

Exam Report: 11.3.7 Practice Questions

Date: 5/11/2020 12:27:40 pm
Time Spent: 16:30

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 36%

View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following is a physical or virtual network device set up to masquerade as a legitimate network resource?

- ☐ Server
- ☐ Switch
- ➡ ☒ Honeypot
- ☐ Firewall

Explanation

A honeypot's purpose is to look like a legitimate network resource to attract and occupy attackers. A honeypot can be a host, a service on a host, a network device, a virtual entity, or even a single file set up to attract attackers to a secure area away from an organization's real network.

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

A server is a computer, a device, or a program that is dedicated to managing network resources.

In an networking context, a switch is a high-speed device that receives incoming data packets and redirects them to their destinations on a local area network.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots
[e_honeypots_eh1.exam.xml Q_HONEYPOTS_FACT_01_EH1]

▼ Question 2: Correct

Which of the following best describes a honeypot?

- ☐ A honeypot is a substitute for an IDS or firewall and protects a system.
- ☐ Virtual honeypots can only simulate one entity on a single device.
- ☐ A honeypot is a server/client-based application that manipulates packets.
- ➡ ☒ A honeypot's purpose is to look like a legitimate network resource.

Explanation

A honeypot's purpose is to look like a legitimate network resource. A honeypot can be a host, a service on a host, a network device, a virtual entity, or even a single file set up to attract attackers to a secure area away from an organization's real network. Even better, while it's distracting the attacker, you can monitor the malicious activity to learn what the attacker is trying to do.

A honeypot is not a substitute for an IDS or firewall and doesn't protect a system.

Virtual honeypots are simulated on a physical device and are more cost-effective because you can simulate multiple entities on a single device.

Sebek is a server/client-based honeypot application that captures rootkits, and Snort inline is a modified version of Snort IDS that manipulates packets.


References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_HONEYPOTS_FACT_02_EH1]

▼ Question 3: Correct

Which of the following honeypot interaction levels simulate all service and applications and can be completely compromised by attackers to get full access to the system in a controlled area?

- ☐ Low-level
- ☐ Medium-level
-  ☒ High-level
- ☐ Critical-level

Explanation

A high-level honeypot simulates all services and applications and can be completely compromised by attackers to get full access to the system in a controlled area.

A low-level honeypot will simulate only a limited number of services and applications of a target system or network and relies on the emulation of services and programs that would be found on a vulnerable system.

A medium-level interaction honeypot simulates a real OS, applications, and services.

A critical-level is not a honeypot interaction level.


References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_HONEYPOTS_INTER_LEVEL_01_EH1]

▼ Question 4: Correct

Which of the following honeypot interaction levels can't be compromised completely and is generally set to collect information about attacks like network probes and worms?

- ☐ Critical-level
-  ☒ Low-level
- ☐ High-level
- ☐ Medium-level

Explanation

A low-level honeypot will simulate only a limited number of services and applications of a target system or network and rely on the emulation of services and programs that would be found on a vulnerable system. This means the honeypot can't be compromised completely and is generally set to collect information about attacks like network probes and worms.

A medium-level interaction honeypot simulates a real OS, applications, and services. This provides a better facade of an OS than low-interaction honeypots.

A high-level honeypot simulates all services and applications and can be completely compromised by attackers to get full access to the system in a controlled area.

Critical-level is not a honeypot interaction level.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_HONEYPOTS_INTER_LEVEL_02_EH1]

▼ Question 5: Incorrect

Mark, an ethical hacker, is looking for a honeypot tool that will simulate a mischievous protocol such as devil or mydoom. Which of the following honeypot tools should he use?

- ☒ ~~HoneyDrive~~
- ➡ ☐ HoneyBOT
- ☐ Honeyd
- ☐ KFSensor

Explanation

HoneyBOT is capable of simulating echo, ftp, telnet, smtp, http, POP3, and radmin, as well as a range of mischievous protocols such as devil, mydoom, lithium, blaster, netbus, and sub7.

KFSensor is a host-based intrusion detection system. It acts as a honeypot to attract and detect the hackers and worms by simulating vulnerable system services and Trojans.

HoneyDrive is a Linux-based Xubuntu-driven honeypot that includes pre-installed and pre-configured honeypot software and many useful pre-configured scripts and utilities to analyze, visualize, and process the data it captures.

Honeyd is a widely used honeypot. It makes it easy to create thousands of honeypots, and it can distract potential attackers.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_HONEYPOTS_TOOLS_01_EH1]

▼ Question 6: Incorrect

Frank, an attacker, has gained access to your network. He decides to cause an illegal instruction. He watches the timing to handle an illegal instruction. Which of the following is he testing for?

- ☐ A Snort inline
- ☐ A Tarpit
- ☒ ~~A Fake AP~~
- ➡ ☐ A virtual machine

Explanation

VMware is a commercially available virtual machine that is used to launch multiple instances of operating systems simultaneously on the same physical machine. The first step in detecting VMware is to look at the hardware, since VMware is supposed to emulate hardware. Some specific pieces of hardware attackers look for that are not configurable on some VMware are the video card, display adapter, and network card.

Another VMware detection method is to cause an illegal instruction. As the VMware's exceptions handler checks whether the instruction must be handled by VMware itself or by a specific handler, the attacker watches the timing to handle an illegal instruction. On a host OS system, the timing is usually 776mms; it increases to 2530mms inside running VMware.

Tarpits are an older honeypot technique that can operate at different levels of the OSI model, depending on their function.

Snort inline is a modified version of Snort IDS that is capable of packet manipulation.

Fake access points (Fake APs) are used to create fake 802.11b beacon frames with randomly generated ESSID and BSSID (MAC-address) assignments.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_EVADE_HONEYPOTS_DETECT_TOOLS_01_EH1]

▼ Question 7:

Incorrect

Julie is looking for a honeypot detection tool that is capable of packet manipulation. Which of the following tools should she use?

- ☐ Honeyd
- ☒ Sebek
- ☐ Bait and switch

➡ ☐ Snort inline

Explanation

A computer whose sole purpose is to listen for connection attempts on interesting ports, then log the data about each attempt is called a honeypot.

Snort inline is a modified version of Snort IDS, which is capable of packet manipulation.

Bait and switch is a technology that works with other IDS software, mainly Snort, to detour suspected malicious traffic into a honeypot that mirrors or closely resembles the real network without the attacker knowing.

Honeyd is a widely used honeypot. It can create thousands of honeypots easily. Honeyd can act as a distraction for potential attackers.

Sebek is a server/client-based honeypot application that captures rootkits and other malicious malware that hijacks read() system calls.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_EVADE_HONEYPOTS_DETECT_TOOLS_02_EH1]

▼ Question 8:

Incorrect

An attacker is attempting to determine whether a system is a honeypot. Which of the following actions should the attacker take?

- ➡ ☐ Craft a malicious probe packet to scan for services.
- ☐ Capture raw packet-level data, including the keystrokes.
- ☐ Simulate echo, FTP, Telnet, SMTP, HTTP, POP3, and Radmin.
- ☒ ~~Attempt to exploit or upload a rootkit or Trojan to a server.~~

Explanation

An attacker can detect the presence of honeypots by probing the services running on the system or crafting malicious probe packets to scan for services such as HTTP over SSL, SMTP over SSL, and IMAP over SSL. Ports that show a particular service running but deny a three-way handshake connection indicate the potential presence of a honeypot. When all else fails, you can often reach out to the ethical hacking community and utilize other hackers' knowledge and wisdom. If a honeypot cannot be detected, it cannot be evaded.

HoneyBOT is a decoy robot designed as a fully functional factory machine to attract hackers. It can simulate ICMP echo, FTP, Telnet, SMTP, HTTP, POP3, and Radmin protocols, as well as a range of malware such as Devil, Mydoom, Blaster, and Netbus.

Honeypots should be heavily monitored so you're aware of activity and you can see early warning signs of a larger attack. A honeypot's logging capability is far greater than other network security tools and captures raw packet-level data, including keystrokes made by attackers. The captured information is highly valuable because it contains malicious traffic with few false positives.

A honeypot's purpose is to look like a legitimate network resource. A honeypot can be a host, a service on a host, a network device, a virtual entity, or even a single file set up to attract attackers to a secure area away from an organization's real network. Even better, while it's distracting the attacker, you can monitor the malicious activity to learn what the attacker is trying to do. For example, if an attacker attempts an exploit or uploads a rootkit or Trojan to a server, the honeypot environment will safely store these files for malware collection and analysis.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_EVADE_HONEYPOTS_DETECT_TYPE_01_EH1]

▼ Question 9:

Incorrect

An older technique for defeating honeypots is to use tarpits, which sometimes operate at different levels of the OSI model, depending on their function. Which of the following layers of the OSI model do tarpits work at?

- ☒ ~~OSI layers 2 (Data Link), 3 (Network), and 4 (Transport)~~
- ☐ OSI layers 1 (Physical), 3 (Network), and 5 (Session)
- ☐ OSI layers 1 (Physical), 4 (Transport), and 6 (Presentation)
- ➡ ☐ OSI layers 2 (DataLink), 4 (Transport), and 7 (Application)

Explanation

Layer 7 (Application layer) tarpits act as security entities and are designed to respond to incoming packet requests slowly. Layer 4 (Transport layer) tarpits use the TCP/IP stack and slow the spread of worms, backdoors, and other attacks. Layer 2 (Data Link layer) tarpits can discover an attack from the same network and the same MAC address for multiple IP addresses.

Tarpits do not work at Layers 1 (Physical layer), 3 (Network layer), 5 (Session layer), or 6 (Presentation layer).

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_EVADE_HONEYPOTS_FACTS_01_EH1]

▼ Question 10:

Incorrect

User-Mode-Linux (UML) is an open-source tool used to create virtual machines. It's efficient for deploying honeypots. One of the big issues with UML is that it doesn't use a real hard disk, but a fake IDE device called `/dev/ubd*`. How can an attacker find a UML system?

- ☐ Attackers look for specific video cards, display adapters, and network cards.
- ➡ ☐ Attackers need to take a look at the `/etc/fstab` file or execute the `mount` command.
- ☒ ~~Attackers cause an illegal instruction, then watch how it is handled.~~
- ☐ Attackers detect a honeypot by measuring the execution time of the `read()` system call.

Explanation

You can find a UML system by looking at the `/etc/fstab` file, executing the `mount` command, or checking the `/dev/ubd/` directory. Another sign of a UML is the TUN/TAP backend for the network device 0 (zero). This isn't common on a real system, so it identifies a UML.

Another useful tool is VMware. VMware is a virtual machine software used to simultaneously launch multiple instances of operating systems on the same physical machine. To detect VMware, you have to look at the hardware, since VMware emulates it. Attackers look for specific video cards, display adapters, and network cards. Another VMware detection method is to cause an illegal instruction. As the VMware's exceptions handler checks to see if the instruction must be handled by VMware itself or by a specific handler, the attacker watches how the illegal instruction is handled. VMware takes longer to process the instruction than a host machine.

Sebek is a server/client-based honeypot application that captures rootkits and other malicious malware that hijacks read() system calls. You can detect Sebek by measuring the execution time of the read() system call.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_EVADe_HONEYPOTS_FACTS_02_EH1]

▼ Question 11:

Incorrect

Ports that show a particular service running but deny a three-way handshake connection indicate the potential presence of which of the following?

☒ Trojan

☐ Cavity

☐ Zombie

➡ ☐ Honeypot

Explanation

A computer whose sole purpose is to listen for connection attempts on interesting ports and log the data about each attempt is called a honeypot.

When a hacker finds a target machine but wants to avoid getting caught, so he will find another system to take the blame. This other system is frequently called a zombie machine because, to the hacker, it's disposable, and it creates a good distraction.

Hackers use Trojan horse programs quite extensively. A Trojan horse provides the hacker with covert remote access to the victim's system.

A cavity is also known as an overwriting virus. This virus fills in the empty space in a file or program without increasing the length of the file or affecting its functionality.

References

TestOut Ethical Hacker Pro - 11.3 Honeypots

[e_honeypots_eh1.exam.xml Q_EVADe_HONEYPOTS_FACTS_03_EH1]