Exam Report: 11.1.11 Practice Questions

Date: 5/11/2020 11:09:44 am
Time Spent: 5:56

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 36%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

An IT technician receives an IDS alert on the company network she manages. A seemingly random user now has administration privileges in the system, some files are missing, and other files seem to have just been created. Which of the following alerts did this technician receive?

- False positive
- False negative
- True negative
- True positive

Explanation

A true positive alert is when an event triggers an alarm and causes the IDS to react as if a real attack is in progress.

A false positive occurs if an event triggers an alarm when no actual attack is in progress.

A true negative is a condition that occurs when an IDS identifies an activity as acceptable behavior and the activity is authorized and accepted.

A false negative is a condition that occurs when an IDS fails to react to an actual attack event.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_IDS_ALERT_TYPE_01_EH1]

Question 2: Incorrect

An IDS can perform many types of intrusion detections. Three common detection methods are signature-based, anomaly-based, and protocol-based. Which of the following best describes protocol-based detection?

- This detection method notices when behavior goes outside an acceptable range.
- This detection compares behavior to baseline profiles or network behavior baselines.
- This detection method can include malformed messages and sequencing errors.
- ~~This detection method analyzes network traffic for common patterns referred to as signatures.~~

Explanation

Protocol-based detection can include malformed messages, sequencing errors, and similar variations from a protocol's known good behavior. Protocol detection can be useful against unknown or zero-day exploits, which might attempt to manipulate protocol behavior for malicious purposes.

A signature-based IDS analyzes network traffic for common patterns, referred to as signatures.

Anomaly-based detection compares behavior to baseline profiles or network behavior baselines.

Anomaly-based profiles are similar to a white list because the anomaly-based IDS detects when behavior goes outside an acceptable range.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_IDS_DETECTION_TYPE_01_EH1]

Question 3: Incorrect

Which of the following IDS detection types compare behavior to baseline profiles or network behavior baselines?

- ~~Signature-based~~
- Anomaly-based
- Cloud-based
- Protocol-based

Explanation

Anomaly-based detection compares behavior to baseline profiles or network behavior baselines. These baseline profiles are used to define what is normal behavior on the network or host.

A signature-based IDS analyzes network traffic for common patterns, referred to as signatures.

Protocol-based detection can include malformed messages, sequencing errors, and similar variations from a protocol's known good behavior.

Cloud-based computing resources such as platforms, applications, and storage are made available to the general public by a cloud service provider.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_IDS_DETECTION_TYPE_02_EH1]

Question 4: Correct

What are the two types of Intrusion Detection Systems (IDSs)?

- HIS and NIS
- HID and NID
- HIDS and NIDS
- HIP and NIP

Explanation

The different types of IDSs include Host Intrusion Detection Systems (HIDS) and Network Intrusion Detection Systems (NIDS).

Network Information Service (NIS) is a client's server directory service protocol for distributing system configuration data, such as user and host names between computers on a computer network.

Non-Impact Printer (NIP) is a printer that prints without banging a ribbon onto paper.

Network Interface Device (NID) is a device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring.

High-Intensity Discharge (HID) is an overarching term for a gas-discharge light.

Host Identity Protocol (HIP) is a host identification technology for use on Internet Protocol (IP) networks, such as the Internet.

Healthcare Information System (HIS) refers to a system designed to manage healthcare data.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_IDS_TYPE_01_EH1]

Question 5: Correct

You are on a Windows system. You receive an alert that a file named MyFile.txt.exe had been found. Which of the following could this indicate?

- Compliance-based IDS
- Host-based IDS
- Cloud-based IDS
- Network-based IDS

Explanation

The following is a list of host-based intrusion signs:

- Unknown files inserted into the system
- Altered file attributes
- Unrecognized file extensions such as .ODIN, .OZD, and .BUK in a Windows-based system
- Rogue suid or sgid files on a Linux system
- Changes to the file or folder metadata
- Changes to the hidden status of files
- New files that do not match the existing naming scheme

For example, if a file named FileName.txt.exe is discovered, in this case, this Windows file is an executable file and could potentially be malicious by tricking a user to click on it, thinking it was a text file.

Network intrusion signs are more focused on the network devices. These devices are routers, switches, firewalls, proxy servers, and the security software and security devices that protect the network.

Cloud-based computing resources, such as platforms, applications, and storage, are made available to the general public by a cloud service provider.

Compliance-based penetration testing ensures that the organization is in compliance with federal laws and regulations is a major purpose of performing a penetration test.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_AVOID_IDS_HOST_BASED_01_EH1]

Question 6: Incorrect

Which of the following is a sign of a network-based intrusion?

- New or unusual protocols and services running.
- Unknown files, altered file attributes, and/or alteration of the files themselves.
- Missing logs or logs with incorrect permissions/ownership.
- ~~Suspect, unrecognized file extensions, or double extensions.~~

Explanation

If you detect new or unusual protocols and services running, those are signs of possible network intrusion.

All of the other answers are signs of host-based intrusion.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_AVOID_IDS_NETWORK_BASED_01_EH1]

Question 7: Incorrect

ARP, DNS, and IP are all examples of which of the following?

- Session hijacking methods
- Spoofing methods
- ~~IDS detection methods~~
- Malware detection methods

Explanation

Common spoofing methods include Address Resolution Protocol (ARP), Domain Name Server (DNS), and Internet Protocol (IP). Spoofing is also used in email phishing schemes.

Using anti-malware software is one layer of system defense in detecting malware. These programs use a variety of methods to detect malware.

Session hijacking is usually done in one of three ways. Brute force hijacking is done by guessing an ID. This method is usually used if the hacker has some knowledge about the IDs being used by the server. An attacker could steal an ID using sniffing, or they could calculate an ID by looking at current session IDs and determining the sequencing algorithm being used.

An IDS can perform many types of intrusion detections. The three common methods you should know are signature-based detection, anomaly-based detection, and protocol-based detection.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_AVOID_IDS_PROTOCOL_ANOMALY_01_EH1]

Question 8: Correct

An attacker conducts a normal port scan on a host and detects protocols used by a Windows operating system and protocols used by a Linux operating system. Which of the following might this indicate?

- A honeypot
- A legitimate host
- Cache poisoning
- Protocol anomalies

Explanation

The likelihood of the scanned system to host standard Linux protocols and standard Windows protocols on ports at the same time may be an indicator of a honeypot rather than a legitimate host. A high-level honeypot simulates all services and applications.

Protocol anomalies can include malformed messages, sequencing errors, and similar variations from a protocol's known good behavior.

Cache poisoning attacks are one way to avoid IDS detection. Protocol detection requires the IDS to maintain its state information. This type of IDS deterrence can use the DNS service, which is a two-step process. Therefore, a protocol IDS can detect that when a number of DNS responses occur without a DNS request, this is cache poisoning.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_AVOID_IDS_PROTOCOL_ANOMALY_02_EH1]

Question 9: Correct

Which of the following is another name for the signature-based detection method?

- Identity detection
- Digital signature
- Obfuscation
- Misuse detection

Explanation

The signature-based detection method is also sometimes called misuse detection. The system compares traffic to known signatures in the signature file database. Remember, signature IDS systems rely on matching signatures to pattern traffic, or signature keys, in the signature file database.

Another method an attacker can use is obfuscation, which is changing the malicious code with the intent to disguise it as legitimate. Because an IDS relies on the ability to identify an attack signature, the process of obfuscating malicious code can be an effective evasion technique.

A digital signature adds increased protection by encrypting the signed email for confidentiality, which also serves as a means for nonrepudiation.

Integrity-based detection works by running a tool to scan a clean system to create a database. The integrity-based detection scans the system and compares the current scan to the clean database.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_AVOID_IDS_SIGN_DETECT_01_EH1]

Question 10: Incorrect

Ping of death, teardrop, SYN flood, Smurf, and fraggle are all examples of which of the following?

- ~~DoS attack prevention~~
- DoS attack categories
- DoS attack types
- DoS attack tools

Explanation

Some of the popular DoS attack types are:

- TCP fragmentation
- Ping flood
- Smurf attack
- Fraggle attack
- Phlashing
- SYN flood
- Ping of death
- Land attacks

The five general categories of denial-of-service attacks are:

- Fragmentation attacks
- Volumetric attacks
- Amplification attacks
- Application-level attacks
- Protocol attacks

Some of the DoS tools that can be used are:

- Trinoo
- Low Orbit Ion Cannon (LOIC)
- DoSHTTP
- UDPFlood

- Targa
- Jolt2
- Shark
- PlugBot
- Poison Ivy

The two ways to prevent DoS and DDoS attacks are to limit access points and limit services.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_EVADE_IDS_DOS_DDOS_ATTACK_01_EH1]

Question 11: Incorrect

Robin, an IT technician, has implemented identification and detection techniques based on the ability to distinguish legitimate traffic from illegitimate traffic over the network. Which of the following is he trying to achieve?

- Defend the network from attacks.
- Defend the network against natural disasters.
- ~~Defend the network against WPA/WPA2 cracking.~~
- Defend the network against IDS evasions.

Explanation

Identification and detection techniques based on the ability to detect and distinguish legitimate from illegitimate traffic can help play a part in defending a network against IDS evasions. Although countermeasures may not prevent the attack, they can help proactively detect attacks early on.

There are several methods for encrypting and authenticating packets, but Internet Protocol Security (IPsec) is one of the most common methods used to protect packet information and defend networks from attacks.

When working with a wireless network, always upgrade to WPA2 with AES/CCMP (or newer) encryption whenever possible. WPA2 provides per-frame or per-packet authentication. This means that each packet includes its own unique authentication. Despite the increase of security offered by WPA2, it can still be hacked if additional countermeasures are not taken.

To defend against natural disasters, your data center should be located in safe geographical area, you should have your backups at different locations, take mitigation measures, and have a disaster recovery plan.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_EVADE_IDS_IDS_EVASION_01_EH1]

Question 12: Incorrect

When it comes to obfuscation mechanisms, nmap has the ability to generate decoys, meaning that detection of the actual scanning system becomes much more difficult. Which of the following is the proper nmap command?

- **nmap -S RND:11** ***target_IP_address***
- ~~**nmap -D RND:01** ***target_IP_address***~~
- **nmap -D RND:10** ***target_IP_address***
- **nmap -S RND:20** ***target_IP_address***

Explanation

nmap has the ability to generate decoys, meaning that detection of the actual scanning system becomes much more difficult. The nmap command used to generate decoys is **nmap -D RND:10**

target_IP_address. This will generate a random number of decoys implementing another obfuscation evasion technique.

nmap -D RND:01 ***target_IP_address*** would not work; you always need to have more than one decoy.

nmap -S sends SYN packets, also called a half-open scan or stealth scan.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_EVADE_IDS_OBFUSCATION_01_EH1]

Question 13: Incorrect

Penetration testing is a practice conducted by an ethical hacker to see how an organization's security policies and security practices measure up to the organization's actual overall successful system security. When can an ethical hacker start the penetration test?

- Once you have had the project planning meetings and all the legal contracts are signed.
- Once all the legal contracts are signed, formalities are settled, and permissions are given.
- Once you have established an extensive plan, formalities are settled, and permissions are given.
- ~~Once all the legal contracts are signed and you scope out the penetration testing project.~~

Explanation

Penetration testing usually begins by establishing an extensive plan and scope of the penetration testing project. There are usually many project planning meetings between the penetration testers, organization system administrators, network administrators, and security personnel. Then, once all the legal contracts are signed, formalities are settled, and permissions are given, the actual testing can begin.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems
[e_ids_eh1.exam.xml Q_IDSPENTEST_FACT_02_EH1]

Question 14: Incorrect

Allen, the network administrator, needs a tool that can do network intrusion prevention and intrusion detection, capture packets, and monitor information. Which of the following tools would he most likely select?

- Cain & Abel
- ~~Nmap~~
- Snort
- Nessus

Explanation

Snort is an open-source network intrusion prevention system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, so it can detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

Nmap provides many commands and scripts that are used to evade firewalls and intrusion detection systems.

Nessus is often considered the industry standard for vulnerability scanning. The software helps to identify software flaws, malware, missing or outdated patches, and configuration errors across a network.

Cain and Abel is a collection of tools including ARP poisoning. Cain and Abel redirects packets from a target by forging ARP replies.

References

TestOut Ethical Hacker Pro - 11.1 Intrusion Detection Systems

[e_ids_eh1.exam.xml Q_IDSPENTEST_FACT_03_EH1]