Exam Report: 10.3.13 Practice Questions

Date: 5/11/2020 10:33:32 am
Time Spent: 13:19

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 62%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Which of the following best describes the key difference between DoS and DDoS?

○ Results in the server being inaccessible to users.

○ Sends a large number of legitimate-looking requests.

➡ ● Attackers use numerous computers and connections.

○ The target server cannot manage the capacity.

Explanation

The DoS attacks that you probably hear the most about are distributed denial-of-service attacks (DDoS). The key difference is these attacks use numerous computers and numerous internet connections across the world to overload the target systems. DDoS attacks are usually executed through a network of devices that the attacker has gained control of.

DoS attacks use a single connection to attack a single target. With all DoS attacks, the attacker sends a large number of legitimate-looking requests to the server in a way that the server cannot determine which requests are valid and which are not. This barrage of requests will overwhelm the system to the point that the server cannot manage the capacity, resulting in the server being inaccessible to other users.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DENIEL_OF_SERVICE_FACT_01_EH1]

Question 2: Incorrect

An attacker may use compromised websites and emails to distribute specially designed malware to poorly secured devices. This malware provides an access point to the attacker, which he can use to control the device. Which of the following devices can the attacker use?

➡ ○ Any device that can communicate over the intranet can be hacked.

○ Only servers and workstations on the intranet can be hacked.

● ~~Only servers and routers on the Internet can be hacked.~~

○ Only routers and switches on the Internet can be hacked.

Explanation

With the advancement of the Internet of Things, it's important to note that zombie devices aren't limited to desktops and laptops. Any device that can communicate over the Internet can be hacked. This includes security cameras, DVR players, and even kitchen appliances.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DENIEL_OF_SERVICE_FACT_02_EH1]

Question 3: Correct

Which of the following motivates attackers to use DoS and DDoS attacks?

○ Distraction, extortion, and theft

○ Distraction, turf wars, and fun

○ Hacktivism, turf wars, and profit

➡ ◉ Hacktivism, profit, and damage reputation

Explanation

The following are motivation for DoS and DDoS Attacks:

- Distraction
- Damage reputation
- Hacktivism
- Fun
- Profit

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DENIEL_OF_SERVICE_MOTIVATION_01_EH1]

Question 4: Incorrect

Which of the following is an attack where all traffic is blocked by taking up all available bandwidth between the target computer and the Internet?

○ Fragmentation attack

➡ ○ Volumetric attack

◉ ~~Amplification attack~~

○ Phlashing attack

Explanation

Volumetric attacks block traffic by taking up all available bandwidth between the target and the Internet.

Fragmentation attacks target a system's ability to reassemble fragmented packets.

Amplification attacks exploit vulnerabilities in protocols and broadcast networks. The name is derived from the idea that the attacker uses intermediary computers and networks to amplify the impact of their attack.

Phlashing, also known as bricking, involves pushing incorrect updates to a system's firmware, causing irreversible damage and rendering the device about as useful as a brick.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_ATTACKS_CATEGORIES_01_EH1]

Question 5: Correct

Which of the following tools can be used to create botnets?

○ Poison Ivy, Targa, and LOIC

○ Trin00, Targa, and Jolt2

○ Jolt2, PlugBot, and Shark

➡ ● Shark, PlugBot, and Poison Ivy

Explanation

Botnets are typically used to carryout DoS and DDoS attacks. You can use the following tools to create botnets:

- Shark
- PlugBot
- Poison Ivy

Trin00 is a set of programs used for DoS attacks.

Jolt2 is a DoS tool that sends numerous fragmented packets to a Windows machine.

Targa is a multifunctional tool that can execute WinNuke and teardrop attacks.

Low Orbit Ion Cannon (LOIC) is a free and easy to use DoS tool.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_ATTACKS_TOOLS_01_EH1]

Question 6: Incorrect

A hacker has discovered UDP protocol weaknesses on a target system. The hacker attempts to send large numbers of UDP packets from a system with a spoofed IP address, which broadcasts out to the network in an attempt to flood the target system with an overwhelming amount of UDP responses. Which of the following DoS attacks is the hacker attempting to use?

● ~~SYN flood~~

➡ ○ Fraggle attack

○ Smurf attack

○ Teardrop attack

Explanation

A fraggle attack is a DoS attack that targets UDP protocol weaknesses. A large number of UDP packets from a spoofed IP address are broadcast to a network in an attempt to flood the target computer.

A Smurf attack is a DoS attack that targets ICMP protocol weaknesses.

A SYN flood exploits the TCP three-way handshake. An attacker creates SYN packets with a non-existent source address. When the target machine responds with a SYN-ACK, it goes to the non-existent address, causing the target machine to wait for a response that they will never get.

A Teardrop attack prevents TCP/IP packets from being reassembled. This is done by setting the flags on all frames to indicate that they are fragments and providing instructions to connect to another frame that doesn't actually exist.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_ATTACKS_TYPES_01_EH1]

Question 7: Correct

The ping command is designed to test connectivity between two computers. There are several command options available to customize ping, making it a useful tool for network administrators. On Windows, the default number of ping requests is set is four. Which of the following command options will change the default number of ping requests?

➡ ● **-n**

○ **-a**

○ **-l**

○ **-f**

Explanation

ping -n defines the number of echo requests to send.

ping -a is used to resolve adresses to hostnames.

ping -l is used to send the buffer size.

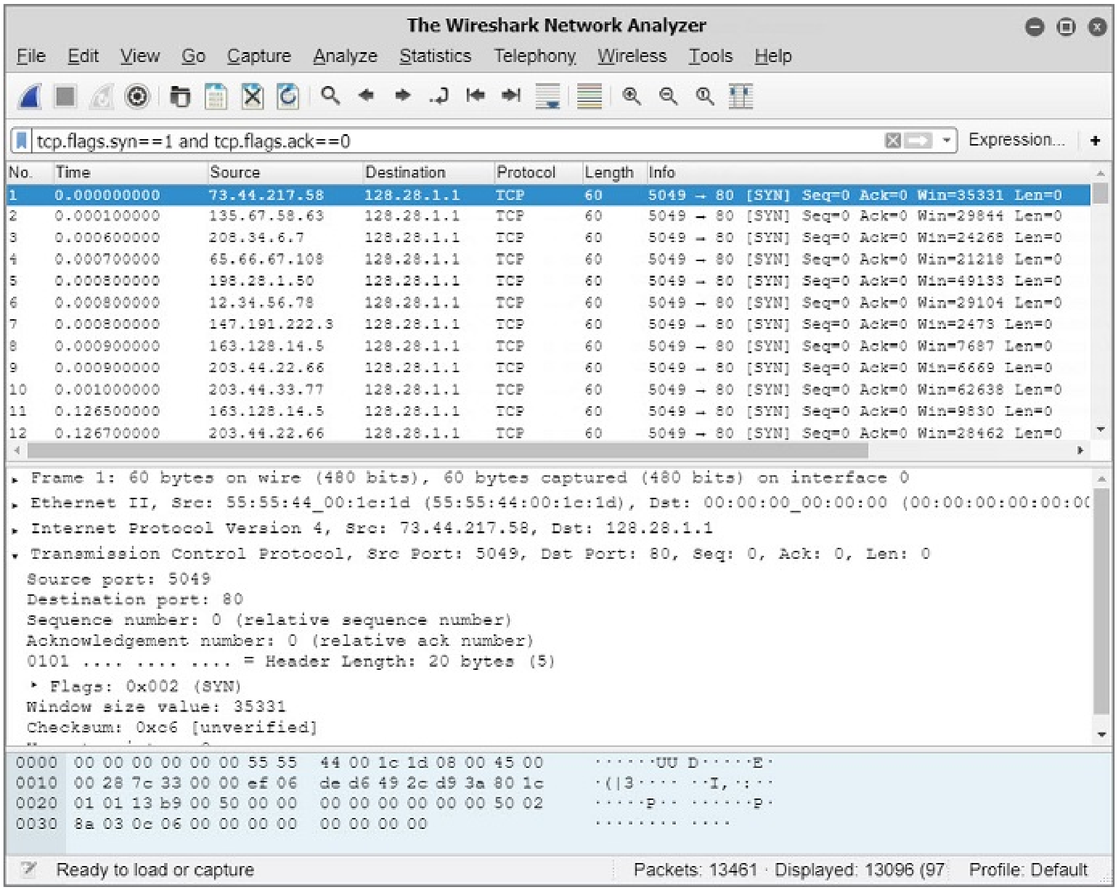
ping -f is used to set the don't fragment flag in packet.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_ATTACKS_TYPES_02_EH1]

Question 8: Correct

You are using Wireshark to try and determine if a denial-of-service (DDoS) attack is happening on your network (128.28.1.1). You previously captured packets using the tcp.flags.syn==1 and tcp.flags.ack==1 filter, but only saw a few SYN-ACK packets. You have now changed the filter to tcp.flags.syn==1 and tcp.flags.ack==0. After examining the Wireshark results shown in the image, which of the following is the best reason to conclude that a DDoS attack is happening?



```
tcp.flags.syn==1 and tcp.flags.ack==0

No. Time         Source          Destination  Protocol Length Info
1   0.000000000  73.44.217.58    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=35331 Len=0
2   0.000100000  135.67.58.63    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=29844 Len=0
3   0.000600000  208.34.6.7      128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=24268 Len=0
4   0.000700000  65.66.67.108    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=21218 Len=0
5   0.000800000  198.28.1.50     128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=49133 Len=0
6   0.000800000  12.34.56.78     128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=29104 Len=0
7   0.000800000  147.191.222.3   128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=2473 Len=0
8   0.000900000  163.128.14.5    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=7687 Len=0
9   0.000900000  203.44.22.66    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=6669 Len=0
10  0.001000000  203.44.33.77    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=62638 Len=0
11  0.126500000  163.128.14.5    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=9830 Len=0
12  0.126700000  203.44.22.66    128.28.1.1   TCP      60     5049 → 80 [SYN] Seq=0 Ack=0 Win=28462 Len=0

▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: 55:55:44_00:1c:1d (55:55:44:00:1c:1d), Dst: 00:00:00_00:00:00 (00:00:00:00:00:0(
▸ Internet Protocol Version 4, Src: 73.44.217.58, Dst: 128.28.1.1
▾ Transmission Control Protocol, Src Port: 5049, Dst Port: 80, Seq: 0, Ack: 0, Len: 0
   Source port: 5049
   Destination port: 80
   Sequence number: 0 (relative sequence number)
   Acknowledgement number: 0 (relative ack number)
   0101 .... .... .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x002 (SYN)
   Window size value: 35331
   Checksum: 0xc6 [unverified]

0000  00 00 00 00 00 00 55 55  44 00 1c 1d 08 00 45 00   ······UU D·····E·
0010  00 28 7c 33 00 00 ef 06  de d6 49 2c d9 3a 80 1c   ·(|3···· ··I,·:··
0020  01 01 13 b9 00 50 00 00  00 00 00 00 00 00 50 02   ·····P·· ······P·
0030  8a 03 0c 06 00 00 00 00  00 00 00 00              ········ ····

Ready to load or capture          Packets: 13461 · Displayed: 13096 (97     Profile: Default
```

○ The Transmission Control Protocol shows the hex value of the SYN flag is 0x002.

○ There was a flood of SYN packets without a matching SYN-ACK packet.

➡ ● There are multiple SYN packets with different source addresses destined for 128.28.1.1.

○ The source address for all SYN packets is 198.28.1.1.

Explanation

The captured and filtered packets show many SYN packets being sent from many different sources, but all destined for the same target or destination address. This is a strong indication that a DDoS attack is currently happening.

Whether they are legitimate or created by a hacker, SYN packets have a hex value of 0x002.

Since a DDoS flood is happening, there isn't time or bandwidth available to see many (if any) matching SYN-ACK packets.

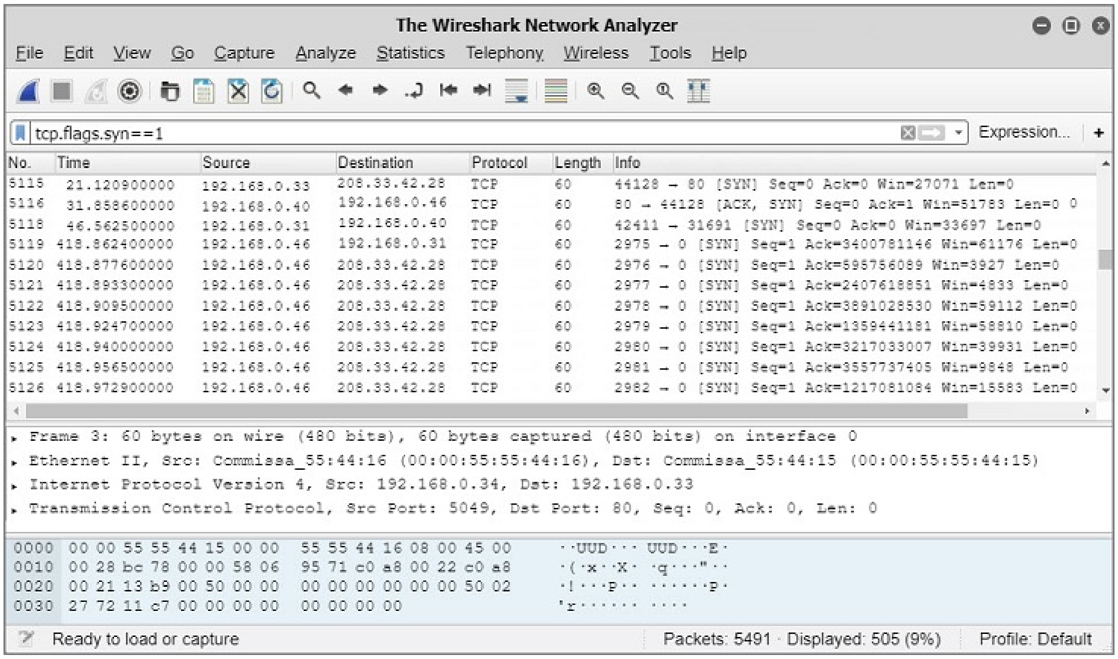
References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_ATTACKS_WIRESHARK_DDOS_ATTACK_01_EH1]

Question 9: Correct

You suspect that an ICMP flood attack is taking place from time to time, so you have used Wireshark to capture packets using the tcp.flags.syn==1 filter. Initially, you saw an occasional SYN or ACK packet. After a short while, however, you started seeing packets as shown in the image.

Using the information shown, which of the following explains the difference between normal ICMP (ping) requests and an ICMP flood?



```
tcp.flags.syn==1
```

```
No.   Time          Source         Destination     Protocol  Length  Info
5115   21.120900000  192.168.0.33   208.33.42.28    TCP       60      44128 → 80 [SYN] Seq=0 Ack=0 Win=27071 Len=0
5116   31.858600000  192.168.0.40   192.168.0.46    TCP       60      80 → 44128 [ACK, SYN] Seq=0 Ack=1 Win=51783 Len=0 0
5118   46.562500000  192.168.0.31   192.168.0.40    TCP       60      42411 → 31691 [SYN] Seq=0 Ack=0 Win=33697 Len=0
5119  418.862400000  192.168.0.46   192.168.0.31    TCP       60      2975 → 0 [SYN] Seq=1 Ack=3400781146 Win=61176 Len=0
5120  418.877600000  192.168.0.46   208.33.42.28    TCP       60      2976 → 0 [SYN] Seq=1 Ack=595756089 Win=3927 Len=0
5121  418.893300000  192.168.0.46   208.33.42.28    TCP       60      2977 → 0 [SYN] Seq=1 Ack=2407618851 Win=4833 Len=0
5122  418.909500000  192.168.0.46   208.33.42.28    TCP       60      2978 → 0 [SYN] Seq=1 Ack=3891028530 Win=59112 Len=0
5123  418.924700000  192.168.0.46   208.33.42.28    TCP       60      2979 → 0 [SYN] Seq=1 Ack=1359441181 Win=58810 Len=0
5124  418.940000000  192.168.0.46   208.33.42.28    TCP       60      2980 → 0 [SYN] Seq=1 Ack=3217033007 Win=39931 Len=0
5125  418.956500000  192.168.0.46   208.33.42.28    TCP       60      2981 → 0 [SYN] Seq=1 Ack=3557737405 Win=9848 Len=0
5126  418.972900000  192.168.0.46   208.33.42.28    TCP       60      2982 → 0 [SYN] Seq=1 Ack=1217081084 Win=15583 Len=0
```

```
▸ Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Commissa_55:44:16 (00:00:55:55:44:16), Dst: Commissa_55:44:15 (00:00:55:55:44:15)
▸ Internet Protocol Version 4, Src: 192.168.0.34, Dst: 192.168.0.33
▸ Transmission Control Protocol, Src Port: 5049, Dst Port: 80, Seq: 0, Ack: 0, Len: 0
```

```
0000  00 00 55 55 44 15 00 00  55 55 44 16 08 00 45 00   ··UUD··· UUD···E·
0010  00 28 bc 78 00 00 58 06  95 71 c0 a8 00 22 c0 a8   ·(·x··X· ·q···"··
0020  00 21 13 b9 00 50 00 00  00 00 00 00 00 00 50 02   ·!···P·· ······P·
0030  27 72 11 c7 00 00 00 00  00 00 00 00               'r······ ····
```

Ready to load or capture   Packets: 5491 · Displayed: 505 (9%)   Profile: Default

- ● With the flood, all packets come from the same source IP address in quick succession.
- ○ The normal ICMP ping request only has one source address.
- ○ The only difference is the number of packets that are sent.
- ○ With the ICMP flood, ICMP packets are sent and received at a quicker rate than normal ICMP packets.

Explanation

In comparison to the occasional ICMP ping requests that can be seen on a network, when an ICMP flood attack is happening, the ICMP packets are sent in quick succession from the same source IP address. As a result, there is little bandwidth available to receive many (if any) ACK or SYN packets.

As can be seen from the packets captured, normal ICMP packets can come from different source addresses, such as 192.168.0.33 and 192.168.0.31.

The ping command will send 4 by default if -n isn't used.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_ATTACKS_WIRESHARK_ICMP_FLOOD_01_EH1]

Question 10: Correct

Which of the following best describes a DoS attack?

○ A hacker penetrates a system by using every character, word, or letter to gain access.

➡ ● A hacker overwhelms or damages a system and prevents users from accessing a service.

○ A hacker attempts to impersonate an authorized user by stealing the user's token.

○ A hacker intercepts traffic between two systems to gain access to a system.

Explanation

A DoS attack is an attack on the availability of a service by disrupting, denying, or otherwise interfering with the ability to keep a service available. The more you understand what a DoS attack is and what can happen, the better prepared you are to use countermeasures.

Impersonating an authorized user by gaining access to their tokens is a way to gain unauthorized access by using a cryptographic attack.

Using every character, word, or letter to gain unauthorized access is also known as a brute-force attack.

Intercepting traffic is a type of sniffing, which does not cause a DoS attack.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_COUNTER_ATTACK_PREVENT_01_EH1]

▼ **Question 11:** Incorrect

Which of the following best describes a reverse proxy method for protecting a system from a DoS attack?

○ Limits the potential impact of a DoS attack by providing additional response time.

➡ ○ Redirects all traffic before it is forwarded to a server, so the redirected system takes the impact.

● ~~Creates an area of the network where offending traffic is forwarded and dropped.~~

○ Adds extra services so that there are too many platforms for the attacker to be able to flood.

Explanation

When a DoS attack occurs and a proxy server takes the impact, this is known as a Reverse Proxy DoS protection method. This method redirects all traffic to the reverse proxy before it is forwarded to the real server.

Creating an area of the network called a black hole, where offending traffic is forwarded and dropped, is another attack protection method called Black Hole Filtering.

Enabling router throttling can limit the potential impact of a DoS attack and can provide a bit of additional time for administrators to respond to an attack.

Adding extra services, such as load balancing and excess bandwidth, can help provide too many platforms for the attacker to be able to flood. This method is called absorbing the attack.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_COUNTER_ATTACK_PROTECT_01_EH1]

▼ **Question 12:** Correct

Creating an area of the network where offending traffic is forwarded and dropped is known as _________?

○ Enable router throttling

○ Reverse proxy

○ Anti-spoofing measures

➡ ● Black hole filtering

Explanation

Black hole filtering creates an area of the network called a black hole where offending traffic is forwarded and dropped.

Router throttling limits the potential impact of a DoS attack and can provide a bit of additional time for administrators to respond to an attack.

All traffic is redirected to the reverse proxy before being forwarded to the real server. In the event of an attack, the proxy takes the impact.

Anti-spoofing measures ensure that spoofed packets are unable to infiltrate your network.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_COUNTER_ATTACK_PROTECT_02_EH1]

▼ **Question 13:** Incorrect

It is important to be prepared for a DoS attack. These attacks are becoming more common. Which of the following best describes the response you should take for a service degradation?

○ Add extra services, such as load balancing and excess bandwidth.

➡ ○ Services can be set to throttle or even shut down.

● ~~Have more than one upstream connection to use as a failover.~~

○ Include a checklist of all threat assessment tools.

Explanation

To respond to a service degradation, services can be set to throttle or even shut down in the event of an attack.

You should have more than one upstream connection to use as a failover in the event of a flooding attack.

To absorb an attack, add extra services such as load balancing and excess bandwidth so that you have too much on your network for the attacker to execute a flood attack.

Your response plan should include a checklist of all the threat assessment tools and hardware protections that you have in place.

References

TestOut Ethical Hacker Pro - 10.3 Denial of Service
[e_denial_of_service_eh1.exam.xml Q_DOS_COUNTER_ATTACK_RESPONSE_01_EH1]