

## Advanced Persistent Threats (APTs)

You may have heard the term APT before, but if not, we are talking advanced persistent threats. Advanced persistent threats refer to nefarious actors who possess a significant amount of expert level knowledge, endless motivation, and experience in exploiting targets to include the ability to discover and exploit various attack vectors until the desired goal is achieved. Often, APTs a grouped into several categories.

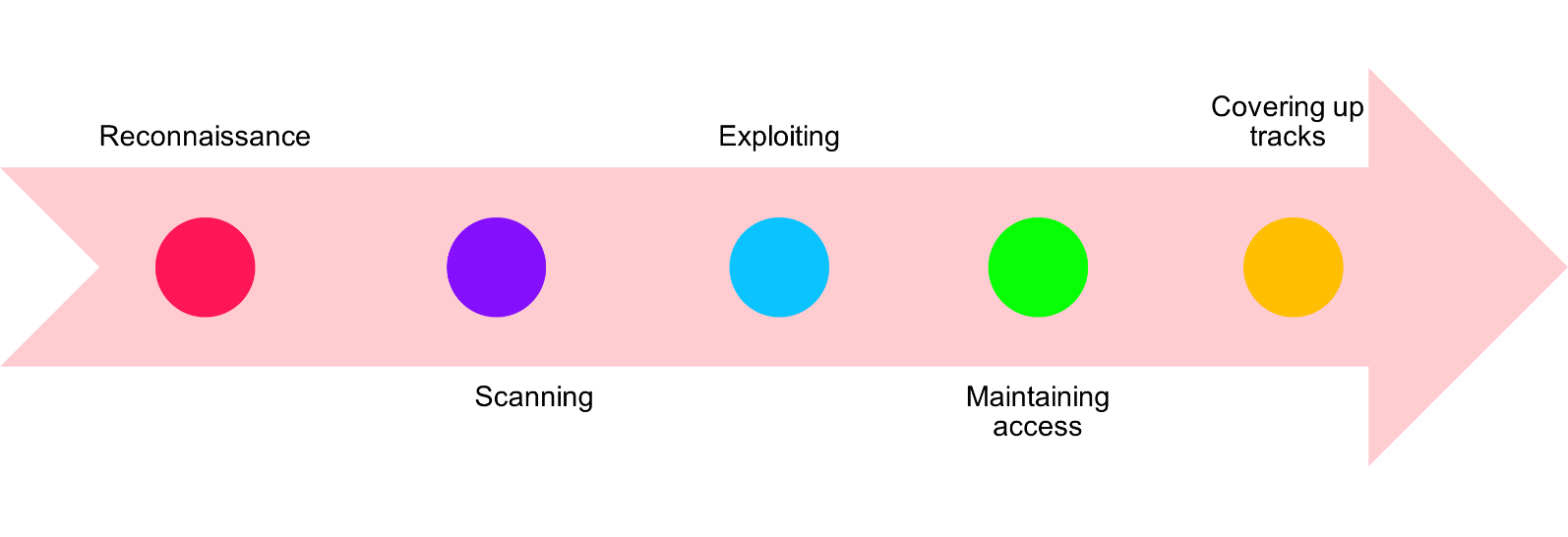
# Lecture: Attack Methodology

**Content Author:** Dr. Michael J. Simko

Today's lecture will address attack methodology. In order to provide your organization the best possible honest effort of cyber defense, you must learn to think like the attacker. Thinking outside of the box and assessing all potential avenues of attack is a necessary skill. Once you are truly able to see through the eyes of the attacker, the horizons will expand.  
  
Defensive cybersecurity is like a chess game, where the good guys must always stay at least 5 steps ahead of the bad guys. The methodology of an attack or phases of attack can be categorized into 5 stages as in the graphic below.

## Methodology of an Attack

**Figure 1. Methodology of an Attack Process**



### Reconnaissance

Reconnaissance is where an attacker **attempts to gather any information about individuals or an organization**, which could provide an upper end. Gathering of data **may be harvested either actively or passively**. Some methods an attacker may use to gather information may range from:

* Rummaging through trash (dumpster diving)
* Searching social media for personal identifiable information (PII)
* Reviewing company websites for individuals to target through means of social engineering.

This is the phase where specific targets are determined, if not already identified.

### Scanning

During the scanning phase, **several tools and methods are actively used to probe a network, determine open ports and protocols and identify exploitable vulnerabilities**. The scanning process also contributes to **determining the layout of a network and understanding how particular services are functioning within the organization**.

Two of the most common methods of scanning involve utilizing:

* NMAP (port and protocol scanning)
* Nessus (Vulnerability scanning)

Identifying opportunities to elevate privilege and exploit vulnerabilities, leads to the next phase of an attack: the exploitation phase.

### Exploiting

The exploitation phase consists of the attacker **identifying points of entry and vulnerabilities through scanning a target network or hosts**. Once a method to exploit is identified, the attacker will **continue pushing forward to carry out the attack**. This is where tools such as Metasploit may be utilized. This stage may also be referred to gaining access to critical systems or hosts on a company's internal network. An attacker or black hat hacker will utilize any means necessary to gain access, which is different from the mindset of an ethical or white hat hacker. An ethical hacker will require written consent from the stakeholder to perform any of the five attack stages.

### Maintaining access

During this phase, the attacker wants to **determine if the method used to gain access is persistent and reliable**. The end goal of an attacker is maintain elevated privilege or access to systems for future endeavors. Maintaining access to contaminated systems may also open doors to exploit future technologies, devices or hosts added to the infrastructure in the future.

### Covering up tracks

Have you ever known a nefarious actor or hacker who wanted to be caught? Through the duration of each phase of an attack, the attacker is **being especially careful to cover up tracks in order to prevent discovery**. Whether:

* Spoofing IP addresses, or;
* Passively scanning a network;

attackers will do everything in their power to remain anonymous. Less experienced hackers or script kiddies may not have the background or knowledge to **adequately escape detection or law enforcement**. Hackers commonly possess malicious intent with the end goal of financial gain. How can an attacker enjoy or profit from what they have stolen if they have been caught?

|  |
| --- |
| **The good guys must always stay at least 5 steps ahead of the bad guys!** |

## White, Grey and Black Hackers

|  |  |
| --- | --- |
| **What is a White Hat Hacker?** | A white hat hacker is also known as an ethical hacker or a person who practices hacking to assess security on systems, not to necessarily exploit them. |
| **Where does a Grey Hat Hacker come into play?** | A grey hat hacker is a person who does not possess intent to harm anyone or anything but is willing to break the law and bend the rules when necessary. |
| **So, I am guessing a Black Hat Hacker is probably not a good person?** | You are correct. Black hat hackers possess malicious intent and possess means, opportunity, and motive (MOM). Black hatters will do what they have to do in order to accomplish their goal. |

## Types of Testing

### White box testing

All knowledge of the systems, technology, enterprise architecture, personnel or operations are known. The attacker or ethical hacker initiates phases of the attack with all knowledge of the target(s).

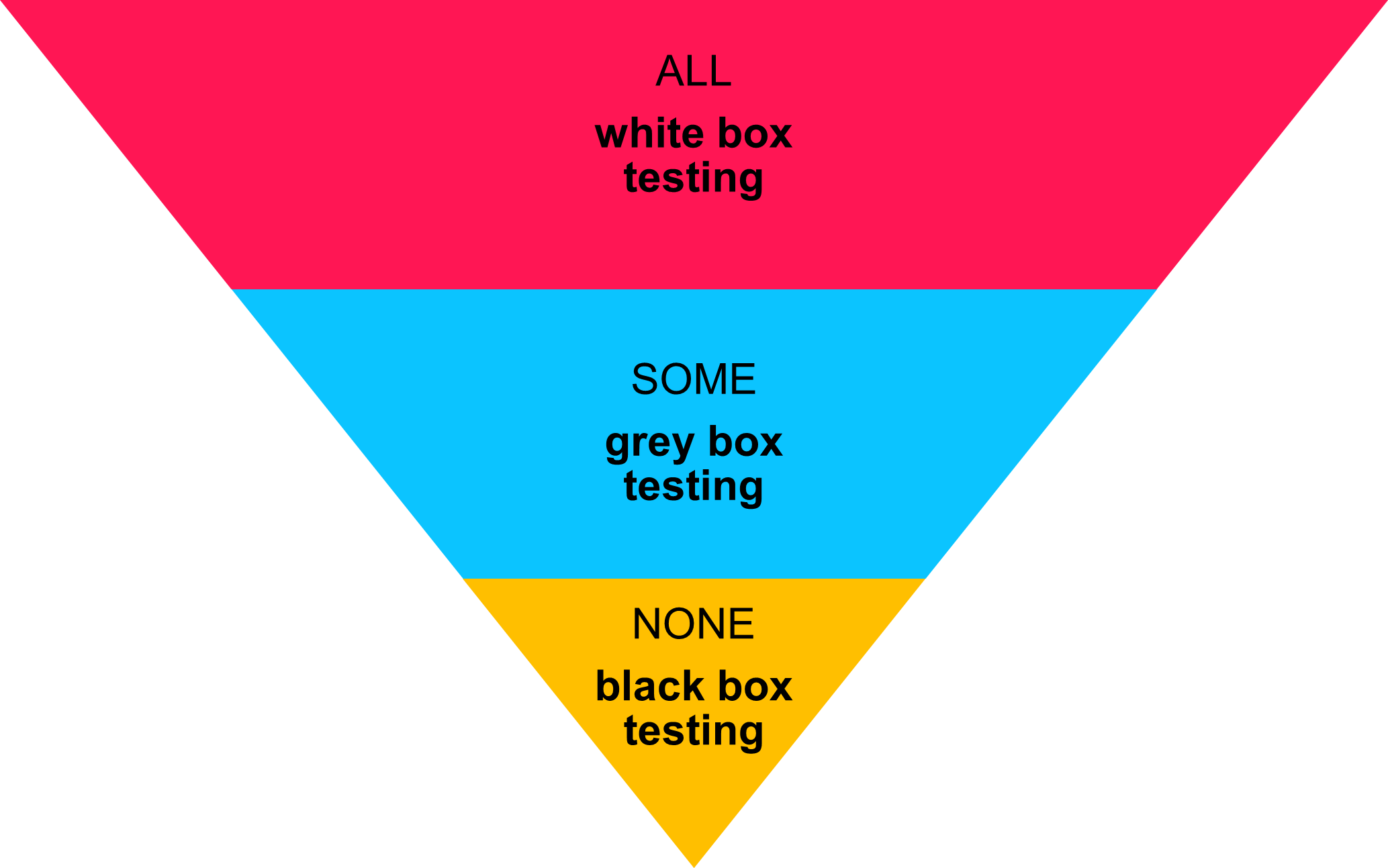
### Grey box testing

Some knowledge of the systems, technology, enterprise architecture, personnel or operations are known. The attacker or ethical hacker initiates phases of the attack with some knowledge of the target(s).

### Black box testing

No knowledge of the systems, technology, enterprise architecture, personnel or operations are known. The attacker or ethical hacker initiates phases of the attack with zero knowledge of the target(s).

**Figure 2. Different Types of Testing**



A close-up of a magnifying glass

Description automatically generated with medium confidence

Host compromise through means of malware is no situation anyone wants to find themselves in. As a cybersecurity architect, you must understand how malware executes, spreads and is identified. While several tools and methods exist to dissect malware, you must first have a basic understanding of techniques. The two basic techniques for detecting malware are static and dynamic analysis.

|  |  |
| --- | --- |
| Static Analysis Static Analysis is looking at a file or piece of software to determine whether or not the file has malicious intent. This analysis technique is done without reviewing the code of the file or application. This method provides means for studying the functionality and intent of a file in question, without actual execution. Some examples of information gathered during static analysis includes but is not limited to: the name of files or software, the type of file, MD5 info (hashes/checksums) and size of the file. | Dynamic Analysis Dynamic analysis on the other hand actually runs software or an executable file that is determined to be malware. The behavior of the malware is studied to determine any patterns, intent or purpose behind the malware. Some examples of information gathered during dynamic analysis includes but is not limited to: IP addresses, locations of files (paths), domain info, registry keys and more. |

## Understanding Malware

As a reminder, the word malware is actually derived from two words: malicious (mal) software (ware). As indicated by its name, malware is any program, software or code that has been created for malicious intent. There are various types of malware, distinguishable by several traits which will be discussed in great detail further in the course.

## Tools for Malware Analysis

While in theory malware can be dissected piece by piece, many do not have the time or patience to do so (unless this happens to be your job). While performing malware analysis is both important and necessary, there are options to ease the process. The development of several open-source tools provide the ability for hasty and detailed analysis.

A picture containing text, screenshot

Description automatically generated

Here are a few examples of many tools available for use:

|  |
| --- |
| **Google Rapid Response**  This tool, based off an incident response framework, focuses on remote live forensics. There is a server infrastructure, graphical user interface and API endpoint to review harvested data. A separate client is installed on systems you wish to investigate.  [Learn more about Google Rapid Response](https://grr-doc.readthedocs.io/en/v3.2.1/what-is-grr.html) |
| **Bro**  Bro utilizes signature and anomaly detection methods for analyzing network traffic. This tool has the ability to support forensics investigation, monitoring of network traffic for indicators of malware creating suspicious trends or patterns and means for protocol analysis.  [Learn more about Bro](https://bricata.com/blog/what-is-bro-ids/) |
| **Cuckoo Sandbox**  The cuckoo Sandbox provides automated file analyzing, specifically for Malware analysis. This tool expedites the tedious process of analyzing every aspect of a potential malicious file manually. It is customizable and offers several extensions to support multiple malware analysis endeavors.  [Learn more about Cuckoo Sandbox](https://cuckoosandbox.org/) |
| **Yara Rules**  Yet Another Recursive Acronym (Yara) adds on to the capabilities of Cuckoo Sandbox. Yara is a malware attribution tool that takes information on malware analysis from cuckoo and classifies it. This tool is mainly used to categorize and identify malware similar in nature.  [Learn more about Yara Rules](https://virustotal.github.io/yara/) |

# Lecture: Vulnerability Impact

**Content Author:**Dr. Michael J. Simko

Understanding the impact of vulnerabilities is necessary for accurately assessing organizational risk. In order to quantify or measure the impact of vulnerabilities, we must utilize a scoring methodology. This lecture is going to explore a method of ranking vulnerabilities based off several factors. Once a vulnerability has been ranked using the Common Vulnerability Scoring System (CVSS), a category 1, 2, or 3 rating may be assigned. A category 1 rating is a critical or high risk/severity, a category 2 rating is medium, and a category 3 rating is low.

There are three contributing factors towards calculating vulnerabilities rank: Base, Temporal & Environmental Scores.

|  |  |  |
| --- | --- | --- |
| **1. Base Score** | **2. Temporal Score** | **3. Environmental Score** |
| The base score assesses the damage that could result from exploitation and how easy it is to actually exploit the vulnerability. The base score further utilizes exploitability and impact sub-scores.   * **Exploitability Sub-score** takes into account qualities of a vulnerable component or how likely the vulnerability is to be exploited. Several metrics are used to calculate the exploitability sub-score:   + Attack Vector (AV) discusses how easily the vulnerability can be accessed by an attacker.   + Attack Complexity (AC) describes necessary existing conditions that the attacker does not control to exploit the vulnerability.   + User Interaction (UI) determines if multiple users are necessary in order for the attack to be a success.   + Privileges Required (PR) identifies the level of privilege required prior to exploiting the vulnerability. * **Impact Sub-score** determines how specific properties of the target will be affected if the exploit is successful. Impact of the vulnerability is further measured by the Authorization Scope. This scope consists of three areas:   + Confidentiality (C) translates to the amount of authority an exploited vulnerability may provide.   + Integrity (I) refers to the amount of corruption an exploited vulnerability may implement.   + Availability (A) is a measure of lost resources and services due to the vulnerability being exploited. | The temporal score ranks the awareness level of the vulnerability, known remediation steps and determines if threat actors are actively targeting the vulnerability. The temporal score calculation relies on three metrics:   * **Exploit Code Maturity (E)** determines the likeliness a vulnerability will successfully be exploited. This is normally based on exploit kits and coding pertaining to the vulnerability that has already been discovered. * **Remediation Level (RL)** determines how easy or difficult it may be to fix the vulnerability. RL can be viewed as a counterpoint to Exploit Code Maturity. * **Report Confidence (RC)** is the level of confidence correlating to the vulnerability's existence. This actually verifies the vulnerability is real and not rumor. | The Environmental Score is particular to work environments within specific organizations. This would be distinct for each organization conducting common vulnerability scoring and ranking. The Environmental Score is broken down into a security requirements sub-score and modified base score.   * **Security Requirements Sub-score** is a score based off confidentiality, integrity and availability metrics derived from the "impact sub-score." These metrics are determined based off the specific organization and environment being looked at. * **Modified Base Score** reevaluates all metrics within to "base score" to take into account specifics of the organization and environment being evaluated. |

### Final Scores

Upon ranking or scoring the Base, Temporal, and Environmental Scores, values are assigned to determine the potential impact and severity a vulnerability may have. The scores are measured on a ten-point scale:

0.0 implies **no** risk

0.1 to 3.9 is determined as **low** risk

4.0 to 6.9 is a **medium** risk

7.0 to 8.9 is **high** risk

9.0 to 10.0 is scored as **critical** risk

Chart, sunburst chart

Description automatically generated

You can review [details and tutorials on CVSS](https://www.first.org/cvss/) or experiment with an [automated CVSS calculator](https://www.first.org/cvss/calculator/3.0).

# Lecture: Incident Response

**Content Author**: Dr. Michael J. Simko

**Incident response** is the ability of an individual or team to react to an issue, compromise, disaster or any scenario that could cause harm. The ability to resolve issues in a hasty manner is a must, but is difficult without an established procedure and training. Incident response plans (IRPs) lay down the foundation of what should happen following identification of an incident.  
  
This lecture is going to focus on how to develop an actual incident response plan from scratch.

**Now, let's discuss a few of the steps involved in the development of the incident response plan itself!**

|  |  |
| --- | --- |
| Icon  Description automatically generated | Define the Scope of the Plan  * Determine what the incident response plan will be applicable to. Will the plan only pertain to the information technology department? Will the human resources department follow the same plan? * Define the scope and limitations of the plan. The scope of the plan should be particular to a specific data center, building or business process. * Ensure you plan is clear and comprehensible by all employees of the organization. |

|  |  |
| --- | --- |
| Icon  Description automatically generated | Establish a Process The phases of incident response involve preparation, detection, response, investigation, containment, eradication, remediation, and lessons learned.  Each phase should be broken down into processes. Let's use the 'first detection of an incident' as an example:   1. Determine whether the incident requires action or initiation of the IRP. 2. Assess and analyze the scenario incident. 3. Formally document the incident either by paper or electronically. 4. Determine the impact of the incident to the specific environment. 5. Classify the incident by type of incident and how severe it is 6. Assign the incident to the team lead. 7. Delegate incident responders for action. |

|  |  |
| --- | --- |
| Icon  Description automatically generated | Determine Key Stakeholders and Implement Training Similar to business continuity and disaster recovery, you need to identify key individuals who are applicable to each incident. If the incident pertains to malware, you are not going to need an incident responder from legal or budget. You should begin by categorizing groups by different roles or functions. Ensure each individual is trained on both their role and expectations regarding the plan.  Few examples of possible groups you may want to include:   * The Actual Incident Responders - The personnel taking action or charge of the incident. * Leadership - For making those tough decisions. * Technical Personnel - Information Technology and Cybersecurity subject matter experts. * Customers - May be applicable to participate in the event incidents are customer-impacting. |

|  |  |
| --- | --- |
| Icon  Description automatically generated | Define Severity Levels  * Categorize different severity levels numerically. For example, identify a scale of severity with five being the most detrimental to the organization while a severity of one is not a major concern. * Determine the appropriate scale of severity based off your organization and the amount of impact each incident may have on critical business processes and daily operations. |

|  |  |
| --- | --- |
| A picture containing icon  Description automatically generated | Establish a Communications Strategy  * Determine who the first responder should contact. How should communication flow throughout the incident response plan? * Do all participants have a centralized method or location to store data and notes regarding the incident? * Your plan and training should identify who to communicate with, what to communicate, when and how frequently to communicate, and where to record communication at various phases. * It is recommended to implement an automated security alert or notification system so that all employees in the organization are aware an incident has occurred and are advised on how to react. |

|  |  |
| --- | --- |
|  | Analyze Various Incident Scenarios  * Develop different playbooks or plans for each scenario. Make the multiple playbooks tailored to realistic incidents that could possibly harm your organization. * Having a generic incident response plan is great but brainstorming with several employees can help identify multiple scenarios that your organization may specifically encounter. |

|  |  |
| --- | --- |
| Icon  Description automatically generated | Plan Testing and Continuous Improvement  * Schedule frequent simulated scenarios to ensure your plan does not become obsolete. Running through various scenarios and testing each playbook you establish will only identify opportunities for improvement, enhance your plan and educate key players through repletion. * Ensure after action reports and lessons learned are addressed with each exercise. |

# Lecture: SysInternal Tools

**Content Author:** Dr. Michael J. Simko

|  |  |
| --- | --- |
| A picture containing icon  Description automatically generated | What exactly are SysInternal tools? **Sysinternals** are Microsoft Windows administration tools, most of which are built into the Microsoft Windows Server platform. Many of the tools can be downloaded from the Microsoft website, loaded onto a portable drive and used on the go for various administration requirements. During this lecture, we are going to address a few of tools available for system security, monitoring and hardening. It is important to note there are individual Sysinternal tools and Sysinternal suites available for use depending upon your intent. Microsoft's website offers an ample amount of tools available for use and download. |

**Now let's discuss some specific Sysinternal tools...**

|  |  |
| --- | --- |
| **AccessChk** | a tool that administrators can utilize to audit access. The tool possesses the ability to check both group and user permissions regarding data, registry keys, Window services, directories and more. This is a great tool to stream user and group permission modification or auditing. |
| **Autoruns** | provides a list of programs that will start up when the system boots. A list of registry and file locations are provided with each corresponding program that automatically starts at boot up. Autoruns can make you aware of any suspicious programs that may be running in the background of your system. |
| **AccessEnum** | a tool capable of providing a current snapshot of both registry and file system security configurations. The tool will specifically identify any loopholes or gaps that are overlooked, allowing the administrator to modify permissions as applicable. |
| **DiskMon** | a tool that can be utilized to monitor hard drive activity. This tool may be helpful in identifying any suspicious activity on your system, with logging capabilities. |
| **ListDLLs** | provides a report of DLLs in processes and may be used to scan for unassigned DLLs. It provides the ability to list all DLLs either by all processes or a specific process or DLL. It can even view digital signatures and detailed information on DLLs. |
| **AdExplorer** | or Active Directory (AD) explorer allows an administrator to view and navigate AD locations, properties, databases and attributes without the requirement of completing multiple steps. In a sense, it simplifies AD navigation and editing with the helpful ability to save snapshots for review later on. |
| **LogonSessions** | provides a quick list of all current active login sessions and even provides the ability to break down processes being ran in each session. |
| **Process Explorer** | provides a more detailed breakdown of running processes, owning accounts of each process and associated information. DLL mode offers the ability to view DLLs and memory-mapped files that each process has loaded. |
| **Process Monitor** | allows an administrator to view real-time activity of the file system, process and thread activity and the registry. The tool actually merges two other Sysinternal utilities (Filemon and Regmon) providing many additional capabilities. |
| **PsLoggedOn** | yet another tool for determining resource usage on a system and to whom the usage is associated with. This tool will search the network neighborhood and provide locally logged on users. It also has the ability to provide users logged on through means of resources both either a local or remote machine. |
| **PsFile** | a command line tool that lets the administrator view files that are opened remotely. |
| **PsInfo** | allows an administrator to harvest key information regarding a specific local or remote system. |
| **PsLogList** | provides a quick dump of event logs. |
| **PsPing** | provides ping functionality, but more importantly has the ability to measure latency and bandwidth. This can assist an administrator in narrowing down the root cause of an issue or potential live network attacks. |
| **TCPView** | affords the opportunity to review the state of TCP connections, detailed information on TCP and UDP endpoints and the name of the process that owns the endpoint. This program is considered a subset of Netstat with the ability to provide a more detailed and comprehendible report. The tool also comes with a command line version called Tcpvcon. |
| **Sigcheck** | a tool that can validate whether or not system images are digitally signed. |
| **VMMap** | a tool used for physical and virtual memory analysis. VMMap not only provides a breakdown of each process's committed virtual memory, but also presents the amount of physical memory assigned by the actual operating system (OS). |
| **RegDelNull** | is a tool available for administrators to remove registry keys that are undeletable by common registry editing tools. It offers the ability to both scan and delete registry keys containing embedded null-characters. |

While there are many Sysinternals tools presented and available for use, I have not met many administrators in the field who have actually known of all their capabilities and used them all. I would highly recommend looking at Sysinternals further in depth, as these tools are meant to simplify both system hardening, monitoring and auditing. Furthermore, an excellent book I would recommend, covering more advanced Sysinternal capabilities is: Troubleshooting with the Windows Sysinternals Tools (2nd ed.) by Mark Russinovich and Aaron Margosis.

# Lecture: Secure Systems Design

**Content Author:** Dr. Michael J. Simko

|  |  |
| --- | --- |
| A picture containing text, person  Description automatically generated | Implementing security into the initial requirements and design phases of any project should be a common train of thought for a cybersecurity architect. It is much easier to include and justify the requirement and funding for security during the initial phases, rather than later on when hardware is already in production.  It is imperative to understand the difference between design and development. The design phase is actually implemented with the system development lifecycle (SLDC). Development is ongoing through multiple phases often flowing from the requirements phase, to design, to implementation, to verification and then ongoing maintenance.  Several frameworks are available for secure-system design to include the Common Criteria and ISO/IEC 21827 (SSE-CMM). |

|  |  |
| --- | --- |
| Shape  Description automatically generated with low confidence | See if you can find several secure-system design frameworks online and compare the differences. |

## Principles of Secure Systems Design

|  |
| --- |
| The US Cert has noted several guidelines for system development. Some preventative measures are common sense while others are simply taken for granted. Understanding some of the foundational security design principles will truly make you stand out as a cybersecurity architect. We will now discuss some primary system design principles and their applicability to real life scenarios you will run into on the job. |
| **Primary System Design Principles**   * Defense in Depth * Least privilege * Privacy * Separation of duties and privilege * Fail safe * The weakest link |

**Defense in depth**

involves creating several layers of security on the job. In other words, an example of this could be establishing a firewall, host-based security system, antivirus protection and access control lists. There are several layers of security established in the event one layer is breached.

**Least privilege**

refers to granting permissions or administrative privileges to employees pertaining to their role or job only. They do not need permissions to every device on the network. An example of this would be a network administrator having administrative permissions to a switch, while a system administrator would have administrative access to a server.

**Privacy**

involves classifying data or information correctly and configuring folder or file access appropriately. The separation of duties and privileges is similar to the example provided above with the network administrator and system administrator. The network admin will have access to switches not servers based on his/her duties, while the system admin will have access to servers, not switches.

**Separation of duties and privilege**

is similar to the example provided above with the network administrator and system administrator. The network admin will have access to switches not servers based on his/her duties, while the system admin will have access to servers, not switches.

**A fail safe**

is a countermeasure. For example, if someone who doesn't have access to a folder somehow gains access to the folder, encrypting the files in the folder would serve as a fail-safe.

**The weakest link**

in cybersecurity typically deals with people. Many breaches or successful exploits are a result of an employee accidentally clicking a malicious link or not being trained on cybersecurity best practices. Annual cyber awareness training is the best way to help mitigate employee mistakes that could potentially lead to cyber breaches.

## Techniques for Secure Systems Design

|  |
| --- |
| Several techniques are available for implementing principles of secure systems design. We will always come across security concerns in which we may not be able to fully mitigate. Utilizing a compensating control or alternative method to reduce the likeliness of a threat or incident occurring is absolutely necessary. Some of the techniques below can be used to enforce secure systems design in the event funding for hardware and software security is not feasible during the SLDC design phase. |
| **Primary Systems Design Techniques**   * Threat modeling * Risk and vulnerability assessments * Secure coding/code review * Multiple levels of security * Access controls * Cryptographic solutions |

**Threat modeling**

was previously discussed in week 2. Threat modeling is the process in which you would specifically identify threats and countermeasures to mitigate threats.

**Risk and vulnerability assessments**

help identify potential security issues or conflicts such as the risk of a system being breached if not updated or software vulnerabilities that open up attack vectors or the potential for exploitation of known vulnerabilities.

**Secure coding or code review**

is a process programmers conducting after writing software or code to ensure there are no open doors or means of a nefarious actor manipulating the code to exploit the software, system, or application.

**Multiple levels of security**

are just another way of describing defense in depth. Both are often associated with layers and compared to how an onion possesses several layers.

**Access controls**

can be physical or logical. Access control lists on a network control the flow of traffic and what ports are utilized (open or closed) on a network. Access control pertaining to physical security involves carded access (using a CAC, PIV, or PIN) to access perhaps a data center or facility where critical infrastructure is housed.

**Cryptographic solutions**

correlate to encryption and methods of securing data, network traffic, messages, and more.

# Lecture: Embedded System Security

**Content Author:** Dr. Michael J. Simko



When embedded system security crosses my mind, I instantly associate central processing units (CPUs) to the term. Although this is a good example of an embedded system, embedded systems can pertain to many types of:

* Personal computing devices
* Modern day automobiles
* Mobile phones
* Industrial control systems, and even;
* Standard kitchen appliances.

An embedded system is actually **anything inside of a piece of technology that has the role of performing a specific function**. This may seem rather broad with the amount of technology implemented in nearly every device nowadays, however, **it is our duty as cybersecurity architects to defend all genres of embedded systems to the best of our ability**.

|  |  |
| --- | --- |
| Programming and Industry Best Security Practice Utilizing secure programming languages and programming methods is a must. **MISRA or Cert-C are highly encouraged coding methodologies** and defined practices for implementing security in software development. Embedded software developers should obviously not only adhere to established coding practice, but also ensure code reviews and best security practices are enforced during the early stages of software design and development. |  |
| ARM TrustZone ARM TrustZone can be used on any ARM Cortex-based processors. It is an embedded security solution in which two different environments (secure and unsecure) can function on one core. The ARM TrustZone solution **offers the option for secure boot while protecting processors from the physical layer and up**. | Diagram  Description automatically generated  [ARMTRUSTZONE Image Source](https://community.arm.com/support-forums/f/architectures-and-processors-forum/7979/what-is-trustzone-for-armv8-m) |
| Firmware Updates: Digitally Signing & Encrypting Digitally signing and encrypting firmware ensures **only trusted and approved firmware is updated and integrated into organizational equipment**. Establishing a process during the initial development will be beneficial to hardware requiring frequent firmware upgrades, as many firmware updates are either automatic or just not known (no indicators there is a new version). |  |
| Monitoring Buffer & Stack for Indicators of Overflow A buffer overflow attack is **an attack that forces an amount of data into a fixed size buffer, overflowing the buffer with more than it can handle**. The excess data is pushed into other areas often either corrupting data or overwriting existing data. Ensuring buffer or stack space is monitored on a frequent basis will assist in identifying buffer overflow or attempts to inject malicious code. | A glass of water falling into water  Description automatically generated with low confidence  [Overflowing Water Image Source](https://countuponsecurity.com/2016/04/11/evolution-of-stack-based-buffer-overflows/) |
| Locking Flash Space Locking flash will not completely stop a motivated attacker, however, doing so will make it **more difficult to retrieve application code**. Flash program space should be off limits as an insider threat could gain physical access and attempt to reverse engineer application code. |  |
| Meltdown & Spectre If you follow current vulnerabilities and trends, there is a chance you may have heard of Meltdown and Spectre. Both are examples of vulnerabilities pertaining to microprocessors that have been manufactured in the previous twenty years. The vulnerabilities actually exploit two main functions of CPUs: caching and speculative execution. **Caching** is used to enhance the speed at which memory is accessed, while **speculative execution** is a technique processors use to anticipate future actions for enhancing speed (based off past actions). The relevance of these vulnerabilities is not only applicable to computers, but nearly any device that utilizes a processor.  What does this mean for our organizations? Well, the majority of organizations survive and function off computers, mobile phones, multi-function printing devices and more. Although this vulnerability is difficult to patch due to being hardware based, patches have been released by multiples vendors to help implement work arounds and compensating controls. | A picture containing shape  Description automatically generated  [Meltdown Spectre Image Source](https://www.csail.mit.edu/news/better-approach-preventing-meltdownspectre-attacks) |

## The Challenges of Securing Embedded Systems

As we discussed, embedded systems are devices that serve a specific function within many devices. Embedded device security is often taken for granted as many of the preventative measures enforced are specific to software vulnerabilities.

* Some devices have the ability to provide a notification when a firmware update is available, however, many do not.
* Many antivirus and anti-malware tools do not have the ability to scan for embedded system vulnerabilities. For example, industrial protocols are used by embedded systems but security devices such as firewalls, IDS's, IPS's, etc., do not possess the ability to recognize industrial protocol attacks.

Embedded systems are used for many of the necessities not commonly thought about. For example:

* Power grids
* Water treatment facilities
* Infrastructure for transportation
* Communication systems (data and voice)
* HVAC

...and more rely upon some type of embedded system configuration. A large challenge involves most of this equipment being developed many years ago and categorized as legacy equipment. Think about how detrimental a cyberattack would be to any of these critical services we rely upon.

Now that you are aware of the importance of embedded system security and have the ability to identify several examples of embedded devices; you can help your organization manage security and accountability of these devices.

The modern-day cybersecurity architect should not only analyze potential attack vectors pertaining to embedded systems but utilize the risk management process and methodology to mitigate as many security issues as possible. Remember, these systems were built for a specific purpose. Understanding the purpose of an embedded system will help you implement the best security for each of these devices.

# Lecture: Dynamic Naming Standards

**Content Author:** Dr. Michael J. Simko

Why is assigning a name to a network device so important?

Naming conventions are for:

* Organizing different devices
* Categorizing different devices based off their type
* Identifying locations
* Specifying how many devices are on a network
* Specifying types on a network

Please watch the following video on Key Locations:

[Transcript for Video: Key Locations (opens in a new window)](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week04/mp4-FA21-DynamicNamingStandardsAndNetworkUniformity/TranscriptForVideo1.html)

Naming standards are not only pertinent to device uniformity and management but assist in both change and asset management procedures.

Since our devices will all be communicating across the enterprise, we need to differentiate which servers, switches, and routers belong to each location. We would include an indicator such as an abbreviation of the location in the naming standard.

|  |  |  |  |
| --- | --- | --- | --- |
| **Detroit**  **DE** | **Los Angeles**  **LA** | **Las Vegas**  **LV** | **New York**  **NY** |

Next we would want to include some type of building or room indicator. In this case, let's say we are talking about a device in Los Angeles, we will use building 4, and this device is physically located in room 26.

We add delimiters or a dash, to differentiate between data sets in the name.

|  |
| --- |
| **LA-BLDG4-RM26** |

Please watch the following video on Specific Device Types:

[Transcript for Video: Specific Device Types (opens in a new window)](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week04/mp4-FA21-DynamicNamingStandardsAndNetworkUniformity/TranscriptForVideo2.html)

Now lets talk about clarifying devices. We can differentiate by letters within the name of the device.

|  |
| --- |
| **C** = Cluster Server **V** = Virtual **DC** = Domain Controller **FS** = File Server **PS** = Print Server **CTX** = Citrix Server **ORA** = Oracle Database **SQL** = SQL Database **ESX** = Vmware ESX **SW** = Switch **RT** = Router |

For the purpose of this exercise, let's say our device is a print server. We use 4 print servers at your location, so this specific print server is number 3. Now let's add that to our city location and building number to indicate this device will be print server number 3.

|  |
| --- |
| **LA-BLDG4-RM26-PS3** |

Please watch the following video on Specifying Device Model:

[Transcript for Video: Specifying Device Model (opens in a new window)](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week04/mp4-FA21-DynamicNamingStandardsAndNetworkUniformity/TranscriptForVideo3.html)

In this scenario, let's say this server is a Dell Power Edge R440.Why might we want to add the model number? Well...good question. Adding the model number can assist in inventories conducted via the network to establish what devices are approaching end of life or are eligible for technical refresh.

|  |
| --- |
| **LA-BLDG4-RM26-PS3-DELLPE440** |

Additionally, say a vulnerability is identified on this specific model of server. We now are able to tell which servers are applicable to this vulnerability and patch them remotely via the network. If we push the specific fix for this individual server out to other server vendors or models, we risk the possibility of breaking them.

Please watch the following video on Negating Duplicates:

[Transcript for Video: Negating Duplicates (opens in a new window)](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week04/mp4-FA21-DynamicNamingStandardsAndNetworkUniformity/TranscriptForVideo4.html)

|  |  |
| --- | --- |
| A picture containing person, indoor, work-clothing  Description automatically generated | It's very important to maintain accountability of networking devices. Implementing the standard procedure we just used to name a device should be uniform. Uniformity will prevent duplicates on the network.  We don't want the issue of duplicates because two devices with the same name or IP address will conflict, preventing one or both of the devices from performing their intended functions. I have seen this happen more than a few times on the job, especially with printers. Somewhere along the line printers were taken offline and replaced by new printers without anything being updated.  This is mainly a failure on change management. As printers or devices come and go, there should not only be a change management process, but the master asset list or inventory should be updated frequently. |

# Lecture: Data Loss Prevention

**Content Author:** Dr. Michael J. Simko

## What is Data Loss Prevention?

You may have heard a lot in the news over the past few years about protecting personal and customer data. Data Loss Prevention (DLP) is an initiative any organization or company takes to safeguard company (trade secrets/intellectual property) and employee (personally identifiable) data. A DLP program also aims to prevent exposure of data to the outside world in the event of a breach. Take a few minutes to view the following video, summarizing Data Loss Prevention best practices:

## How is data leaked?

While there are many instances that may lead to data being leaked or exposed, there are primarily three.

1. An insider threat or employee with malicious intent (often attempting to seek financial gain or revenge after disciplinary action) is the most common means of data being stolen or leaked.
2. Cyber attacks from outside nefarious actors (exploiting vulnerabilities to gain access to data stored on company computer systems or servers) is the second.
3. Employees who make mistakes (unintentionally) exposing or releasing sensitive data is the third.

## What is required to implement DLP?

|  |
| --- |
| **Data in motion or data moving** from different devices across the network needs to be analyzed as it moves in and outside of the organization’s network. In other words, network traffic and data must be analyzed as it goes out from the organization’s intranet to the World Wide Web and analyzed again as it passes into the company’s intranet from the Internet. This is often accomplished by use of intrusion detection systems (IDS’s) or intrusion prevention systems (IPS’s). You may be wondering why you would analyze company data leaving the intranet (that was created internally)? This helps establish a baseline and teach IDS’s and IPS’s what data would be considered normal. |
| **Data at rest or data stored** on network or file shares within the organization must also be secure. This is often achieved by the “confidentiality” portion of the CIA triad and using encryption. Hard drives can be encrypted with Microsoft Bitlocker or several other encryption tools available for use. Additionally, a company must establish policy and procedure for data storage, use, and destruction. |

## DLP Functionality

DLP uses many methods to analyze traffic, files, or data that can assist in identifying anomalies or generating alerts to notify staff of breaches or of the “integrity” factor of the CIA triad being violated. When data is intentionally altered with malicious intent, it loses its integrity. Let’s discuss some different functions a good DLP solution provides.

* Configurations of Rules: Rules can be configured to identify specific criteria pertaining to credit card numbers, date of birth, identification numbers, or social security numbers. A rule would flag an alarm or block content that has not been approved to leave or enter the network. For example, a rule could identify 9-digit number combinations or formatting matched XXX-XX-XXXX, which would correlate to a social security number.
* Fingerprinting of Databases: A comparative analysis of data from an existing database or baseline. In other words, data is analyzed from an initial source to ensure validity and ensure data has not been altered.
* Statistical Analyzation: Bayesian analysis or artificial intelligence is utilized to identify any red flags pertaining to the validity of data.

## Improving DLP

While data loss prevention may seem very straightforward with similar processes for implementation across multiple industries, **continuous improvement is imperative**, as both technology and the availability of data grow. There are a few initiatives the organization can take to ensure their DLP program remains effective and adaptable:

|  |  |
| --- | --- |
| Icon  Description automatically generated | **Centralization**  Don’t create multiple efforts within an organization to safeguard data. A centralized approach is much more effective to ensure process is standardized across each department or section within the organization. A centralized approach negates inconsistencies and variations of how each department handles data. |
| Icon  Description automatically generated | **Educate Employees**  Ensure separation of duties and train employees on how data should be stored, transferred, transported, safeguarded, and destroyed. Implement training and awareness of external legal and regulatory requirements (such as General Data Protection Regulation (GDPR) requirements). |
| A black rectangle with a white rectangle in the middle  Description automatically generated with low confidence | **Classification**  Classify data appropriately. Identify different types of data to include unclassified, sensitive, and classified data. Establish a process for managing and storing each of the different data types and ensure the information systems storing the specific types of data are labeled clearly (with a physical label stating unclassified, sensitive, or classified). |

## What do you know?

Answer the following questions to find out how much you know. Alternately, you may review a [printable/accessible version of the DLP Activity](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week04/activity-FA22-DataLossPrevention/printable.html).

# Lecture: Cloud Models

**Content Author:** Dr. Michael J. Simko

Diagram, icon

Description automatically generated

By now, you are probably familiar with the term "cloud" often associated with many large companies such as Microsoft, Amazon, and Google, in which we have all come to know over the previous decades. Furthermore, Microsoft Office 365, Microsoft One Drive, and Microsoft TEAMs have helped evolve companies to the next level of enterprise architectural maturity. Let's talk about the three primary types of cloud models.

Icon

Description automatically generated

**Infrastructure as a Service (IaaS)**

Infrastructure as a Service is as it sounds, the infrastructure to perhaps build or run applications on. It is often servers or networks that provide the foundational infrastructure (virtually) to bring an idea to life on the cloud.

Benefits and Uses:

* Increased Availability: Redundant servers can be created at any location to provide contingency in the event of natural disasters.
* Enhanced performance: Data centers are spread out all over different states and countries. Connecting to the datacenter providing cloud services closest to the business, will provide less latency and increased performance.
* Security: Data centers hosting cloud services use advanced security configurations to protect the various types of data being stored. In most cases, they are required to by law!
* IaaS can be a great solution for disaster recovery initiatives, ecommerce solutions, small business website creation, Internet of Things (IoT) initiatives, and the development of software applications.

Icon

Description automatically generated

**Platform as a Service (PaaS)**

Platform as a Service refers to availability of a full "platform" or provides means for the creation or maintenance of software and applications on the cloud. The platform itself is readily available and on demand.

Benefits and Uses:

* Faster Development: employees partaking in software or application development are able to create, test, and implement production environments, which means quicker delivery to the market.
* Shared Environment: Collaboration is simplified, meaning employees developing content from several companies or locations are able to effectively work together anywhere they are able to access the internet.
* Scalability and Management: There is always the availability of purchasing more capacity to expand capabilities while the management of the infrastructure is on the cloud provider (installing patches and updates, storage expansion, configuration requirements, etc.).
* PaaS is great for development of application programming interfaces (APIs), IoT devices, Agile Development methods and DevOps methodologies.

Icon

Description automatically generated

**Software as a Service (SaaS)**

Software as a Service is associated with software or applications that are hosted on the cloud, on demand, and ready for use at any time.

Benefits and Uses:

* Low Risk: all infrastructure and applications are managed by the cloud vendor. Commitments are minimal with opportunities to test software with a free trial or small fee.
* High Availability: SaaS applications or infrastructure are available anywhere in the world via the internet.
* Scalability: Modifying access, expanding, or obtaining more capabilities (such as larger storage or additional software capabilities) is a click away.
* SaaS is great for any modern-day application, business, or even for use at home.

Take a moment to dive further into Cloud Computing Services Models by watching this video: