Unofficial Study Guide for CompTIA CySA+ Exam

EXAM NUMBER: CS0-001 | CREATED BY: AMY HEYEN

Defensive Stance SECURITY BLOG

1.0 THREAT MANAGEMENT

1.1 GIVEN A SCENARIO, APPLY ENVIRONMENTAL RECONNAISSANCE TECHNIQUES USING APPROPRIATE TOOLS AND PROCESSES.

TOPOLOGY DISCOVERY

A form of active reconnaissance that uses scanning tools like Nmap/Zenmap to send an ICMP Echo Request, a TCP SYN to port 443, a TCP ACK to port 80, and an ICMP Timestamp request by default across a network and see who responds. The results should generate a map of the network.

OS FINGERPRINTING

Some software like Nmap can guess the device's operating system. The key thing for the exam is to know that OS fingerprinting is not exact, variants of operating systems are hard to differentiate.

SERVICE DISCOVERY

A port scanner can probe a host or server to determine what ports are open. Since network devices run services on well-known ports, like 80 and 25, port scanning is reliable way to determine services.

PACKET CAPTURE

A packet sniffer or packet analyzer software (like Wireshark) puts the computer into promiscuous mode, and listens to all traffic. You can do a header capture: data about the data, faster scan or a full packet capture: need more storage, but may be able to reconstruct the content of the exchange.

LOG REVIEW

Logs can be pulled from various devices into a log reader tool for analysis.

- Firewall Logs: Report whether a packet is accepted, denied, or dropped.
- IDS/IPS Logs: Report any threat behavior detected (IDS) or blocked (IPS) and why.
- System Logs: Windows Event Logs and syslog (Non-Windows operating systems)
- Syslog Server: Network devices can forward their logs to a secured syslog server.

ROUTER/FIREWALL ACLS REVIEW

Network ACLs selectively permit or deny access for inbound and/or outbound traffic. Router ACLs may use the IP, network protocol, port or another feature to decide. Switches may use the IP or MAC address to decide. The order of ACLs matter, the first rule takes precedence. Review should be done periodically to ensure that best practices are still being upheld.

EMAIL HARVESTING

Process of collecting email addresses to use for a convincing phishing email or to compromise information systems.

SOCIAL MEDIA PROFILING

Where an attacker creates a profile for a target based on social media to determine their patterns and likely actions.

SOCIAL ENGINEERING

Attacker tricks target into revealing information or otherwise compromising a security system. Most commonly seen as phishing attacks.

DNS HARVESTING

Automation of tools like nslookup, host, and dig in command line to gain information about a network from the DNS server(s). Or using a zone transfer to copy all of the DNS server's records and map a network. Information obtained could be name servers, mail exchange records, or hostname and could be utilized in DNS poisoning or spoofing.

PHISHING

Phishing attacks are a form of social engineering. Their goal is to trick users into doing something that helps the attacker, such as clicking a link in an email or revealing information over the phone.

WIRELESS VS WIRED

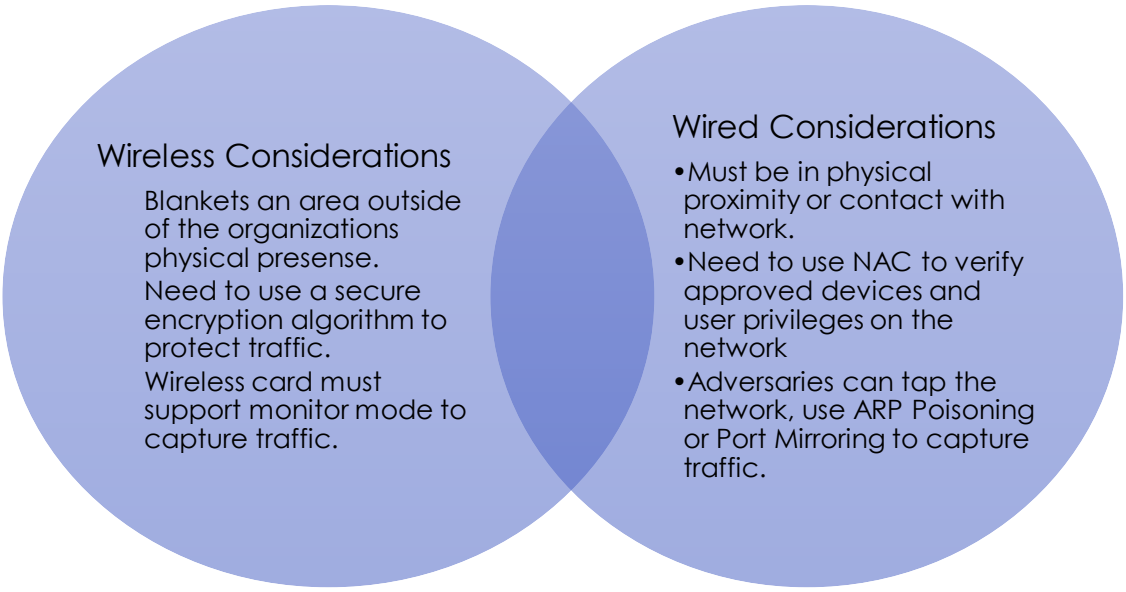


Figure 1 Wireless vs Wired Considerations for Reconnaissance

VIRTUAL VS PHSYCIAL

- Virtual: Increases the layers of security and agility of IT infrastructure. Many systems can be hosted by one physical system, which could be a single point of failure.
- Physical: More expensive to implement, but provides possibility of air gap (physical isolation).

INTERNAL VS EXTERNAL

- Internal: Has physical access to endpoint on the network, doesn't need to get past the firewall. Still needs to authorize and their activity can be identified through internal network monitoring.
- External: More anonymity through spoofing, but also more difficult to get past security measures.

ON-PREMISES VS CLOUD

- Cloud Services: Requires trust in service provider, no direct control over what happens.
- On-Premises: Allows direct control of security, but requires more expertise.

NMAP

Nmap is a network scanning tool runs in command line interface features host discovery, port scanning, version detection and OS fingerprinting. GUI version available is called Zenmap.

HOST SCANNING

A host scanning tool sends a message to a target system, and uses the response to provide detailed information about the system or continue exploring.

NETWORK MAPPING

Network mapping tools send a message to a target IP or range of IPs and its goal is to understand the topology including perimeters, DMZs and key devices such as web servers.

NETSTAT

A command-line utility tool that can output network connections, interface stats, listening ports, and PIDs. A common use would be: `netstat -l` the results will show all ports that are listening.

PACKET ANALYZER

Packet analyzers like Wireshark (GUI)/Tshark (CLI) capture packets across one or more network interfaces and allows for filtering, analysis and graphing of the results.

IDS/IPS

- Intrusion detection systems (IDS): A software or appliance that analyzes network events and identifies suspicious behaviors.
- Intrusion prevention systems (IPS): An IDS that quarantines hosts to prevent malicious activity.

HIDS/NIDS

- Host IDS (HIDS): Analyzes events on a single host to identify suspicious behaviors.
- Network IDS (NIDS): Analyzes events across a network to identify suspicious behaviors.

FIREWALL RULE-BASED AND LOGS

- Rule-based firewalls: Examines packets and denies traffic based on predetermined rules.
- Firewall Logs: Logs can be configured to be sure that pertinent information is recorded for any future incident. Typical log fields include: timestamp, source address, source port, destination address, destination port, protocol, IN interface, OUT interface, rule name, action taken.

SYSLOG

Syslog is the reporting standard for non-Windows device logs. Syslog can be configured to be stored on a secure server so that intruders have a harder time covering their tracks. Also many products will be able to take syslog and/or Windows event logs and aggregate them to one event log for review.

VULNERABILITY SCANNERS

- Nikto: Open source web server vulnerability scanner. Reports name of offending files and the Open Source Vulnerability Database (OSVDB)
- OWASP Zed Attack Proxy (ZAP): Open source web application vulnerability scanner also functions as web proxy for capture and manipulating traffic that passes through it.
- Nessus: Vulnerability scanner includes port scanning and comprehensive configuration check for vulnerabilities, misconfigurations, default passwords, and compliance level.

1.2 GIVEN A SCENARIO, ANALYZE THE RESULTS OF A NETWORK RECONNAISSANCE

POINT-IN-TIME DATA ANALYSIS

An incident response approach that looks at data pertaining to the time of the incident.

PACKET ANALYSIS

Packets have a ton of data that could create a timeline of a network event. The key to finding the data you need is using the correct filters. A full packet capture can be used in Wireshark to recreate a TCP steam and recover a malicious file that may have been downloaded. There are legal implications regarding privacy for full packet captures, consult your legal team first. Encryption will make the content incomprehensible, you'll need SSL proxies to capture the contents of an encrypted session.

PROTOCOL ANALYSIS

Analyzing the protocol used in a packet capture can reveal misuse of a protocol for malicious intent. Protocol analysis is also used to determine vulnerabilities in a program. If a session is encrypted, the protocol is still viewable in the header capture.

TRAFFIC ANALYSIS

Analyzing the source and destination of traffic or a change in the volume of traffic can be an early-warning technique to identify a compromised host. An open source tool to try is Etherape.

NETFLOW ANALYSIS

Provides statistics on traffic that is grouped by characteristics into the following "flows:" arrival interface at the network device, source and destination IP addresses, source and destination port numbers, IP protocol, & IP type of service.

WIRELESS ANALYSIS

The wireless interface must be in monitor mode to use WLAN analyzer such as Kismet. The goal is to map out WAPs and identify rogue access points. Rogue clients are difficult to identify due to MAC spoofing and so organizations should implement WPA Enterprise and IEEE 802.1x authentication

DATA CORRELATION AND ANALYTICS

An approach of looking at collections of data to find patterns that correspond to an event.

ANOMALY ANALYSIS

Focuses on deviation from *baseline* and determining whether it is significant enough to investigate.

TREND ANALYSIS

Study of patterns over time to determine how, when and why they change. Security firms publish their trend analyses of adversaries and make projections for the next year.

AVAILABILITY ANALYSIS

Process of determining the likelihood that systems will be available to authorized users in different scenarios. Results are used in determining budget to put towards defending availability.

HEURISTIC ANALYSIS

Using known information on behaviors to create rules of thumb or heuristics, then use those rules to identify threats. Commonly used by Next-Generation Firewalls (NGF) to identify incoming malware or other threats for further investigation.

BEHAVIORAL ANALYSIS

Similar to anomaly analysis by leveraging baselines to determine suspicious events for further investigation, but considers multiple factors such as size, destination and time of day.

FIREWALL LOGS OUTPUT

Firewall logs output can be configured to ensure data stored would be relevant for incident response.

Typical Firewall Log Fields

Field	Descriptions
Timestamp	Data and time packet was logged
Source address	IP address of the source of the packet
Source port	Port number at the source
Destination address	IP address of the destination of the packet
Destination port	Port number at the destination
Protocol	IP Protocol of the packet (e.g. TCP, UDP, or ICMP)
IN interface	Firewall interface that received the packet
OUT interface	Firewall interface that forwarded the packet (unless denied or dropped)
Rule name	Firewall rule that was applied to the packet
Action	Action taken by the firewall (e.g. accept, deny or drop)

Table 1 Firewall Log Fields

PACKET CAPTURE RESULTS

Review packet structure for IPv4 (IETF RFC 791) and IPv6 (IETF RFC 2460 & its update RFC 5871).

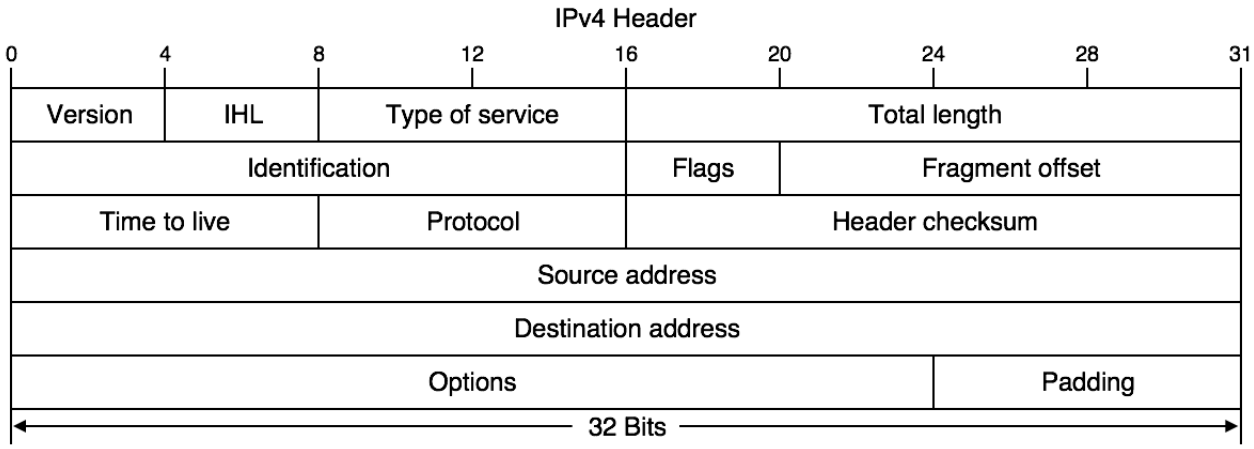


Figure 2 IPv4 Header Fields

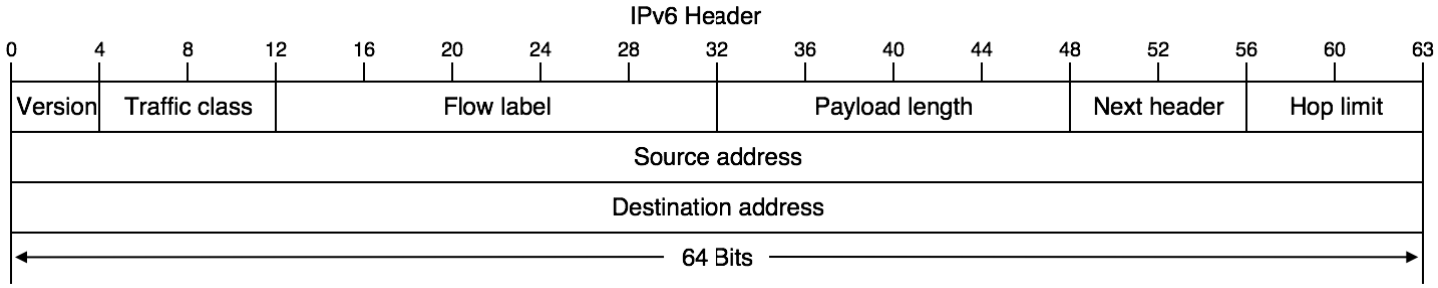


Figure 3 IPv6 Header Fields

NMAP SCAN RESULTS

Nmap outputs open ports on a target, and the service associated with that port. Review well known ports and Nmap's guide for understanding logs. Example:

```
PORT     STATE SERVICE
135/TCP  open  msrpc
139/TCP  open  netbios-ssn
445/tcp  open  Microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
5800/tcp open  vnc-http
5900/tcp open. Vnc
MAC Address: 00:15:5D:XX:XX:XX (Microsoft)
```

EVENT LOGS

Windows event logs are a standardized format for Windows programs/systems. Here are some of the logs that you would encounter as described in ManageEngine's tutorial.

Windows Event Logs

Event Log Type	Description
Application Log	Any event logged by an application. These are determined by the developers while developing the application. E.g.: An error while starting an application gets recorded in Application Log.
System Log	Any event logged by the Operating System. E.g.: Failure to start a drive during startup is logged under System Logs
Security Log	Any event that matters about the security of the system. E.g.: valid and invalid Logins and logoffs, any file deletion etc. are logged under this category.

Directory Service log	records events of AD. This log is available only on domain controllers.
DNS Server log	records events for DNS servers and name resolutions. This log is available only for DNS servers
File replication service log	records events of domain controller replication This log is available only on domain controllers.

Table 2 Windows Event Logs

SYSLOG DATA

Syslogs are a standard logging format for systems/programs as described in IETF's RFC5424. These logs can be configured to be stored in a remote secured server and compiled by log tools to easily review logs from multiple sources at once.

IDS REPORT DATA

IDS use rules to determine threats. In these rules, the message that will be recorded if an action is taken is also defined. Each time an IDS identifies a threat whether signature or anomaly based, it will create a log of the threat detected and why.

SIEM TOOLS

- Splunk: Accepts data from virtually any source, and then indexes and stores that data. The data can be processed by a heavy forwarder before sent to its indexer so that big data is condensed to smaller, more relevant data. Splunk also has a web-based front end used to search and view the data with a dashboard type screen.
- ELK: A collection of open source java based tools called Elasticsearch, Logstash, & Kibana. Elasticsearch indexes data to allow quick searching. Logstash is a data processing pipeline that will remove PII and forward to data store. Kibana performs visualization of data and reporting.

PACKET ANALYZER TOOLS

Packet analyzers like Wireshark (GUI)/Tshark (CLI) capture packets across one or more network interfaces and allows for filtering, analysis and graphing of the results.

IDS/IPS TOOLS

- Snort: Popular NIDS but also can work as a packet analyzer or NIPS. Snort uses a customizable rules language to identify threats. Clients can subscribe to threat intelligence agencies and receive new signature rules as they're released.
- Bro: Bro-IDS is signature & anomaly based. Instead of just analyzing a packet to see if it fits within a rule, it will monitor sessions and retain data for forensic investigations. Uses policies to determine if sessions or events are anomalous, can also be used as an IPS.
- Suricata: IDS/IPS that is multithreaded and can use Snort signatures but with added hardware acceleration to process packets. Can also pull files from sessions like Bro.

RESOURCE MONITORING TOOLS

Resource monitoring tools like Nagios Core will monitor hardware metrics like disk or CPU utilization, and will log events such as major changes in utilization and then send a notification and can also take predetermined steps to try and resolve the issue.

NETFLOW ANALYZERS

Netflow analyzers can aggregate NetFlow data from devices into an analysis console used to monitor and query for detailed information. Some software like ntopng can also monitor other network metrics that aren't included in NetFlow data.

1.3 GIVEN A NETWORK-BASED THREAT, IMPLEMENT OR RECOMMEND THE APPROPRIATE RESPONSE OR COUNTERMEASURE

NETWORK SEGMENTATION

The goals of network segmentation are to thwart adversaries, improve traffic management, and prevent spillover of sensitive data. This should be achieved through each layer of the network stack from physical link to application layer. VLANs are not enough.

- System Isolation: The use of additional policies in addition to segmentation plan for sensitive systems. Ideally start with an *air gap*, but if that isn't possible, ACLs can be used.
- Jump Box: Or Jump server is a specifically configured machine used to connect to secured parts of the network.

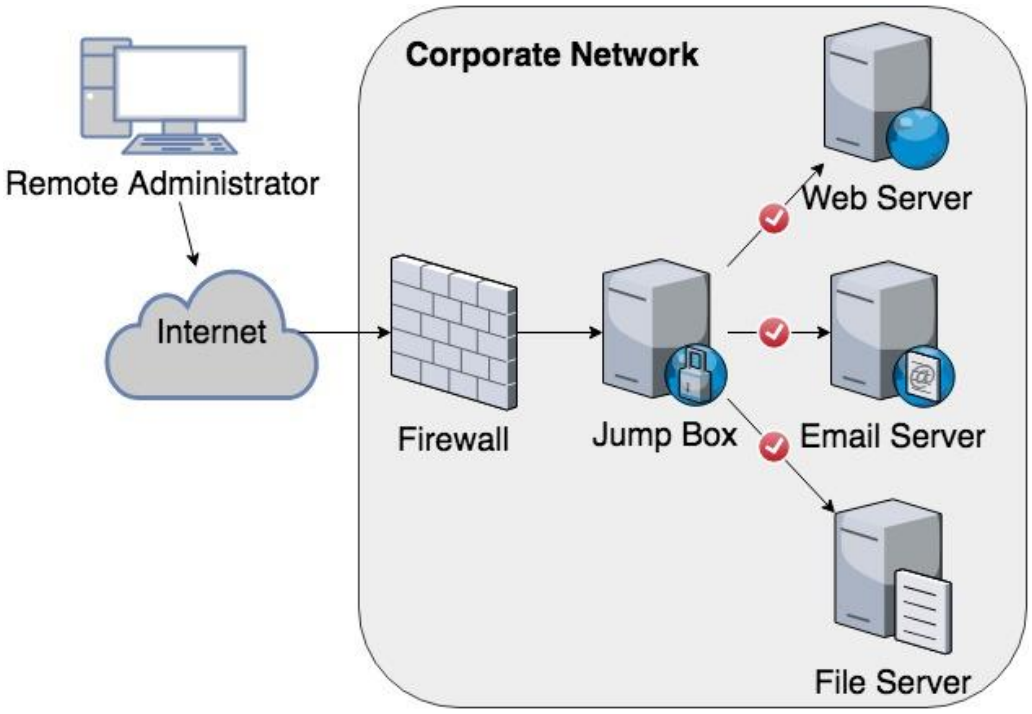


Figure 4 Jump Box Topology

HONEYPOTS

Honeypots are used to learn more about an adversary by intentionally exposing a machine that appears to be valuable target. Usually isolated from the rest of the network, the system will attract an attacker, and administrators can learn their tactics, techniques and procedures (TTPs). The services are not used in production for any users so any interaction would be assumed malicious intent.

- Honeynets: are a network of honeypots designed to attract attackers, look like real network environments and provide realistic feedback.

ENDPOINT SECURITY

While a lot of security is focused on the perimeter or network, it is important to ensure the hosts are thoroughly hardened too. Always do defense in layers. End points should only have the services needed for the user to perform their role. Malware protection should be configured properly. Users should only have access to what they need and updates should be applied early and often.

GROUP POLICIES

Most enterprise devices use a directory service, such as Active Directory, to grant permissions to shared resources. Group policies can force those devices to a baseline of settings for anyone in that group. Security settings are designated at local, domain or network level using the group policies.

DNS ACLS

- Blackhole: A DNS blackhole is a device configured to specifically receive packets for a specific source or destination address and not respond to them. The sender will not be alerted that it failed because the packets are received but silently dropped after.
- Sinkhole: A DNS sinkhole will provide a response to a DNS query for a known malicious site and resolve it to a safe IP set by the administrator. If machines are infected to reach out to a command and control site, the admin can resolve it to something safer to protect the machines while also pointing out which machines are infected by seeing their attempt to query that DNS.

HARDENING

Hardening is a term to describe the use of security practices to improve the defensive posture of a device or network. It should be a constant process of monitoring and improving.

- Mandatory Access Control (MAC): MAC requires authorization for a user on an object. When a user attempts to access a file, MAC checks the *classification level* on the file, and the *clearance level* of the user.
- Compensating Controls: A mean for an organization to achieve a security requirement in an alternative way because they cannot meet the goals explicitly. According to PCI DSS, a compensating control will “meet the intent and rigor of the original stated requirement.”
- Blocking Unused Ports/Services: If you don’t need a service, it should be disabled. Each open port or service is an avenue for an adversary and wasted resources for the machine to wait for the connection. Study the UDP & TCP well-known ports, 0-1023.
- Patching: A necessary evil, you don’t want to risk outages, or new vulnerabilities, but a majority of patches include important security updates. Testing a patch in a sandbox is ideal before pushing to production.

NETWORK ACCESS CONTROL (NAC)

NAC forces policies by verifying device security requirements are met before the device is allowed to connect to the network. Some features like version checking and offering users easy remediation, can use up a lot of resources. The IEEE 802.1X standard was the defector NAC standard but is not as popular for more complex networks.

- Time Based: Prohibits users from joining the network at certain timeframes or prevents users from accessing a network over a certain time limit.
- Rule Based: Queries the host to verify OS, version of security software, or other criteria, such as unauthorized storage devices, and shares this information back with the network to make a decision based on predetermined rules.
- Role Based: Limits connectivity between nodes to prevent unauthorized data access based on the user’s role in the company. Helps with data loss prevention (DLP).
- Location Based: Uses the device location to make decision, for identity verification and asset tracking.

1.4 EXPLAIN THE PURPOSES OF PRACTICES USED TO SECURE A CORPORATE ENVIRONMENT

PENETRATION TESTING

Also known as pen testing, is simulated attacks on a network & systems requested by the owner to gauge the organization’s level of resistance and identify any weaknesses.

PEN TEST PROCESS/KILL CHAIN:

1. Reconnaissance: Gather information about target and foot printing.

2. Exploitation: Gain access through compromising a security control.
3. Lateral Movement: Compromise connected systems to the breach one.
4. Report to Management: Deliver documentation of test findings and suggested counter measures.

DEGREE OF KNOWLEDGE ABOUT TARGET BEFORE TEST

- Zero Knowledge/Black-Box Testing: Start from ground zero like an external attacker would.
- Partial Knowledge/Gray-Box Testing: Some information is provided about target.
- Full Knowledge/White-Box Testing: Intimate knowledge of target is provided.

RULES OF ENGAGEMENT

Full consent must be given regarding the test and certain systems may be off limits or must be available throughout the test.

- Timing: Scope will include the minimum duration of attack and during which hours the test be active.
- Scope: A list of go systems and no-go systems, such as a roster of IP subnets.
- Authorization: An authorization letter or “Get Out of Jail Free Card” from senior management in the event of a systems outage and a list of contacts for the system owners.
- Exploitation: Use of a vulnerability such as specially crafted software, data or commands (exploits) to cause desired behavior.
- Communication: Who knows what and when, also what constitutes a problem needing to contact system owners, and who to contact in such situations.
- Reporting: A detailed report for the successful attack and recommendations for mitigation.

REVERSE ENGINEERING

Reverse engineering is deconstructing something to its features and parts, the purpose is to learn what the system is capable of doing and how it was put together to do that.

ISOLATION/SANDBOXING

A less resource intensive alternative to reverse engineering. A sandbox environment like Cuckoo Sandbox can be used to run malware without impacting the production environment. The purpose is to analyze its behaviors to help identify the malware and its attack vector.

HARDWARE REVERSE ENGINEERING

This can void warranty and possibly violate laws, confer with legal team and end user license. This involves opening up the hardware and verifying it matches to manufacture specifications. Other tests are to extract firmware, perform packet analysis or review voltage level fluctuations.

- Source authenticity: is the verification a product was sourced from an authentic manufacturer. Counterfeit merchandise can have malicious intent and lower quality. When considering authenticity, ensure the price is average for the market, buy from authorize retailers, and check the serial number.
- Trust foundry: is an organization reviewed by the National Security Agency to ensure they are capable of developing microelectronics in a manner that ensures integrity of their products.
- Original equipment manufacturers (OEMs) Documentation: detail the characteristics of their products that can be used to verify the product you have is performing as intended.

SOFTWARE/MALWARE REVERSE ENGINEERING

Reverse engineering software or more commonly in this field, malware, requires an understanding of the architecture of processors. Binary executables are specific to an OS and processor family. Windows programs are packaged in Portable Executable (PE) format, and every file starts with the 2-byte sequence 5A 4D or 4D 5A.

- Fingerprinting/Hashing: To ensure integrity of a file, you would perform the *hashing* function and compare the resulting hash with the previously stored or manufacturer supplied hash value. If the values are different, then the file was modified. You can search your hash VirusTotal to see if it is a known malware file.

- Decomposition: Advanced analysis of the malware may require code analysis. This requires a dissembler like IDA Pro to convert the *machine language*, back to *assembly language*. There are also decompilers that attempt to translate to a high level language, but they don't tend to work for this purpose.

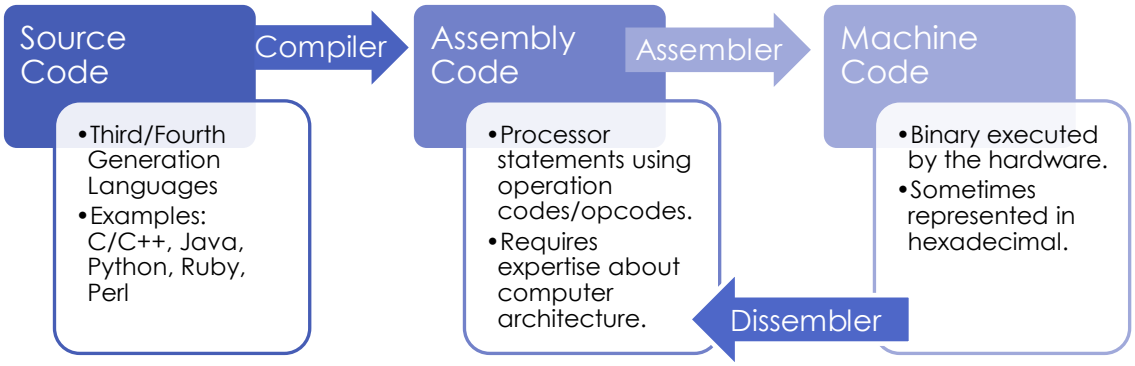


Figure 5 Flow of Code Levels

TRAINING AND EXERCISES

The purpose of training is to develop a set of skills to do their jobs effectively, this should be done regularly. An exercise is an event where individuals or teams apply their skills to a scenario, the results help determine skill gaps or opportunities for business improvements.

- Tabletop Exercises (TTXs): Leadership develops a scenario with a goal targeting a procedure or type of event the team may encounter. The planning should have scoped out branches of different approaches and sequels or follow-ons to a course of action.
- Live-Fire Exercises (LFX): An exercise where the participants defend live or sandbox systems against real friendly attackers. This is more challenging to arrange the infrastructure and teams needed.
- Red Team: Acts as adversaries during an exercise, must be highly skilled.
- Blue Team: Acts as defenders during an exercise, should perform the same tasks they perform in their positions normally and are the focus of the exercise.
- White Team: Overseeing personnel that plans, documents and moderates an exercise.

RISK EVALUATION

Risk Evaluation is the processes of ranking risks and balancing the risks with the cost of the control that mitigates it. Risk = Likelihood x Impact

- Quantitative analysis: Assigns numeric values to assets that could be impacted by a given risk.
- Qualitative analysis: Uses descriptors such as "high" or "category 3" instead of precise numeric value.

Likelihood	**Impact**				
	Insignificant	Minor	Moderate	Major	Severe
Very Likely	Medium	Medium	High	High	High
Likely	Medium	Medium	Medium	High	High
Possible	Low	Low	Medium	High	High
Unlikely	Low	Low	Medium	High	High
Rare	Low	Low	Medium	Medium	Medium

Table 3 Common Qualitative Risk Matrix

- Technical/Logical Control Review: An assessment of *technical controls* (also called logical controls) such as firewall rules, and their effectiveness and relevance to update as needed.
- Operational Control Review: An assessment of *operational controls* such as policies and how they are being managed and how they can be improved. Vulnerability Management

2.1 GIVEN A SCENARIO, IMPLEMENT AN INFORMATION SECURITY VULNERABILITY MANAGEMENT PROCESS

IDENTIFICATION OF REQUIREMENTS

Requirements come from external authorities, internal authorities and best practices.

REGULATORY ENVIRONMENTS

A regulatory environment is when an organization environment is controlled to a significant degree by laws, rules or regulations put in place by government, industry groups, or other organizations.

- ISO/IEC 27001 Standard: Most popular voluntary security standard that covers Information Security Management Systems (ISMS) with strict audit and certification process.
- PCI-DSS: Payment card industry data security standard applies to any organization that processes credit card payments and requires regular scans and risks are properly mitigated.
- HIPAA: Health insurance portability and accountability act has penalties for organizations that fail to defend protected health information (PHI).

CORPORATE SECURITY POLICY

A corporate security policy is produced by senior management to dictate the role security plays in an organization. An issue-specific policy, or functional policy, will address specific security issues such as vulnerability management.

DATA CLASSIFICATION

All data should have a data classification metadata tag to determine the type of protective controls apply to the information. Typical levels include the following:

- Private: Data that could raise personal privacy issues.
- Confidential: Data that could cause grave damage to the organization.
- Proprietary (or Sensitive): Data that could cause some damage to the competiveness of the organization.
- Public: Data that would cause no adverse effect on the organization.

A company would want to consider the following: The level of potential damage if data were disclosed, modified, not available. Legal, regulatory and contractual obligation to protect the data. The age of data and its effects on security.

ASSET INVENTORY

In the Center for Internet Security's (CIS's) Critical Security Controls (CSC) the first thing to do is inventory authorized and unauthorized devices, and number two is to inventory software running on those devices.

- Critical asset: is anything essential to performing the primary function of the business.
- Noncritical asset: not required for the mission of the organization, but still inventoried.

ESTABLISH SCANNING FREQUENCY

Scanning procedure should be planned as far as frequency, intensity and response tactics.

RISK APPETITE

The risk appetite of an organization is how much risk senior executives are willing to assume. Risk will never be zero, and eventually there are diminishing returns on mitigations.

REGULATORY SCANNING REQUIREMENTS'

Regulations will specifically outline when scans should be done and the acceptable level of response to resulting threats.

TECHNICAL CONSTRAINTS

Resources such as personnel, time, bandwidth, hardware or software are limited and are factors in determining frequency of scans.

WORKFLOW

Qualified personnel are a limited resource and the workflow of security operations may limit the time available to perform vulnerability scanning.

CONFIGURE TOOLS TO PERFORM SCANS ACCORDING TO SPECIFICATION

There a lot of considerations when determining how to configure tools to perform scans in a way that best suits the security needs for the organization.

SCANNING CRITERIA

- Sensitivity Levels: Based on the classification level on the asset, tools should be configured to ensure that they're appropriately protecting sensitive assets and also does not compromise the availability.
- Vulnerability Feed: Databases of vulnerabilities are often updated, it is important to pick one that is updated quickly and spend the time reviewing them to ensure you're running scans that appropriately detect the modern vulnerabilities.
- Scope: Since scanning does put a load on the systems, scope should be carefully planned to get the best bang for your resources.
- Credentialed vs. Non-credentialed: A non-credential scan uses the perspective of an outsider, like a black-box test, and tends to be quicker and still realistic. A credentialed scan will give you full coverage of the target.
- Server Based vs. Agent Based: Agent based scans required a running process (agent) on each device, a server-based consolidated data and processes on scanning host(s) and depend on more bandwidth. Agent based scans are better for mobile devices because they can still run their scan when not on the network.
- Types of Data: The output of the scan should be configured to include data that is pertinent for the intended database.

TOOL UPDATES & PLUG-INS

Scanning tools need to be updated for new features regularly. Plug-ins are simple programs used to look for presence of specific flaws. They're used based on new vulnerabilities or business criteria.

- SCAP: Security Content Automation Protocol (SCAP) uses baselines of standards for minimum vulnerability management to automate tools per the standard.

PERMISSIONS AND ACCESS

The scanning program must have the correct privileges on the hosts that it runs on as well as the network infrastructure. Best practice to dedicate an account for scanning tool. Network IDS & IPS may flag the scan and will need to be configured to recognize it correctly. Scan reports also need the accurate amount of permissions.

EXECUTE SCANNING

- Nessus: From Tenable Network Security, provides port-scanning, but mostly known for vulnerability identification, misconfiguration detection, default password uses, & compliance requirements determinations. The Nessus server is installed on the machine or on the network, the client is run from web interface for example: http://localhost:8834 where the setup, scan configuration and scheduling. Plug-ins are also installed on the server for more advanced/specific

scanning. Targets can be IP addresses or hostname. “Safe checks” option will avoid destructive scans. Admins can create an audit file that gives specific configuration for compliance checks.

- OpenVAS: From Greenbone Networks, a free framework of analysis tools that do both vulnerability identification and managmenet. Supports browser-based http://localhost:9392 OpenVAS Manager and OpenVAS Scanner based on Network Vulnerability Tests (NVTs).
- Nikto: Sponsored by Netsparker, is included in Kali Linux and is a web server vulnerability scanner. Can find vulnerabilities in SQL & command injection as well as cross-site scripting (XSS) and misconfigured server. Ran through command line interface. The following command scans host IP 10.10.0.116 and outputs the results to a text file.

```
Nikto –host 10.10.0.116 –output results.txt
```

GENERATE REPORTS

All scanners have some kind of reporting, as an admin you need to know what your reporting utility can do and how you are getting the pertinent information to the right people quickly.

- Automated Vs. Manual Distribution: Automated distribution can sense the type of vulnerability such as web server and send to the system owner such as web server admin.

REMEDIATION

After discovering a vulnerability, remediation should be done thoroughly and as quickly as possible. As well as repeat scans to ensure the remediation was successful.

PRIORITIZING

Discussions with senior leadership and technical team should lay out how to prioritize vulnerability remediation ahead of time for smooth operations.
Criticality: Scanners will determine the severity of the vulnerability in the results in some way, like color-coding. A well-known standard for scoring is the Common Vulnerability Scoring System (CVSS). The metrics it uses are base, temporal and environmental.
Difficulty of Implementation: When challenges to remediation take up too many resources, then a compensating control may be needed to be prioritized instead.

COMMUNICATION/CHANGE CONTROL

When implementing remediation for vulnerabilities, a systematic approach should be taken to ensure that the fix is thorough, and doesn’t hurt system performance or security. Many organizations use a Change Advisory Board (CAB) to approve changes and assist in the change management process.

SANDBOXING/TESTING REMEDIATION

Prior to releasing a patch to production, testing should be done in a sandbox environment to ensure the patch not only corrects the issue, but also doesn’t cause any unwanted side effects.

INHIBITORS TO REMEDIATION

- Memorandum of Understanding (MOU): Outlines duties and expectations of all concerned parties.
- Service Level Agreement (SLA): A contract that outlines roles and responsibilities of service providers, including their limitations. Remediation may not be included in an SLA and thus can’t be enforced upon a service provider.
- Organizational Governance: Also called Corporate Governance, is a system of processes and rules to control its operations in a way that balances the priorities of company stakeholders. This can impact remediation because it could affect other business areas.
- Business Process Interruption: Due to the amount of stress on a system and its importance to business process, a patch may cause interruptions and leadership may delay implementation.
- Degrading Functionality: Sometimes remediation would break critical applications and compensating controls would need to be used to address the vulnerabilities until a suitable patch is developed.

ONGOING SCANNING & CONTINUOUS MONITORING

Automated scanning should be scheduled frequently, and with the most updated version of the scanning tool. Remediation of critical vulnerabilities should be done within 48 hours if possible.

2.2 GIVEN A SCENARIO, ANALYZE THE OUTPUT RESULTING FROM A VULNERABILITY SCAN

ANALYZE REPORTS FROM A VULNERABILITY SCAN

Tools should have comprehensive reports and visual tools like color coding and graphing to help understand the results from scans.

REVIEW AND INTERPRET SCAN RESULTS

The role of the analyst is to review the report before passing it on to others in the organization, the goal is to remove any false positives, exceptions and to prioritize the results.

- Identify false positives: Scanners may be misconfigured, or unable to correctly identify the OS and report a problem that doesn't exist which spends company resources unnecessarily.
- Identify exceptions: Some compensating controls may still show the risk in the vulnerability scan until an appropriate patch can be done, also some networks may have exceptions allowed.
- Prioritize response actions: Once the vulnerabilities are accurately identified, you can prioritize responses that have minimal impact throughout the company.

VALIDATE RESULTS AND CORRELATE OTHER DATA POINTS

Results from a scan should provide details on the vulnerability and suggestions for remediation, sometimes the database (OSVDB & CVE) is not useful. Check Bugtraq, OWASP & CERT.

- Compare to best practices or compliance: On military networks, standards developed by Defense Information Systems Agency (DISA) called Security Technical Implementation Guides (STIGs), combined with National Security Agency (NSA) guides are standards for hardening network devices, endpoints and software. Many are publicly available, some require Department of Defense (DOD) Common Access Cards (CACs) to access, but can be implemented by SCAP.
- Reconcile results: Taking notes in how a vulnerability was discovered until remediation testing, will assist with reconciling other vulnerabilities and may be required, Nessus and OpenVAS both have ways to track how remediation performs on the network.
- Review related logs and/or other data sources: Check event logs and network data to ensure results are doing what you expect on the network. SIEM tools assist with this.
- Determine trends: Some trending functionality may be built in, or other software available, use trends to determine how vulnerabilities have changed over time, and helps security team evaluate their performance and processes.

2.3 COMPARE AND CONTRAST COMMON VULNERABILITIES FOUND IN THE FOLLOWING TARGETS WITHIN AN ORGANIZATION

COMMON VULNERABILITIES

- Missing Patches/Updates: Systems may have missing patches or updates for legitimate reasons such as an industrial control system that can't be offline, then it should be noted tracked and mitigated with a compensation control, otherwise it should be patched using a change control process.
- Misconfigured firewall rules: The ability to reach a device across a network should be only what is required and firewalls should be configured accordingly.
- Weak Passwords: Default, weak or passwords in the clear can easily allow an attacker to bypass all of the other controls put in place.

SERVERS

- Misconfigured unnecessary software, ports, services: If they are not absolutely necessary they should be disabled to reduce the attack surface for a server.

ENDPOINTS

- Lack of user training: Security awareness training should be required on onboarding and usually annually thereafter to ensure that users are not doing anything to compromise the security.
- Outdated malware protection: Malware should be updated early and often to get the latest technologies and signatures.
- Misconfiguration of baseline: Baselines are the core of the security configuration for a device, if not scrutinized for security, devices could be insecure as early as they are provisioned.

NETWORK INFRASTRUCTURE

- Wireless Access Points (WAPs) not on WPA2: Older authentication/encryption technologies like WEP have been considered insecure since 2004 and should be updated to WPA2.
- IEEE 802.1X Network Access Control (NAC) not configured: NAC for wired or wireless networks will enable granular access controls and require devices to meet certain security conditions.

VIRTUAL INFRASTRUCTURE

- Virtual hosts: Improper disposal of VMs, rogue VMs can add attack surface that isn't monitored by security team.
- Virtual networks: Flaws in virtual network may allow bypass of network segregation.
- Management interface (hypervisor): Flaws in software allow jump between virtual machines or to host OS.

MOBILE DEVICES

- Theft: Devices are small and easily misplaced or stolen and as such can be compromised.
- Malicious Apps: Apps can be installed with malware that could compromise the device.
- Outdated hardware preventing updates: Eventually devices are so outdated that the OS will not be able to update any further, causing loss of security patches and they should be replaced.

INTERCONNECTED NETWORKS

- Interconnected Networks: Flaws in connecting a vendor network like HVAC could allow a breach.

VIRTUAL PRIVATE NETWORKS

- Network Access Control (NAC) not configured: Enable granular access controls and require devices to meet certain security conditions.

INDUSTRIAL CONTROL SYSTEMS (ICS)

- Updates: Software is burned as firmware so updates must be done manually.
- Vendor Patches: Some security flaws may never be fixed by vendors and should be mitigated through a compensating control or replacing the system.
- Passwords: Many are stored in plain text, passed in the clear or forced to be default password.

SCADA DEVICES

- Unsecured radio signals: Could be compromised with the proper hardware to spy.
- Unsecured isolated unattended facilities: Could be physically insecure and allow direct access.

2.0 CYBER INCIDENT RESPONSE

3.1 GIVEN A SCENARIO, DISTINGUISH THREAT DATA OR BEHAVIOR TO DETERMINE THE IMPACT OF AN INCIDENT.

THREAT CLASSIFICATION

- Known threat: is one that has a captured signature/hash stored in a database. These threats are easily identified by updated signature-based antivirus software.
- Unknown threat: Recently more common due to new techniques that make changes to malware to create a different signature. These threats are potentially identified by heuristic analysis that observes the behavior of the program.
- Zero Day Vulnerability: Refers to a vulnerability or exploit that is new with no vendor patch or advisory to resolve.
- Zero Day Exploit: Code written to take advantage of a Zero Day Vulnerability.
- Advanced Persistent Threat: An APT is an attacking force with military like efficiency due to a support infrastructure behind their operations. Their goal is to gain and maintain persistent access to target systems while remaining undetected.

FACTORS CONTRIBUTING TO INCIDENT SEVERITY AND PRIORITIZATION

- Scope of Impact: the determination of whether the event is enough deviation from normal to be called an incident and to what degree services were affected.
- Downtime: A primary factor in determining scope. If a network is unavailable any of the other metrics are irrelevant. Maximum Tolerable Downtime (MTD) should be established ahead of time.
- Recovery Time: Time is money, the quicker the recovery, the better it is for business. Recovery Time Objective (RTO) is the earliest time to restore without going over MTD.
- Data Integrity: Some attacks target data such as ransomware. Depending on the sensitivity of the data and the condition of the backups, impact could be more devastating.
- Economic: Some economic impact is obvious like a fine due to a contract or regulation, some are more difficult to quantify like work done to create, protect or repair the service/data.
- System Process Criticality: Criticality of processes should be prioritized to determine order of recovery, often categorized as High, Moderate or Low.

TYPES OF DATA

- Personally Identifiable Information (PII): information related an individual's identity such as: social security number, name, date of birth, anything that can be used in identity theft. Protect by The Privacy Act of 1974 and other regulations.
- Personal Health Information (PHI): information related to an individual's past, present or future physical or mental health condition protected by HIPAA.
- Payment Card Information: Information related to cardholders that could be used for credit card fraud protected by PCI DSS.
- Intellectual Property: information related to knowledge of how to make something or a unique creation that is how an organization distinguishes itself from others protected by company policies and legal guidance. Falls into four categories: patent, copyright, trademark and trade secrets.
- Corporate Confidential: information related to the internal operations of a company such as correspondence about upcoming changes, details about marketing campaign. Sometimes referred to as proprietary information protected by company policies.
- Accounting Data: Information related to financial data that could give insight to the health of the company. Protected by company policies and legal guidance.
- Mergers and Acquisitions: Information related to upcoming mergers and acquisitions is sensitive corporate information that could create financial losses to both companies. Insider trading is a serious crime by an employee trades stock due to pending acquisition.

3.2 GIVEN A SCENARIO, PREPARE A TOOKIT AND USE APPROPRIATE FORENSIC TOOLS DURING AN INVESTIGATION

FORENSICS KIT

- Digital Forensics Workstation: Computer used to collect and analyze data to validate an incident and its cause.
- Jump Bag: Packaged set of tools prepared to respond to incidents.
- Write Blockers & Drive Adapters: Prevent modifications to a storage device while you acquire their contents. Tools differ by what types of disk interfaces they support.
- Cables: Ethernet cables, serial cables, power cables, a small Ethernet hub, antistatic wrist straps and anything else pertinent to the environment.
- Wipes Removable Media: A blank drive supported by your write blocker with a large enough capacity to be used to hold forensic data.
- Cameras: needed to photograph incident site, also useful to pack a ruler for scale.
- Crime Scene Tape: To protect the integrity of the scene and prevent accidental entry.
- Tamper-Proof Seals: Evidence should be contained with a tamper proof seal when transported.
- Documentation and Forms:
    - Chain of Custody Form: a tailored form kept with the evidence to track the transfer of ownership between handlers.
    - Incident Response Plan: a copy should be kept in the bag in the event there is no network access during the response.
    - Incident Log: Used to document every action taken and each hypothesis during investigation to ensure anyone with access to the same evidence can come to the same conclusions.
    - Call/Escalations List: If conditions at the scene change, and you have questions or additional authorization is needed, a list should be at bag or the respond plan.

FORENSIC INVESTIGATION SUITE

- Image Acquisition Utilities:
    - Forensic Duplicators: Copy data from a source to destination without altering even a bit of the data. Linux: dd command utility default with most systems, should be used with sha1sum command to get a hash of output file. FTK Imager is a free data preview and image tool by Access Data allows forensically sound acquisition and hashing verification.
- Analysis Utilities: Used to display acquired data for analysis.
    - EnCase: Most widely used analysis tool among law enforcement agencies and some large corporations. Can perform acquisition, analysis and reporting functions. Creator of EnCase Evidence File format (.E01) that integrates compression, encryption and metadata.
    - Forensic Toolkit (FTK): Almost as widely used as EnCase, built on top of a data management system, easily processes large volumes of data. Indexing can take a longer than other solutions.
    - The Sleuth Kit: Open source collection of interoperable tools, many used in the command-line. Can be used with Autopsy for a GUI.
- Chain of Custody: A form included in jump back with a copy for each piece of evidence used to track the ownership and history of how evidence was collected, transported and preserved.
- Hashing Utilities: Most popular algorithms are MD5 and SHA-1 are available in the OS command line for Mac or Linux, or in Windows download File Checksum Integrity Verifier (FCIV).
- OS and Process Analysis: Each OS manages computer resources such as memory, CPU, and disks, and has different key areas for analysis. Practice finding information in:
    - Windows systems: Event log for application log data & registry for things like autorun locations, most recently used lists (MRUs) & wireless networks.

  - Linux systems: Be familiar with utilities like dd, sha1sum, and ps. Linux directory structure, / = root, /etc = primary system configuration directory with sub directories for most applications, /var/log = application log plain text files, & /home/$USER = $USER is a variable name that should be replaced with the username of a given user to view user and configuration data.
- Mobile Device Forensics: Requires a custom bootloader and tools to access the SQLite data.
- Password Crackers: Software to crack password on encrypted files or drives in the event the suspect or owner is unable to provide the password, like Passware Kit Forensic.
- Cryptography Tools: Software to encrypt evidence of an investigation, there are built in tools in OS but also more robust tools like VeraCrypt.
- Log Viewers: Used to aggregate logs from multiple computers. Tools include Splunk, SolarWinds' Event Log Consolidator/Manager, and Ipswitch's WhatsUp.

3.3 EXPLAIN THE IMPORTANCE OF COMMUNICATION DURING THE INCIDENT RESPONSE PHASE

STAKEHOLDERS

- Stakeholders: Individuals/teams within the organization that have a role in the IR process.
- HR: When IR team determines an employee had a role (whether accidental or purposeful) in the incident, HR may be needed for disciplinary action.
- Legal: Provide counsel for forensic gathering and reporting whenever IR escalates to involve government agencies.
- Marketing: Handle the public image of the company and must have high-level technical information to decide what, when and how to provide communication to public.
- Management: For managers not directly participating in IR, they may need to be informed for buy-in and resources from other business areas.

PURPOSE OF THE COMMUNICATION PROCESS

- Limit Communication to trusted parties: A war room or group chat should be established to promote communication but only to trusted parties.
- Disclosure based on regulatory/legislative requirements: Although sometimes disclosure is required to customers, high-level information should still be shared cafefully in a way that assuages customer fears.
- Prevent inadvertent release of information: Media/Marketing should have a premade template for providing information early to control the narrative with factual information.
- Secure method of communication: Internal communication should be limited and secured to either a physical or virtual war room with access controls.

ROLE-BASED RESPONSIBILITIES

- Technical: The members of the team vary depending on the incident, but based on different threats, should be pre-determined especially who makes the authorizes certain activities.
- Management: Key senior leaders should be included to provide support, shape the response process, address regulatory issues, and interface with affected business units.
- Law Enforcement: Sometimes a law enforcement agency (LEA) may need to be involved. LEA will bring a different perspective into forensic evidence preservation.
- Retain Incident Response Provider: Contractors may be needed to augment staffing/resources to response to incidents, requires a degree of prior coordination, NDAs etc.

3.4 GIVEN A SCENARIO, ANALYZE COMMON SYMPTOMS TO SELECT THE BEST COURSE OF ACTION TO SUPPORT THE INCIDENT RESPONSE

COMMON NETWORK-RELATED SYMPTOMS

- Bandwidth Utilization: Each network should have a pattern of utilization; IR team may notice a spike in bandwidth or unusual end points or directionality of traffic. Suspicious NetFlow activity example below. Host 10.0.0.6 is running a webserver to other hosts on its own subnet, but it appears to be connecting to a high port to a remote web server and sending significantly more packets to host 172.31.21.3 outside its subnet.

Src IP	Src Port	Det IP	Det Port	Protocol	Packets	Bytes/Pkt
10.0.0.3	54901	192.168.0.7	80	TCP	2491	740
10.0.0.6	55097	172.31.21.3	443	TCP	100227	1528
10.0.0.12	993	10.0.0.3	48450	TCP	2210	762
10.0.0.6	443	10.0.0.7	54122	TCP	2271	1040
10.0.0.6	443	10.0.0.3	53112	TCP	1022	810

Table 4 Example Suspicious NetFlow from CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001)

- Beaconing: A malware command-and-control (C2) will have a host send recurring outbound connection to an external controller. Some are randomized timeframe between connections, but most have a predictable pattern that can be discovered by sorting traffic logs by internal source address, then by destination address, and then by time.
- Irregular Peer-to-Peer Communication: Most networks work by connecting to a server to create a client/server relationship. When peers/clients connect to each-other, this could indicate a compromised host. Attackers often attempt lateral movement to compromise additional hosts after their initial entry to a network. To find lateral movement, look for: unprivileged accounts connecting to hosts, privileged accounts connecting from regular hosts, repeated failed remote logins.
- Rogue Devices on the Network: An inventory of your network should be established to determine when a rogue device is connected, either through a network plug or wirelessly. Best way to avoid is to employ NAC or have logs from access points sent to a server and search for rogue MACs.
- Scan Sweeps: Some attackers will use a scan sweep to identify other hosts once they compromise a host on a network. Identified by monitoring ARP messages an abnormally large amount of queries.
- Unusual Traffic Spikes: covered in bandwidth section.

COMMON HOST-RELATED SYMPTOMS

- Processor Consumption: One of first tasks in responding to an incident is look at running processes. A high consuming process taking a substantial amount of CPU cycles could indicate a suspicious running process. Sometimes rootkits can hide running processes from built-in OS tools so capture volatile memory first.
- Memory Consumption: A volatile memory capture takes time but will capture rootkits and other malware that reside entirely in memory.
- Drive Capacity Consumption: It is extremely difficult to compromise a computer without leaving evidence of their actions on a file system.
- Unauthorized Software: An illicit binary executable file can be located easily if you have an authorized software list.
- Malicious Processes: Baselines can provide normal processes inventory to help identify rogue processes. Sometimes a rogue process will disguise itself by changing just one character of a known good process.
- Unauthorized Changes: OS can detect unauthorized changes such as Windows DLLs and log these changes using a feature called Object Access Auditing. Linux has a similar audit system. Important files can be hashed and stored hashes kept securely to use in integrity checking.
- Unauthorized Privileges: Adversaries will attempt privilege escalation, to acquire unauthorized privileges by acquiring privileged credentials or exploiting software flaws or misconfigurations. Monitoring systems for use of privileged accounts can assist in detecting this.

- Data Exfiltration: Data for exfiltration will commonly be moved to a staging location then attempt encrypted exfiltration that will look like a normal activity like a web service request or email but the endpoint and volume of data can identify suspicious activity. Automated alarms for large data especially to an unusual destination are helpful. Or data loss prevention (DLP) solutions.

COMMON APPLICATION-RELATED SYMPTOMS

- Anomalous Activity: When an application behaves differently such as web browser freezing pages or changing URLs, or Word exploited to create malicious payloads.
- Introduction of New Accounts: Attackers may create new accounts to gain additional access. If a new privileged domain account, when identified, admins should log off the user and change the password.
- Unexpected Output: Unexpected pop-ups like certificate warnings or User Account Control (UAC) pop-ups are usually malicious if the user is just doing normal activities.
- Unexpected Outbound Communication: An IDS can detect if an application like notepad for example attempts a remote connection via port 443 for example when it definitely should not.
- Service Interruption: When services start acting differently such as a missing antimalware icon, that could indicate an attacker has disabled protections on the computer.
- Memory Overflows: Memory errors can be forced in an attack to trigger an exploit.

3.5 SUMMARIZE THE INCIDENT RECOVERY AND POST-INCIDENT RESPONSE PROCESS

CONTAINMENT TECHNIQUES

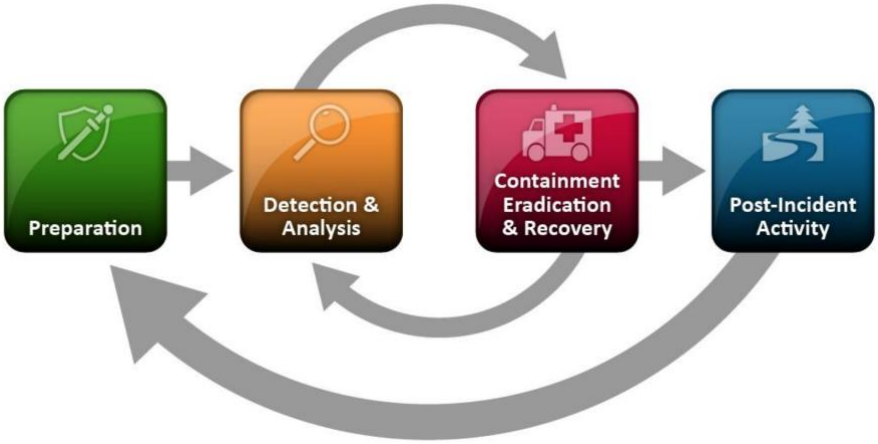


Figure 6 Incident Response Process as seen in NIST SP 800-62 R2

- Segmentation: A well-designed security architecture has network segmentation by predetermined criteria. Implemented virtually through VLANs, or physically through different wired networks, traffic must go through a gateway device. Provides a layer of defense, compromised hosts could be moved to an isolated segment below.
- Isolation: An isolation VLAN like a quarantine for suspicious hosts to prevent communications to peers or C2 nodes. Some advance malware can detect this and eradicate itself from the host. While isolated, team can analyze activity to investigate nature of compromise that can be shared with Computer Emergency Readiness Team (CERT) or Information Sharing Analysis Center (ISAC).
- Removal: It may be necessary to remove compromised hosts from the network entirely, when removing the decision should be made to keep it powered on, shut it down, or simply rebuild it.
- Reverse Engineering (RE): is analysis of a product to learn it's functions. RE malware can be done through dynamic analysis, letting it run in a sandbox and observing its behavior, or static code analysis which requires a skilled professional to disassemble and analyze the code.

ERADICATION TECHNIQUES

- Sanitization: According to NIST SP 800-88 R1 (Guidelines for Media Sanitization), sanitization is the process by which access to data on a given medium is made infeasible for a given level of effort. In IR, these levels can be cursory or sophisticated. The following techniques are in increasing level of effectiveness:
    - Overwriting: Replaced ones and zeroes with a random or fixed patterns of ones and zeroes to render original data unrecoverable, should be done at least once.
    - Encryption: Mobile devices take this approach of storing data in encrypted format using a strong key, then deleting the encryption key to make the data unrecoverable.
    - Degaussing: Removing or reducing the magnetic field patterns on conventional disk drives or tapes through the application of powerful magnetic force. Typically renders the drive unusable.
    - Physical Destruction: To shred or use caustic / corrosive chemicals to destroy the media.
- Reconstruction/Reimage: Images sometimes called gold masters are used to rebuild the host to a known good state. Restoring data can be done if up-to-date backups are available.
- Secure Disposal: Can be done through sanitization or hiring an accredited service provider to destroy and dispose of the devices/media.

VALIDATION

- Patching: Centralized patching should be used where possible, or manual patching for devices such as BYOD that cannot be centrally managed to ensure no further use of vulnerabilities.
- Permissions: After an IR investigation, permissions should be reviewed to ensure no changes were made or no privilege creep to allow for another attacker to have too much access.
- Scanning: Verifying no further vulnerabilities exist in the environment should be done with the aid of vulnerability scanning.
- Verify Logging/Communication in Security Monitoring: Tour monitoring solution should be reviewed and adjusted as needed to detect this incident in the future.

CORRECTIVE ACTIONS

- Lessons Learned Report: Every participant in the investigation should meet and create a lessons learned report that includes any issues that arose during the operations, discussion of what was observed and why it is important to learn from, and recommendations to either sustain current procedures or improve response.
- Change Control Process: Suggestions made after the incident should go through a change control process that includes all impacted business units to determine feasibility, acceptance criteria and testing needed before implementation.
- Update Incident Response Plan: The plan should be reviewed and updated with any recommendations from the IR team

INCIDENT SUMMARY REPORT

- Post-Incident Report: Considering the audience of who will read the report, and the purpose of the report before writing, the report will typically include a summary of the event and response and recommendations for technical or business improvements.

3.0 SECURITY ARCHITECTURE AND TOOL SETS

4.1 EXPLAIN THE RELATIONSHIP BETWEEN FRAMEWORKS, COMMON POLICIES, CONTROLS, AND PROCEDURES

REGULATORY COMPLIANCE NETWORKS

- NIST: National Institute for Standards and Technology develops and publishes standards and guidelines aimed at improving practices.

- SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations): Outlines controls to be compliant with the Federal Information Processing Standards (FIPS).

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environment Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PM	Program Management
CM	Configuration Management	PS	Personnel Security
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

Table 5 Control Categories as seen in SP 800-53 R4

- Cyber Security Framework (CSF): Per executive order in 2013, NIST published the framework as a voluntary cybersecurity framework for organizations. Consists of three components, the Framework Core provides references that are relevant for all organizations, the Implementation Tiers categorize degree of rigor and sophistication as Partial (tier 1), Risk Informed (tier 2), Repeatable (tier 3) or Adaptive (tier 4), the Framework Profile describes state of organization to allow business decision-makers to prioritize.

Figure 7 CSF Core Categories

- ISO: International Organization for Standardization and International Electrotechnical Commission (IEC) worked together to build a family of Information Security Management System (ISMS) standards, known as the ISO 27000 series. Organizations can volunteer to be certified ISO 27001 compliant by an accredited third party.
- COBIT: Control Objectives for Information and related Technology is a framework with a set of control objectives developed by ISACA (Information Systems Audit and Control Association. Broken into categories: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate with additional subcategories. Provides a checklist approach and roadmap.
- SABSA: Sherwood Applied Business Security Architecture is a layered model and each layer decreases in abstraction and increases in detail as it builds upon others. SABSA asks at each layer: What are you trying to do? Why are you doing it? How are you trying to do it? Who is involved? Where are you doing it? When are you doing it? Also provides a lifecycle model.
- TOGAF: The Open Group Architecture Framework originated from the U.S. Department of Defense, uses its Architecture Development Method (ADM) so a technology architect can be developed with consideration of all views (business, data, application and technology).
- ITIL: Information Technology Infrastructure Library (ITIL) is a customizable framework that provides goals, actions needed to complete goals, and input and output values for each process required to meet goals. It has components for security but focuses on SLAs.

POLICIES

- Password Policy: Should motivate users to manage their passwords securely and will include requirements such as minimum length, complexity, age, reuse restrictions, or prohibition against certain words.
- Acceptable Use Policy (AUP): specifies what is acceptable and prohibited use of company information systems, should document when user was made aware of AUP.
- Data Ownership Policy: Establishes the roles and responsibilities of data owners who are responsible for use and security of data, personal data must also be addressed.

- Data Retention Policy: Some legal and regulatory requirements exist for how long to retain data which can be applied or specific data sets can be set more specific retention periods.
- Account Management Policy:
- Data Classification Policy: Organizes data according to it sensitivity to loss, alteration, disclosure or unavailability.

CONTROLS

- Control Selection Based on Criteria: Consists of baseline security levels for each system combined with requirements imposed by laws, regulations or policies.
- Organizationally Defined Parameters: A variable that defines portions of controls to support organizational requirements or objectives, such as risk appetite, or regulations.
- Physical Controls: Safeguards to deter, delay, prevent, detect, or respond to threats against physical property.
- Logical Controls: aka Technical Controls, software used to restrict subjects' access to objects.
- Administrative Controls: Security implemented by management through policies and procedures.

PROCEDURES

- Continuous Monitoring: NIST SP800-137 defines as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." When monitoring reveal actionable intel, the remediation plan is activated.
- Evidence Production: A legal request for documents, files, or other tangible items that could have bearing on a legal procedure. Sometimes called electronic discovery or e-discovery. Includes:
    - Identification of data required under order.
    - Preservation of this data to ensure it is not accidentally or routinely destroyed while the order is being complied with.
    - Collection of the data from the various stores in which it may be housed.
    - Processing to ensure the correct format is used for both the data and its metadata.
    - Review of the data to ensure it is relevant.
    - Analysis of the data for proper context.
    - Production of the final data set to those requesting it.
    - Presentation of the data to external audiences to prove or disprove a claim.
- Patching: Process by which fixes to software vulnerabilities are identified, tested, applied, validated and documented. Patches may break something and should be tested, then rolled out one at a time with rollback procedures and documented after installation.
- Compensating Control Development: Codified process by which compensating control decisions are made and developed.
- Control Testing Procedures: Describes steps security staff will verify and validate the controls they use to. Ensure it was implemented correctly and mitigates the intended threat.
- Manage Exceptions: When procedures must be violated this procedure will define decision-makers how they will reach a decision and what to do if there are irreconcilable differences.
- Remediation Plans: Describes the steps to take whenever a security posture worsens.

VERIFICATIONS AND QUALITY CONTROL

- Audits: A systematic inspection by an independent third party, often due to regulatory compliance.
- Evaluations:
- Assessments: Process that gathers information to make determinations such as vulnerability assessment, penetration test, red team assessment, risk assessment, threat modeling, etc.
- Maturity Model: A measure of how introspective a company is in regard to cybersecurity. For example the, Capability Maturity Model Integration (CMMI).

- Certification: Technical evaluation of security components and their compliance with applicable regulations to meet pre-determined requirements Accreditation is a second step as a formal acceptance of the adequacy of the system's overall security and functionality by management.

4.2 GIVEN A SCENARIO, USE DATA TO RECOMMEND REMEDIATION OF SECURITY ISSUES RELATED TO IDENTITY AND ACCESS MANAGEMENT

SECURITY ISSUES ASSOCIATED WITH CONTEXT-BASED AUTHENTICATION

- Time: Used to determine authenticity of the users based on when the activity occurs. Some logins can only be during business hours, or a two factor token is only active within a short time window. Time and location should be tied together to prevent the use of time-zone manipulation to bypass.
- Location: Network-based location would look-up the IP to determine the country, city and zip code. This is weak though because it is easy to falsify an IP. Device-based location uses built in location GPS sensors. An attacker can falsify GPS signal data or manipulate the location data on the device with an app on a jailbroken/rooted phone. NAC can prevent such devices from connecting.
- Frequency: Frequency & speed of login attempts at a rate impossible to humans can be blacklisted or throttled. Attackers can adjust their attempts to be more human like but password cracker tools put a priority on speed. Analysts can be alerted by their attempts to investigate.
- Behavioral: To detect if a session has been hijacked without forcing multiple logins, a process called "Active Authentication" uses a learning system to generate a fingerprint based on user behavior with their machines. Attackers can develop AI to simulate human behaviors.

SECURITY ISSUES ASSOCIATED WITH IDENTIES

- Personnel: People can share passwords, lose devices, fall for phishing/scams. User training is referred to as "securing the human" by the SANS Institute. Also look for signs of compromise.
- Endpoints: aka Device authentication, relies on values derived from hardware or OS, such as MAC address, are easily to spoofed or replayed.
- Servers: Typically authenticated with X.509 standard digital certificates issues by a trusted Certificate Authority (CA). It is possible to steal a certificate or insert into a chain and present fake certificates which shows errors that are often dismissed by users. Mutual authenticating is better such as Kerberos protocol which uses an Authentication Service (AS), Ticket Granting Server (TGS), & Key Distribution Center (KDC). SANS paper on Kerberos.
- Services: Counterfeir services can be used to phsich users, can be prevented with Windows .NET Framework Service Identity and Authentication.
- Roles: Role-based access often tacks on roles to an individual that climbs the corporate ladder will often have all the access from previous roles, auditing roles should be done periodically to ensure least privilege.
- Applications: Attackers will try privilege escalation on a target application by exploiting a software flaw or misconfiguration.

SECURITY ISSUES ASSOCIATED WITH IDENTITY REPOSITORIES

- Directory Services: A central repository for storing and managing information relied upon by admins to provide management and security options at scale.
    - Active Directory (AD): Allows organizations to centrally manage resources and network security policy in Windows environments. All users, resources, or services are called objects with attributes associated such as name and description. Attackers goal is to gain access to the AD to get complete control over all objects. Use least privilege, event log monitoring and detailed object auditing to mitigate this threat.
    - Lightweight Directory Access Protocol (LDAP): cross-platform open standard for maintaining directory services on a network. Attackers can craft statements to LDAP server to provide more information than should be available. Defend by validating and sanitizing user input by escaping special characters and restricting regular expressions.

- TACACS+: Terminal Access Controller Access Control System Plus, provides authentication authorization and accounting (AAA). An alternative to Kerberos, uses client/server TCP session with encrypted username/password to determine access level. Vulnerable to replay attacks because sequences always start with number 1 and session IDs are short during exchanges.
- RADIUS: Remote Authentication Dial-In User Services is also a AAA protocol but does not encrypt usernames during process and uses UDP so less reliable. Attackers can forge packets easily. Also RADIUS uses a shared secret across the network so attackers can breach the entire network easily and some versions are susceptible to buffer-overflow attacks.

SECURITY ISSUES ASSOCIATED WITH FEDERATION AND SINGLE SIGN-ON

- Manual vs. Automatic Provisioning/De-provisioning: Manual provisioning allows admins to create user accounts on a service with their roles and access rapidly. Auto-provisioning creates an account as users are authenticated to a new system, the identity provider (IDP) is asserting that the user should be allowed to hold an account with the service provider (SP). Manual control is difficult but important to reduce attack surface such as orphan accounts or incorrect access.
- Self-service password reset: By removing administrator oversight to password reset process, attackers can take advantage.

EXPLOITS

- Impersonation: Attackers may impersonate a user by fabricating user information to authentication system or impersonate a service to harvest credentials or intercept communications by stealing a server key or gain trust as the CA, or if the client doesn't check if it is a trusted CA.
- Man in the Middle: MITM are impersonation attacks that face the client and the server acting as a proxy/relay between a conversation between parties to collect credentials, capture traffic, or add false communications.
- Session Hijack: Takes advantage of valid session information by stealing and replaying it. Session information is a string that appears in a cookie file, the URL or other parts of HTTP that can be obtained through traffic capture or prediction.
- Cross-site Scripting: XSS uses a browser to execute code that can access sensitive information such as passwords and session information. Take advantage of inherent trust between browser and site to run code. Persistent attacks store code on a site, such a on a message board or comments so when users access the site the code executes. Non-persistent attacks aka reflected XSS take advantage of flaw in server software to create a link that when clicked on by users would cause the browser to visit the site and execute the code.
- Privilege Escalation: Any action that allows a user to perform attacks they should be able to do. Vertical means that user gains privileges of a higher-privilege users. Horizontal means that user accesses information at the same privilege level. Can be used to modify files, extract data, or install malicious code.
- Rootkit: Challenging malware designed to maintain persistence at root-level access without being detected.

4.3 GIVEN A SCENARIO, REVIEW SECURITY ARCHITECTURE AND MAKE RECOMMENDATIONS TO IMPLEMENT SECURITY CONTROLS

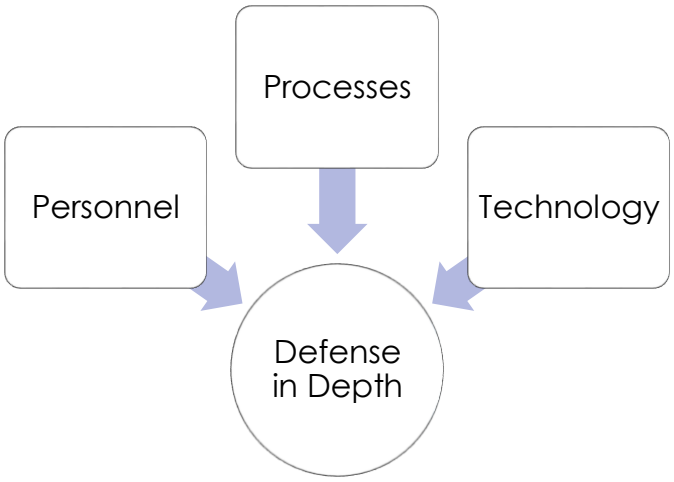
SECURITY DATA ANALYTICS

- Data aggregation and correlation: Data is the raw numbers, information is the collection of data pertaining to an object, knowledge is insight brought by combining various pieces of information and adding context. Wisdom is knowledge combined with experience to make decisions. Aggregation is to collect and categorize data for analysis. In a SIEM data is aggregated and correlation rules provide meaning information from patterns.
- Trend Analysis: Using data from the past to predict the future.
- Historical Analysis: Using data from the past as compare new events with past events.

MANUAL REVIEW

- Firewall Logs: Review various firewall log examples and pick out information such as action, time, source IP, and port number. Check out this SANS white paper for more info.
- Syslogs: Standard for logs developed at University of California, Berkeley. Syslogd process collects logs on UNIX, Linux, (found in /var/log directory) and variants such as routers and firewalls (location of logs will vary). Best Practice to configure to a centralized log server for aggregation & analysis (UDP/TCP 514).
- Authentication Logs: Analysis of login events is crticial for incidents, linus uses auth.log file. Consider the time zone difference for each device.
- Event Logs: Similar to syslogs in detail but for Windows systems via the Event Viewer.

DEFENSE IN DEPTH



- Personnel:
  - Training: Security Awareness Training for all employees usually includes network behavior and how to deal with suspicious activity. Training Security employees entails keeping up with new threats and defense technologies.
  - Dual Control: Requires two parties to complete a task. Like missile launch keys.
  - Separation of Duties: Two parties are given two different tasks that work towards a goal. Rotation of duties requires roles to change to prevent abuse.
  - Third Party/Consultants: Should sign an NDA, have defined policies, and expectations and should be monitored as they are not as vetted as regular employees.
  - Cross Training: Rotate employees to expose them to new jobs and ensuring there are backup personnel.
  - Mandatory Vacation: Employees need to destress. Problems may be revealed when an employee goes on vacation.
  - Succession Planning: To ensure continuity, a procedure 'play book' should be developed to allow any employee to pick up the roles of the lost employee.
- Processes:
  - Continual Improvement: As personnel and technology changes, processes must be constantly updated to meet new threats, this is a hallmark of mature organizations.
  - Scheduled Reviews: Organization shall review its security strategy such as policies and this is generally required in regulated environments.
  - Retirement of Processes: A process that is no longer relevant, has been replaced, or no longer aligns with the business should be formally removed.
- Technologies:
  - Automated Reporting: Found in most modern security products but must be configured to avoid getting too many alerts.
  - Security Appliances: Hardware that performs functions that are typically spread across multiple devices like firewalls, content filters, IDS/IPS, and load balancers with a central management console.

Change Control Process

⇒ Request for a change.
⇒ Get approval for the change.
⇒ Document the change.
⇒ Perform testing and certification.
⇒ Implement the change.
⇒ Report finalized change to stakeholders.

    - Security Suites: Software to provide multiple functions such as endpoint scanning, mobile device management (MDM), phishing detection. AKA Multilayered security.
    - Outsourcing: When outsourcing, additional security steps must be taken such as access control, contractor vetting, and agree upon incident handling and reporting.
        - Security as a Service: (SECaas) Security companies provide technology and people as a service with a subscription model.
    - Cryptography: Integrity through hash functions, and digital signatures, confidentiality through encryption.
- Other Security Concepts: Network should be architectures with security in mind.
    - Network Design: Design needs to take in mind that new technologies reduce the effectiveness of their perimeter.
    - Network Segmentation: Improves the efficiency of the network by reducing workload on routers and switches, and security by separating usage and access within the network.

4.4 GIVEN A SCENARIO, USE APPLICATION SECURITY BEST PRACTICES WHILE PARTICIPATING IN SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC).

BEST PRACTICES DURING SOFTWARE DEVELOPMENT

- Security Requirements Definition: Defines requirements for finished products:
    - Functional requirements that describe what the software must do such as inputs, processing, & outputs.
    - Nonfunctional requirements that describe how the software must do these things such as characteristics, constraints, or limitations. AKA Quality requirements.
- Security Testing Phases:
    - Static Code Analysis: Technique to identify security policy violations by evaluating the code without needing to run the program.
    - Web App Vulnerability Scanning: External tests conducted from the perspective of a malicious user to identify vulnerabilities.
    - Fuzzing: Sends massive amounts of malformed/unexpected/random data to program to attempt and trigger failures.
    - Use Interception Proxy to Crawl Application: An interception proxy is a tool placed between two endpoints to examine, modify or log communications, and then it can used to inspect those messages for any security characteristics or vulnerabilities.
- Manual Peer Reviews: AKA Code Reviews, a peer other than the author must review the code prior to any release to ensure secure development practices were implemented.
- User Acceptance Testing: Every software has a purpose to satisfy needs of the users, and it is not considered acceptable until the users declare all feature have been implemented adequately, may not be a formal event, more like a continuous engagement.
- Stress Test Application: Tries to break software by creating extreme demands beyond normal thresholds to determine how robust the system is. Focus is to try and create a DoS.
- Security Regression Testing: After release, flaws and vulnerabilities may need to be patched, regression testing is to ensure that patching a flaw doesn't reveal a new flaw or break a function.
- Input Validation: Never trust input from the user. Improper input validation leads to code injection attacks, SQL injection. Client-side validation is often implemented through JavaScript and embedded in code of page with form, but can be easily negated. So, server-side validation should be done to check input before processing it.

Example of insecure PHP SQL query:

```
$result = mysql_query("SELECT * FROM userdb WHERE username='$form username'
          AND password='$form_password'");
$num_rows = mysql_num_rows($result);
if($num_rows > 0){
    $authenticated = True;
else
    $authenticated = False;
```

Example of attacker SQL injection in username and password of application:

Username: `attacker' or 1=1`
Password: `pawned`

Resulting SQL query string:

```
*SELECT * FROM userdb WHERE username='attacker' or 1=1 --'
        AND password='pawned'"
```

SECURE CODING BEST PRACTICES

- OWASP: Open Web Application Security Project has resources for developers to build secure software. Well known for top 10 security risks reports (2013) (2017).
- SANS: Cybersecurity training institute provides a lot of training resources and best practices such as this DevSecOps checklist.
- Center for Internet Security (CIS): Nonprofit with the goal to enhance cybersecurity around the world. The Integrated Intelligence Center receives and shares intelligence reports from public and private sectors.
    - System Design Recommendations: Using focus groups, CIS creates best practices for secure system design such as the 20 CIS Controls.
    - CIS Benchmarks: are guides to securing platforms including pre-hardened images of open source platforms.

4.5 COMPARE AND CONTRAST THE GENERAL PURPOSE AND REASONS FOR USING VARIOUS CYBERSECURITY TOOLS AND TECHNOLOGIES

*(**The intent of this objective is NOT to test specific vendor feature sets)*

PREVENTATIVE

- IPS
    - Sourcefire
    - Snort
    - Bro
    - HIPS
- Firewall
    - Cisco
    - Palo Alto
    - Check Point
- Antivirus (AKA Anti-malware)
- EMET
- Web proxy
- Web Application Firewall (WAF)
    - ModSecurity
    - NAXSI
    - Imperva

COLLECTIVE

- SIEM
    - ArcSight
    - QRadar
    - Splunk
    - AlienVault
    - OSSIM
    - Kiwi Syslog
- Network scanning
    - NMAP
- Vulnerability scanning
    - Qualys
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer
- Packet capture
    - Wireshark
    - Tcpdump
    - Network General
    - Aircrack-ng
- Command line/IP utilities
    - Netstat
    - Ping
    - tracert/ traceroute
    - ipconfig/ ifconfig
    - nslookup/dig
    - Sysinternals
    - OpenSSL
- IDS/HIDS
    - Bro

ANALYTICAL

- Vulnerability scanning
    - Qualys
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer
- Monitoring tools
    - MRTG
    - Nagios
    - SolarWinds
    - Cacti
    - NetFlow Analyzer
- Interception proxy
    - Burp Suite
    - Zap

- Vega

EXPLOIT

- Interception proxy
  - Burp Suite
  - Zap
  - Vega
- Exploit framework
  - Metasploit
  - Nexpose
- Fuzzers
  - Untidy
  - Peach Fuzzer
  - Microsoft SDL File/Regex Fuzzer

FORENSICS

- Forensic suites
  - EnCase
  - FTK
  - Helix
  - Sysinternals
  - Cellebrite
- Hashing
  - MD5sum
  - SHAsum
- Password cracking
  - John the Ripper
  - Cain & Abel
- Imaging
  - DD

APPENDIX A. ACRONYMS

ACL Access Control List
ARP Address Resolution Protocol
BYOD Bring Your Own Device
CIS Center for Internet Security
CoBiT Control Objectives for Information and Related Technology
CCTV Closed-Circuit Television
CRM Customer Relations Management
DDoS Distributed Denial of Service
DNS Domain Name Service
EMET Enhanced Mitigation Experience Toolkit
FISMA Federal Information Security Management Act
FTK Forensic Tool Kit
FTP File Transfer Protocol
HBSS Host Based Security System
HIDS Host Intrusion Detection System
HIPS Host Intrusion Prevention System
HR Human Resources
ICS Industrial Control Systems
IDS Intrusion Detection System
IMAP Internet Message Access Protocol
IOC Indicator of Compromise
IPS Intrusion Prevention System
ISO International Organization for Standardization
ITIL Information Technology Infrastructure Library
LDAP Lightweight Directory Access Protocol
MAC Mandatory Access Control
MD5 Message Digest 5
MOA Memorandum Of Agreement
MOU Memorandum Of Understanding
MRTG Multi Router Traffic Grapher
NAC Network Access Control
NAXSI Nginx Anti XSS & SQL Injection
NIC Network Interface Card
NIDS Network Intrusion Detection System
NIST National Institute of Standards & Technology
OEM Original Equipment Manufacturer
OSSIM Open Source Security Information Management
OWASP Open Web Application Security Project
PAM Pluggable Authentication Module
PCA Principal Component Analysis
PCI Payment Card Industry
PHI Protected Health Information
PII Personally Identifiable Information
RACI Responsible, Accountable, Consulted and Informed
RADIUS Remote Authentication Dial-In User Service
SABSA Sherwood Applied Business Security Architecture
SANS System Administration, Networking, and Security Institute
SCADA Supervisory Control and Data Acquisition
SCAP Security Content Automation Protocol
SDLC Software Development Life Cycle
SEO Search Engine Optimization
SHA Secure Hash Algorithm
SIEM Security Incident and Event Manager
SLA Service Level Agreement
SOC Security Operations Center
SPF Sender Policy Framework
SSH Secure Shell
SSL Secure Sockets Layer
TACACS+ Terminal Access Controller Access Control System Plus
TFTP Trivial File Transfer Protocol
TLS Transport Layer Security
TOGAF The Open Group Architecture Framework
USB Universal Serial Bus
VAS Vulnerability Assessment System
VDI Virtual Desktop Infrastructure
VLAN Virtual Local Area Network

VPN Virtual Private Network **WAF** Web Application Firewall

REFERENCES:

Maymí, F., & Chapman, B. (2018). CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). New York: McGraw-Hill Education. (Amazon)
Postel, J., *Internet Protocol* RFC 791. USC/Information Sciences Institute, September 1981.
Hinden, R. and S. Deering, *IPv6 Specification* RFC 2460. (December 1998).
Arkko, J. and S. Bradner, *IPv6 RH IANA Rules* RFC 5871. (May 2010).
CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives [PDF]. (2017, January). CompTIA Properties, LLC.
Gerhards, R., *The Syslog Protocol* RFC 5424. (March 2009)
NIST SP 800-62 R2
NIST SP 800-88 R1