Exam Report: 5.1.7 Practice Questions

Date: 1/20/2020 3:50:31 pm
Time Spent: 15:03

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following is the main difference between a DoS attack and a DDoS attack?

- ~~The DDoS attack uses an amplification network.~~
- The DDoS attack does not respond to SYN ACK packets in the three-way handshake process.
- The DDoS attack spoofs the source IP address.
- The DDoS attack uses zombie computers.

Explanation

The term denial of service (DoS) is a generic term that includes many types of attacks. In a DoS attack, a single attacker directs an attack at a single target, sending packets directly to the target. In a distributed DoS attack (DDoS), multiple PCs attack a victim simultaneously. DDoS compromises a series of computers by scanning computers to find vulnerabilities and capitalizing on the most vulnerable systems. In a DDoS attack:

- The attacker identifies one of the computers as the *master* (also known as *zombie master* or *bot herder*) .
- The master uses *zombies/bots* (compromised machines) to attack.
- The master directs the zombies to attack the same target.

A distributed reflective denial of service (DRDoS) uses an amplification network to increase the severity of the attack. Packets are sent to the amplification network addressed as coming from the target. The amplification network responds back to the target system.

Spoofed source addresses can be used with both DoS and DDoS attacks. A SYN flood is a form of DoS attack that does not complete the three-way handshake process. DDoS and even DRDoS attacks could use this method to overload the target system.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_01]

Question 2: Correct

Which of the following are denial of service attacks? (Select two.)

- [x] Smurf
- [ ] Hijacking
- [ ] Salami
- [x] Fraggle

Explanation

Smurf and Fraggle attacks are both denial of service attacks. A smurf attack spoofs the source address in ICMP packets and sends the ICMP packets to an amplification network (bounce site). The bounce site responds to the victim site with thousands of messages that he did not send. A Fraggle attack is similar to a Smurf attack, but uses UDP packets directed to port 7 (echo) and port 19 (chargen - character generation).

A salami attack is not a denial of service attack. A salami attack is when a small amount of information, data, or valuables are taken over a period of time. The result is to construct or obtain data or property of great value. A common example of a salami attack is to deposit the fractions of cents from an accounting program into a numbered account. Eventually, the fraction deposits total a significant sum. Hijacking is an attack directed at authentication. Hijacking is stealing an open and active communication session from a legitimate user (an extension of a man-in-the-middle attack). The attacker takes over the session and cuts off the original source device.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_03]

Question 3: Correct

Which attack form either exploits a software flaw or floods a system with traffic in order to prevent legitimate activities or transactions from occurring?

- (✓) Denial of service attack
- ( ) Brute force attack
- ( ) Privilege escalation
- ( ) Man-in-the-middle attack

Explanation

A denial of service attack either exploits a software flaw or floods a system with traffic in order to prevent legitimate activities or transactions from occurring.

A brute force attack tries every valid key or code sequenced in an attempt to discover a password or encryption key. Brute force attacks are always successful given enough time (although enough time could be millennia). A man-in-the-middle attack involves a third party placing themselves between two legitimate communication partners in order to intercept and possibly alter their transmissions. Privilege escalation is stealing or obtaining high-level privileges in a computer system.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_04]

Question 4: Correct

As the victim of a Smurf attack, what protection measure is the most effective during the attack?

- ( ) Block all attack vectors with firewall filters
- ( ) Turn off the connection to the ISP
- ( ) Update your anti-virus software
- (✓) Communicate with your upstream provider

Explanation

The most effective protection measure the victim of a Smurf attack can perform during an attack is to communicate with upstream providers. A simple phone call to request filtering on your behalf can weaken the effectiveness of a Smurf attack.

Turning off the connection to the ISP will result in the same effect of the Smurf attack itself - denial of service. Whether you disconnect or the attack disconnects you, your network will be unable to use its internet pipeline. Blocking all attack vectors with firewall filters will usually result in a self-imposed

denial of service, since most Smurf attacks produce thousands of attack vectors for the inbound flooding packets. Updating your anti-virus software will have no effect on a Smurf attack.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_05]

Question 5: Incorrect

You suspect that an Xmas tree attack is occurring on a system. Which of the following could result if you do not stop the attack? (Select two.)

- [x] The threat agent will obtain information about open ports on the system.
- [ ] The system will send packets directed with spoofed source addresses.
- [ ] The system will be unavailable to respond to legitimate requests.
- [ ] The system will become a zombie.

Explanation

A Christmas (Xmas) tree attack (also known as a Christmas tree scan, nastygram, kamikaze, or lamp test segment) conducts reconnaissance by scanning for open ports. It also conducts a DoS attack if sent in large amounts.

- When it is sent to a target host, the TCP header of a Christmas tree packet has the flags FIN, URG, and PSH. By default, closed ports on the host are required to reply with a TCP connection reset flag (RST). Open ports must ignore the packets, informing the attacker which ports are open.
- Christmas tree packets require much more processing by network devices compared to typical packets, producing DoS attacks when large amounts are sent to the target host.

A *Fraggle* attack sends a large amount of UDP packets with spoofed source addresses. A Distributed DoS (DDoS) attack compromises many computers and turns them into zombies for a concentrated attack.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_06]

Question 6: Correct

You need to enumerate the devices on your network and display the network's configuration details.

Which of the following utilities should you use?

- ( ) **nslookup**
- ( ) **neotrace**
- ( ) **samspade**
- (•) **nmap**

Explanation

Nmap is an open-source security scanner used for network enumeration and to the creation of network maps. **Nmap** sends specially-crafted packets to the target host and then analyzes the responses to create the map.

Use **neotrace** or **traceroute** to trace the devices in a network path between two hosts. Use **samspade** to identify the source of spam emails. Use **nslookup** to submit name resolution requests to identify DNS name servers and IP addresses for hosts.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_08]

Question 7: Correct

An attacker is conducting passive reconnaissance on a targeted company. Which of the following could he be doing?

- Scanning ports
- War driving
- Browsing the organization's website
- War dialing
- Social engineering

Explanation

Browsing the organization's website is a form of passive reconnaissance. Other forms of passive reconnaissance include putting a sniffer on the wire or eavesdropping on employee conversations.

Social engineering, war driving, war dialing, and scanning ports are all forms of active scanning.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_09]

Question 8: Incorrect

Which type of active scan turns off all flags in a TCP header?

- Null
- Christmas tree
- FIN
- Stealth

Explanation

A *null* scan turns off all flags in a TCP header, creating a lack of TCP flags that should never occur in the real world.

A FIN scan sends TCP packets to a device without first going through the normal TCP handshaking, thus preventing non-active TCP sessions from being formally closed. A stealth scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfers with the expectation of receiving a single response. A Christmas tree scan sends a TCP frame to a remote device with the URG, PUSH, and FIN flags set.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_10]

Question 9: Correct

Which of the following denial of service (DoS) attacks uses ICMP packets and is only successful if the victim has less bandwidth than the attacker?

- Ping flood
- LAND
- Ping of death
- Fragmentation

Explanation

A *ping flood* is where the attacker overwhelms the victim with ICMP Echo Request (ping) packets. In a ping flood, the attack succeeds only if the attacker has more bandwidth than the victim.

The *ping-of-death* attack (also known as a *long ICMP* attack) uses the Ping program to send oversized ICMP packets. A *LAND* attack floods the victim's system with packets that have forged headers. *Fragmentation* attacks contaminate IP packet fragments that infiltrate the system.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_11]

Question 10: Correct

In which of the following denial of service (DoS) attacks does the victim's system rebuild invalid UDP packets, causing the system to crash or reboot?

- Banana
- Teardrop
- NACK
- Deauth

Explanation

In a *Teardrop* attack, fragmented UDP packets with overlapping offsets are sent. Then, when the victim system re-builds the packets, an invalid UDP packet is created, causing the system to crash or reboot.

A *Negative Acknowledgment* (NACK) attack denies a LAN/WAN client access to resources. A *Banana* attack uses a router to change the destination address of a frame. A *deauthentication* (Deauth) attack denies wireless clients access to resources.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_12]

Question 11: Incorrect

A SYN packet is received by a server. The SYN packet has the exact same address for both the sender and receiver addresses, which is the address of the server. This is an example of what type of attack?

- Land attack
- Ping of death
- ~~SYN flood~~
- Teardrop attack

Explanation

A land attack is when the SYN packet has the exact same address for both the sender and receiver addresses, which is the address of the server.

The ping of death involves an ICMP packet that is larger than 65,536 bytes. The teardrop attack uses partial IP packets with overlapping sequencing numbers. A SYN flood exploits or attacks the ACK packet of the TCP three-way handshake. By not sending the final ACK packet, the server holds open an incomplete session, consuming system resources. If the attacker can cause the server to open numerous sessions in this manner, all system resources are consumed, and no legitimate connections are established.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_13]

Question 12: Incorrect

Which of the following is a form of denial of service attack that uses spoofed ICMP packets to flood a victim with echo requests using a bounce/amplification network?

- Smurf

- ~~Fraggle~~
- Fingerprinting
- Session hijacking

Explanation

Smurf is a form of denial of service attack that uses spoofed ICMP packets to flood a victim with echo requests using a bounce/amplification network.

Fingerprinting is the act of identifying an operating system or network service based upon its ICMP message quoting characteristics. A fraggle attack uses spoofed UDP packets to flood a victim with echo requests using a bounce network, which makes it similar to Smurf. Session hijacking is the act of taking over a login session from a legitimate client, impersonating the user and taking advantage of their established communication link.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_15]

Question 13: Incorrect

A SYN attack or SYN flood exploits or alters which element of the TCP three-way handshake?

- ACK
- ~~SYN~~
- SYN/ACK
- FIN or RES

Explanation

A SYN attack or SYN flood exploits or attacks the ACK packet of the TCP three-way handshake. By not sending the final ACK packet, the server holds open an incomplete session, consuming system resources. If the attacker can cause the server to open numerous sessions in this manner, all system resources are consumed, and no legitimate connections are established.

A SYN attack or SYN flood must send the initial SYN packet with no malicious content, other than the possibility of spoofing the source address to hide the attacker's identity or location. The SYN/ACK packet is sent by the server; therefore, the attacker cannot modify or alter this element of the handshake. The FIN or RES packet is not part of the handshake or part of the SYN flood or SYN attack process. These packets are often used legitimately to end communication sessions. However, they can be used in other forms of attack to disable communications maliciously.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_16]

Question 14: Correct

When a SYN flood is altered so that the SYN packets are spoofed in order to define the source and destination address as a single victim IP address, the attack is now called what?

- Analytic attack
- Fraggle attack
- Impersonation
- Land attack

Explanation

A land attack is a SYN flood where the source and destination address of the SYN packets are both

defined as the victim's IP address.
A fraggle attack uses UDP packets, not SYN packets from TCP. An impersonation attack is not usually a protocol attack; it is simply taking on an authorized identity in order to gain entry into a secured environment. An analytic attack is an attack on the algorithm of a cryptography system.

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_17]

Question 15: Correct

Which of the following best describes the ping of death?

- Sending multiple spoofed ICMP packets to the victim
- Partial IP packets with overlapping sequencing numbers
- An ICMP packet that is larger than 65,536 bytes
- Redirecting echo responses from an ICMP communication

Explanation

The ping of death involves an ICMP packet that is larger than 65,536 bytes.

The teardrop attack uses partial IP packets with overlapping sequencing numbers. The Smurf attack sends multiple spoofed ICMP packets to the victim. The ability to re-direct echo responses is a feature of ICMP that is often involved in malicious attacks (but is not part of the ping of death).

References

LabSim for Security Pro, Section 5.1.
[All Questions SecPro2017_v6.exm RECON_DENIAL_18]