Exam Report: 10.1.17 Practice Questions

Date: 5/5/2020 8:03:52 pm
Time Spent: 8:01

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 29%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following are network sniffing tools?

○ WinDump, KFSensor, and Wireshark

○ Ufasoft snif, TCPDump, and Shark

● ~~Ettercap, Ufasoft snif, and Shark~~

➡ ○ Cain and Abel, Ettercap, and TCPDump

Explanation

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

Ettercap is a sniffing tool with multiple functions that can be used for ARP poisoning, passive sniffing, packet grabbing, and protocol decoding.

TCPDump is a command line sniffer designed for the Linux environment.

Ufasoft snif is a sniffing tool that has capturing, analyzing, and decryption features.

WinDump is the windows version of TCPdump.

Wireshark is a network packet analyzer that tries to capture network packets and display the data they carry in as much detail as possible.

Shark is a tool that is used to create botnets.

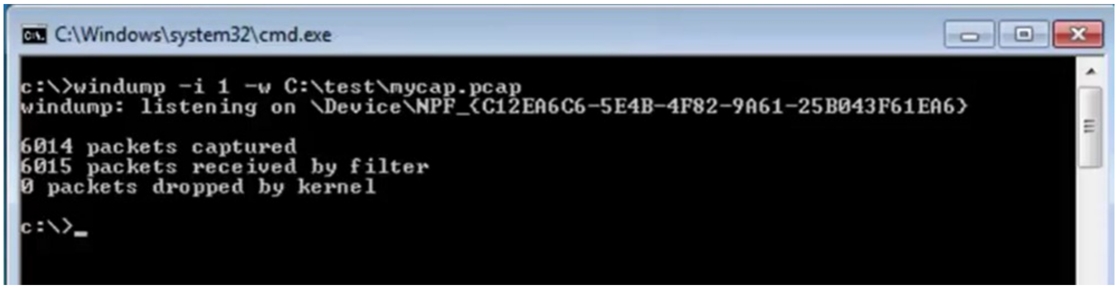
KFSensor is a Windows host-based intrusion detection system. It acts as a vulnerable server to attract hackers and record their activities.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_ADD_SNIFF_TOOLS_01_EH1]

Question 2: Incorrect

Which of the following actions was performed using the WinDump command line sniffer?



```
c:\>windump -i 1 -w C:\test\mycap.pcap
windump: listening on \Device\NPF_{C12EA6C6-5E4B-4F82-9A61-25B043F61EA6}

6014 packets captured
6015 packets received by filter
0 packets dropped by kernel

c:\>_
```

● ~~Requested that hexadecimal strings be included from interface 1 to mycap.pcap.~~

○ Read packet capture files from interface 1 in mycap.pcap file.

○ Requested that asci strings are included from interface 1 to mycap.pcap.

➡ ○ Wrote packet capture files from interface 1 into mycap.pcap.

Explanation

The command line request is to collect packet capture files from -I (interface) and -w (write) them to the C:\test\mycap.pcap file.

The read request on interface 1 would be **-I 1 -r C:\test\mycap.pcap**.

The hexadecimal string output is the -x option, which is not requested in this capture command.

The asci string output is the -a option, which is not requested in this capture command.

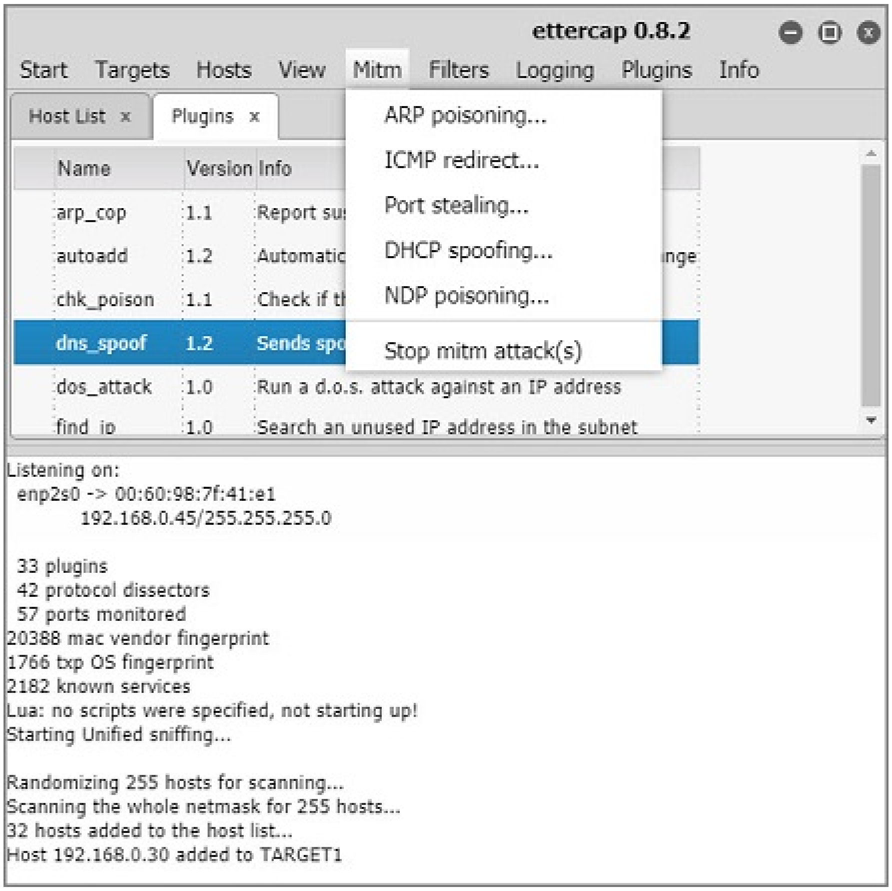
References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_ADD_SNIFF_TOOLS_02_EH1]

Question 3: Correct

As part of your penetration test, you are using Ettercap in an attempt to spoof DNS. You have configured the target and have selected the dns_spoof option (see image).

To complete the configuration of this test, which of the following MITM options should you select?



Name	Version	Info
arp_cop	1.1	Report su
autoadd	1.2	Automatic … nge
chk_poison	1.1	Check if th
dns_spoof	1.2	Sends spo
dos_attack	1.0	Run a d.o.s. attack against an IP address
find_ip	1.0	Search an unused IP address in the subnet

```
Listening on:
 enp2s0 -> 00:60:98:7f:41:e1
        192.168.0.45/255.255.255.0

 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
32 hosts added to the host list...
Host 192.168.0.30 added to TARGET1
```

➡ ● ARP poisoning

○ Port stealing

○ DHCP spoofing

○ NDP poisoning

Explanation

To successfully complete the configuration of your DNS spoofing test, you need to select the ARP poisoning option. ARP requests and replies are sent to victims to poison their ARP cache. Once the cache has been poisoned, the victim sends all packets to the attacker, who modifies them and forwards them to the real destination.

Port stealing is used to sniff a switched environment when ARP poisoning is not effective (for example, where static mapped ARPs are used).

DHCP spoofing pretends to be a DHCP server and tries to force the client to accept the attacker's reply.

NDP poisoning is only supported if IPv6 support is enabled. ND requests and replies are sent to victims to poison their neighbor cache. Once the cache has been poisoned, the victims send all IPv6 packets to the attacker, who can modify them and forward them to the real destination.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_ETTERCAP_DNS_SPOOF_EH1]

▼ **Question 4:** Correct

Which of the following is the term used to describe what happens when an attacker sends falsified messages to link their MAC address with the IP address of a legitimate computer or server on the network?

○ Port mirroring

○ MAC spoofing

➡ ● ARP poisoning

○ MAC flooding

Explanation

Address Resolution Protocol (ARP) poisoning is when an attacker sends fake ARP messages to link their MAC address with the IP address of a legitimate computer or server on the network. Once their MAC address is linked to an authentic IP address, the attacker can receive any messages directed to the legitimate address. As a result, the attacker can intercept, modify, or block communications to the legitimate MAC address.

Port mirroring creates a duplicate of all network traffic on a port and sends it to another device.

MAC flooding is when an attacker intentionally floods a content addressable memory table with Ethernet frames, each originating from different MAC addresses. Once the table starts to overflow, the switch responds by broadcasting all incoming data to all ports, basically turning itself into a hub instead of a switch.

MAC spoofing is done to enable bypassing of access control lists on servers or routers by either hiding a computer on a network or by allowing it to impersonate another network device.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_SWITCH_NETWORK_SNIFF_01_EH1]

▼ **Question 5:** Correct

A security analyst is using tcpdump to capture suspicious traffic detected on port 443 of a server. The analyst wants to capture the entire packet with hexadecimal and ascii output only. Which of the following tcpdump options will achieve this output?

○ **src port 443**

○ **-SXX port 443**

➡ ● **-SX port 443**

○ **-SA port 443**

Explanation

-SX is the command line options for both full packet capture and hexadecimal and ascii output of port

443.

The tcpdump src port will capture source port traffic on 443, but will not capture the entire packet or output the hexadecimal and ascii codes.

-SA will capture full packets, but only ascii output is included.

-SXX performs the same function as -SX and also gives the Ethernet header.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_TCPDUMP_01_EH1]

Question 6: Incorrect

Using Wireshark filtering, you want to see all traffic except IP address 192.168.142.3. Which of the following is the best command to filter a specific source IP address?

● **~~ip.src && 192.168.142.3~~**

○ **ip.src eq 192.168.142.3**

➡ ○ **ip.src ne 192.168.142.3**

○ **ip.src == 192.168.142.3**

Explanation

The ne filter stands for not equal. This command will display all traffic not equal to 192.168.142.3.

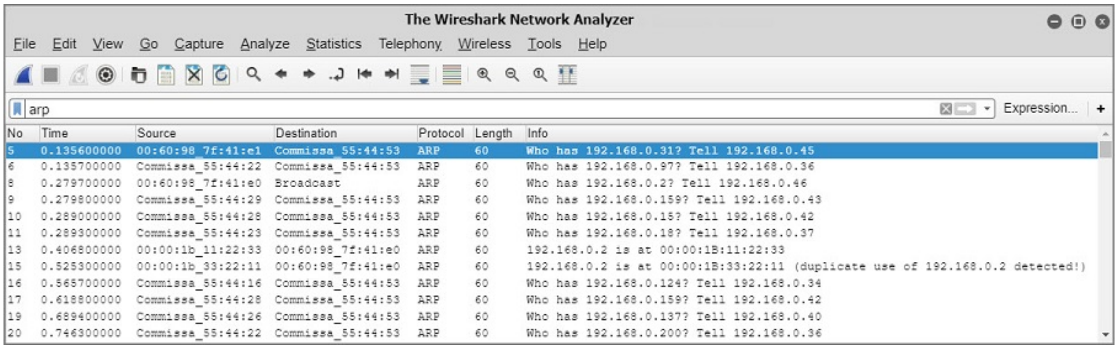
==stands for equal to, && stands for and, and eq is another way to write equal to.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_WIRESHARK_01_EH1]

Question 7: Incorrect

As the cybersecurity specialist for your company, you believe a hacker is using ARP poisoning to infiltrate your network. To test your hypothesis, you have used Wireshark to capture packets and then filtered the results. After examining the results, which of the following is your best assessment regarding ARP poisoning?


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

arp

No	Time	Source	Destination	Protocol	Length	Info
5	0.135600000	00:60:98_7f:41:e1	Commissa_55:44:53	ARP	60	Who has 192.168.0.31? Tell 192.168.0.45
6	0.135700000	Commissa_55:44:22	Commissa_55:44:53	ARP	60	Who has 192.168.0.97? Tell 192.168.0.36
8	0.279700000	00:60:98_7f:41:e0	Broadcast	ARP	60	Who has 192.168.0.2? Tell 192.168.0.46
9	0.279800000	Commissa_55:44:29	Commissa_55:44:53	ARP	60	Who has 192.168.0.159? Tell 192.168.0.43
10	0.289000000	Commissa_55:44:28	Commissa_55:44:53	ARP	60	Who has 192.168.0.15? Tell 192.168.0.42
11	0.289300000	Commissa_55:44:23	Commissa_55:44:53	ARP	60	Who has 192.168.0.18? Tell 192.168.0.37
13	0.406800000	00:00:1b_11:22:33	00:60:98_7f:41:e0	ARP	60	192.168.0.2 is at 00:00:1B:11:22:33
15	0.525300000	00:00:1b_33:22:11	00:60:98_7f:41:e0	ARP	60	192.168.0.2 is at 00:00:1B:33:22:11 (duplicate use of 192.168.0.2 detected!)
16	0.565700000	Commissa_55:44:16	Commissa_55:44:53	ARP	60	Who has 192.168.0.124? Tell 192.168.0.34
17	0.618800000	Commissa_55:44:28	Commissa_55:44:53	ARP	60	Who has 192.168.0.159? Tell 192.168.0.42
19	0.689400000	Commissa_55:44:26	Commissa_55:44:53	ARP	60	Who has 192.168.0.137? Tell 192.168.0.40
20	0.746300000	Commissa_55:44:22	Commissa_55:44:53	ARP	60	Who has 192.168.0.200? Tell 192.168.0.36

➡ ○ ARP poisoning is occurring, as indicated by the duplicate response IP address.

○ ARP poisoning is occurring, as indicated by the multiple Who Has packets being sent.

● ~~No ARP poisoning is occurring.~~

○ ARP poisoning is occurring, as indicated by the short time interval between ARP packets.

Explanation

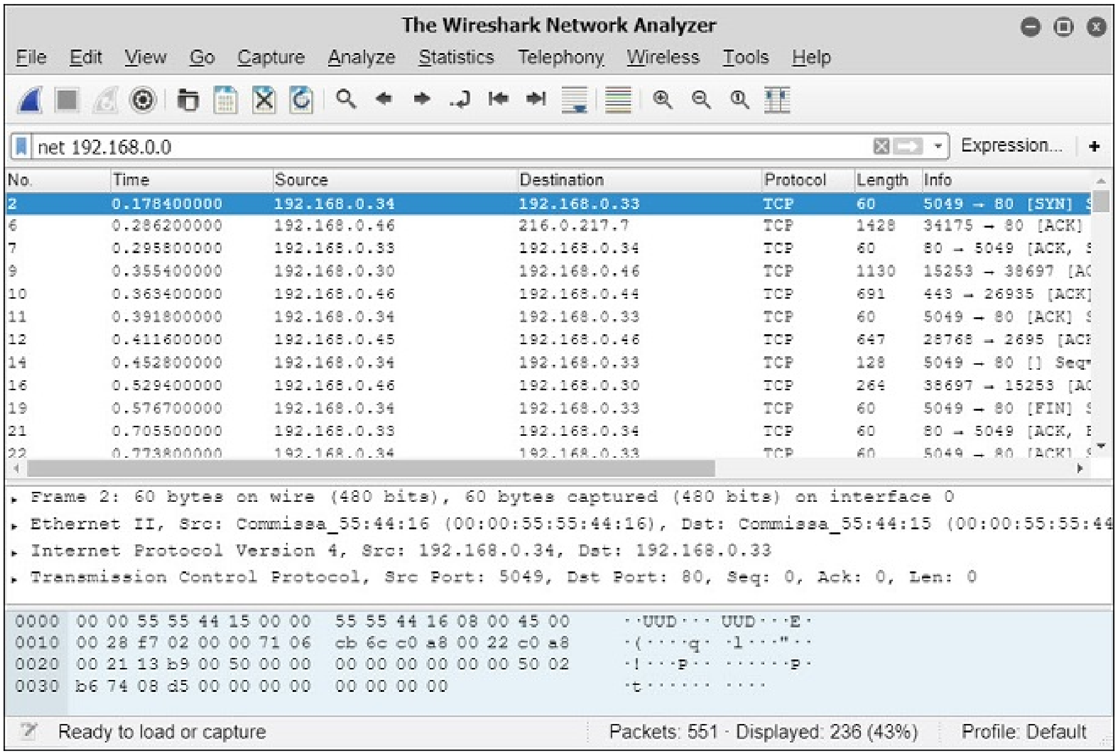
When using Wireshark to detect ARP poisoning, Wireshark displays a duplicate use of IPs detected. Even without this message, seeing two packets with the same IP address is a good indication that ARP poisoning is taking place on your network.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_WIRESHARK_ARP_POISON_01_EH1]

Question 8: Incorrect

Using Wireshark, you have used a filter to help capture only the desired types of packets. Using the information shown in the image, which of the following best describes the effects of using the net 192.168.0.0 filter?


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

net 192.168.0.0

No.	Time	Source	Destination	Protocol	Length	Info
2	0.178400000	192.168.0.34	192.168.0.33	TCP	60	5049 → 80 [SYN] S
6	0.286200000	192.168.0.46	216.0.217.7	TCP	1428	34175 → 80 [ACK]
7	0.295800000	192.168.0.33	192.168.0.34	TCP	60	80 → 5049 [ACK, S
9	0.355400000	192.168.0.30	192.168.0.46	TCP	1130	15253 → 38697 [AC
10	0.363400000	192.168.0.46	192.168.0.44	TCP	691	443 → 26935 [ACK]
11	0.391800000	192.168.0.34	192.168.0.33	TCP	60	5049 → 80 [ACK] S
12	0.411600000	192.168.0.45	192.168.0.46	TCP	647	28768 → 2695 [ACK
14	0.452800000	192.168.0.34	192.168.0.33	TCP	128	5049 → 80 [] Seq
16	0.529400000	192.168.0.46	192.168.0.30	TCP	264	38697 → 15253 [AC
19	0.576700000	192.168.0.34	192.168.0.33	TCP	60	5049 → 80 [FIN] S
21	0.705500000	192.168.0.33	192.168.0.34	TCP	60	80 → 5049 [ACK, F
22	0.773800000	192.168.0.34	192.168.0.33	TCP	60	5049 → 80 [ACK] S

```
▸ Frame 2: 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
▸ 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 f7 02 00 00 71 06   cb 6c c0 a8 00 22 c0 a8    ·(····q· ·l···"··
0020  00 21 13 b9 00 50 00 00   00 00 00 00 00 00 50 02    ·!···P·· ······P·
0030  b6 74 08 d5 00 00 00 00   00 00 00 00                ·t······ ····
```

Ready to load or capture   Packets: 551 · Displayed: 236 (43%)   Profile: Default

● ~~Only packets with a destination address on the 192.168.0.0 network are captured.~~

○ Only packets with a source address on the 192.168.0.0 network are captured.

○ Only packets with a source address of 192.168.0.0 are captured.

➡ ○ Only packets with either a source or destination address on the 192.168.0.0 network are captured.

Explanation

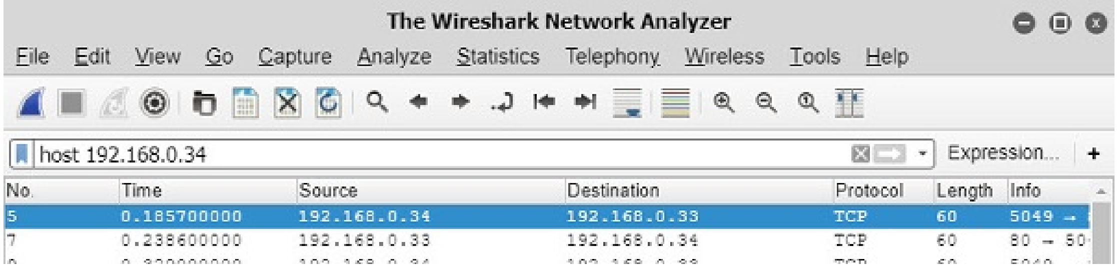
The net filter captures traffic to or from a range of IP addresses. Since the network address of 192.168.0.0 was used, only packets with either a source or destination address on the 192.168.0.0 network are displayed.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_WIRESHARK_FILTERS_01_EH1]

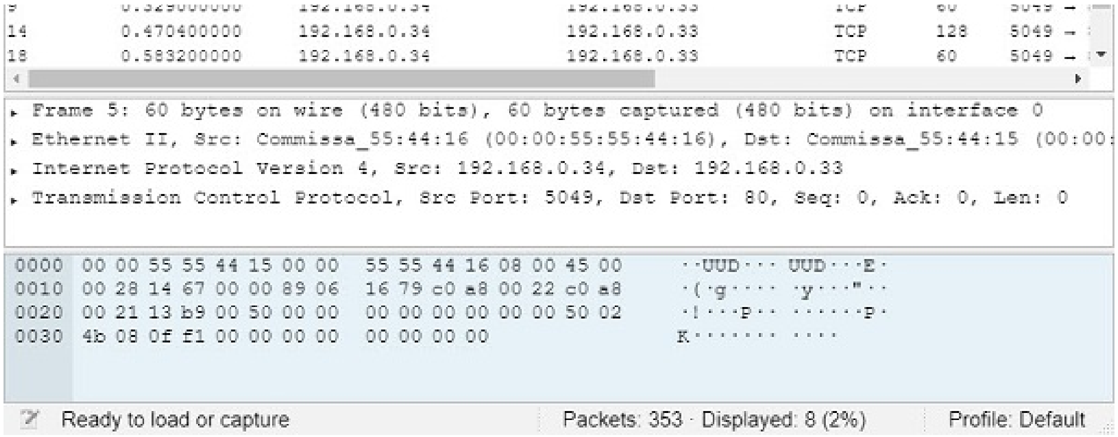
Question 9: Incorrect

Using Wireshark, you have used a filter to help capture only the desired types of packets. Using the information shown in the image, which of the following best describes the effects of using the host 192.168.0.34 filter?


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

host 192.168.0.34

No.	Time	Source	Destination	Protocol	Length	Info
5	0.185700000	192.168.0.34	192.168.0.33	TCP	60	5049 →
7	0.238600000	192.168.0.33	192.168.0.34	TCP	60	80 → 50



```
9       0.329000000   192.168.0.34    192.168.0.33    TCP   60    5049 →
14      0.470400000   192.168.0.34    192.168.0.33    TCP   128   5049 →
18      0.583200000   192.168.0.34    192.168.0.33    TCP   60    5049 →
```

```
▸ Frame 5: 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:
▸ 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 14 67 00 00 89 06  16 79 c0 a8 00 22 c0 a8   ·(·g···· ·y···"··
0020  00 21 13 b9 00 50 00 00  00 00 00 00 00 00 50 02   ·!···P·· ······P·
0030  4b 08 0f f1 00 00 00 00  00 00 00 00              K······· ····
```

Ready to load or capture | Packets: 353 · Displayed: 8 (2%) | Profile: Default

○ Only packets with 192.168.0.34 in either the source or destination address are captured.

○ Only packets with 192.168.0.34 in the source address are captured.

● ~~Only packets with 192.168.0.34 in the destination address are captured.~~

○ Only packets on the 192.168.0.34 network are captured.

Explanation

Wireshark's host filter lets you only capture where the specified IP address is in either the source or the destination address.

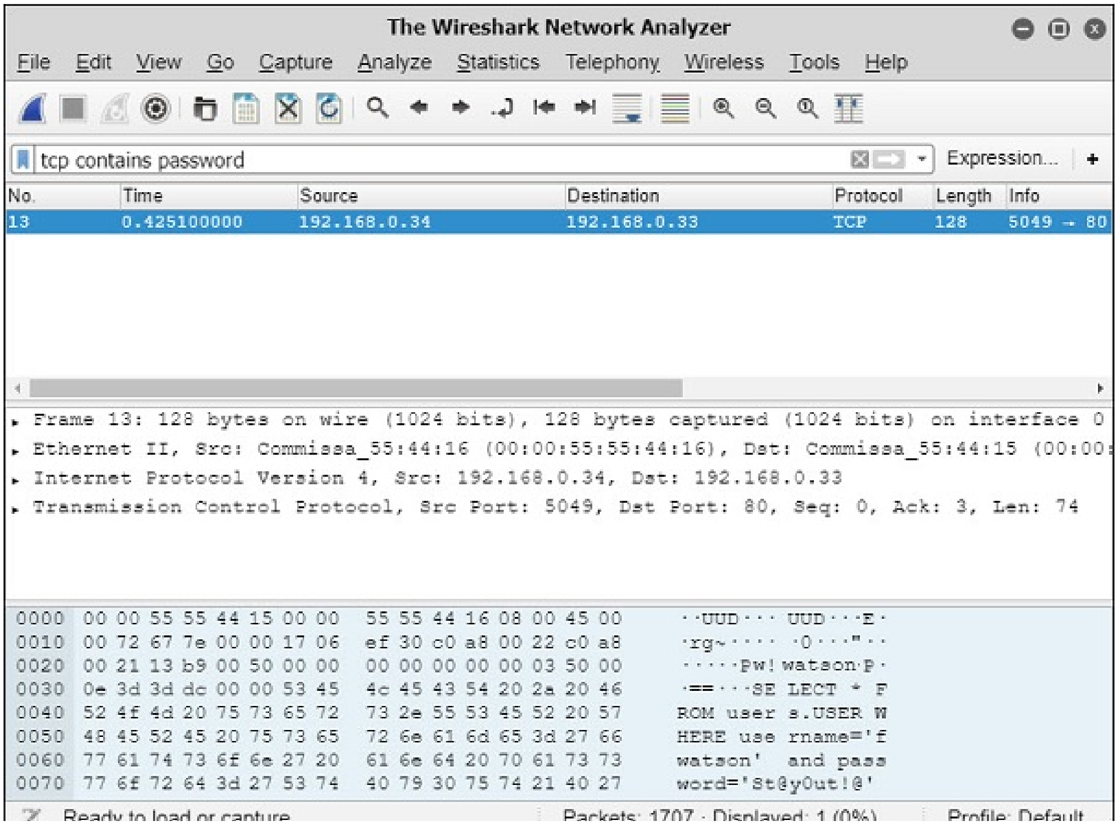
The IP address of 192.168.0.34 is a specific address for an individual device. It is not an address for the entire network.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_WIRESHARK_FILTERS_02_EH1]

Question 10: Correct

You have just captured the following packet using Wireshark and the filter shown. Which of the following is the captured password?



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

tcp contains password

No.	Time	Source	Destination	Protocol	Length	Info
13	0.425100000	192.168.0.34	192.168.0.33	TCP	128	5049 → 80

```
▸ Frame 13: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0
▸ Ethernet II, Src: Commissa_55:44:16 (00:00:55:55:44:16), Dst: Commissa_55:44:15 (00:00:
▸ 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: 3, Len: 74
```

```
0000  00 00 55 55 44 15 00 00  55 55 44 16 08 00 45 00   ··UUD··· UUD···E·
0010  00 72 67 7e 00 00 17 06  ef 30 c0 a8 00 22 c0 a8   ·rg~···· ·0···"··
0020  00 21 13 b9 00 50 00 00  00 00 00 00 00 03 50 00   ·····Pw! watson·P·
0030  0e 3d 3d dc 00 00 53 45  4c 45 43 54 20 2a 20 46   ·==···SE LECT * F
0040  52 4f 4d 20 75 73 65 72  73 2e 55 53 45 52 20 57   ROM user s.USER W
0050  48 45 52 45 20 75 73 65  72 6e 61 6d 65 3d 27 66   HERE use rname='f
0060  77 61 74 73 6f 6e 27 20  61 6e 64 20 70 61 73 73   watson'  and pass
0070  77 6f 72 64 3d 27 53 74  40 79 30 75 74 21 40 27   word='St@y0ut!@'
```

Ready to load or capture | Packets: 1707 · Displayed: 1 (0%) | Profile: Default

○ watson

○ p@ssw0rd

➡ ● St@y0ut!@

○ watson-p

Explanation

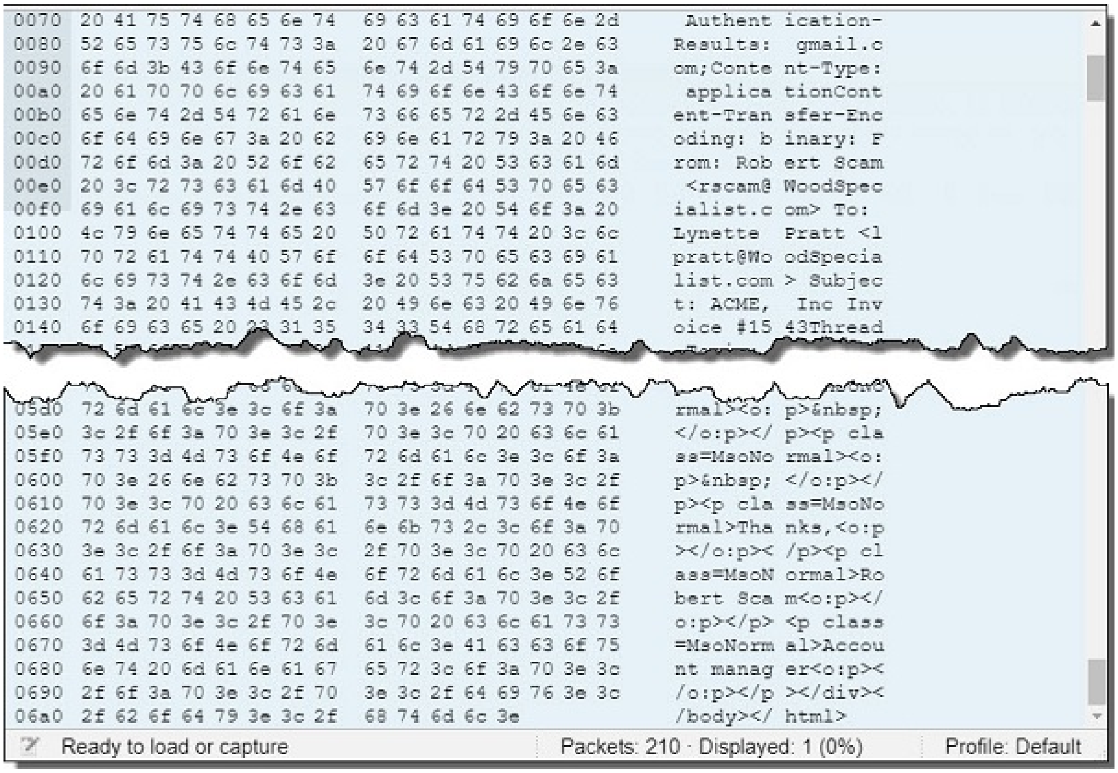
The password is found in the lower pane, following the words *password=*, and is *St@y0ut@*.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_WIRESHARK_FILTERS_03_EH1]

Question 11: Incorrect

You have been asked to perform a penetration test for a company to see if any sensitive information can be captured by a potential hacker. You have used Wireshark to capture a series of packets. Using the tcp contains Invoice filter, you have found one packet. Using the captured information shown, which of the following is the account manager's email address?



```
0070  20 41 75 74 68 65 6e 74  69 63 61 74 69 6f 6e 2d    Authent ication-
0080  52 65 73 75 6c 74 73 3a  20 67 6d 61 69 6c 2e 63   Results:  gmail.c
0090  6f 6d 3b 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   om;Conte nt-Type:
00a0  20 61 70 70 6c 69 63 61  74 69 6f 6e 43 6f 6e 74    applica tionCont
00b0  65 6e 74 2d 54 72 61 6e  73 66 65 72 2d 45 6e 63   ent-Tran sfer-Enc
00c0  6f 64 69 6e 67 3a 20 62  69 6e 61 72 79 3a 20 46   oding: b inary: F
00d0  72 6f 6d 3a 20 52 6f 62  65 72 74 20 53 63 61 6d   rom: Rob ert Scam
00e0  20 3c 72 73 63 61 6d 40  57 6f 6f 64 53 70 65 63    <rscam@ WoodSpec
00f0  69 61 6c 69 73 74 2e 63  6f 6d 3e 20 54 6f 3a 20   ialist.c om> To:
0100  4c 79 6e 65 74 74 65 20  50 72 61 74 74 20 3c 6c   Lynette  Pratt <l
0110  70 72 61 74 74 40 57 6f  6f 64 53 70 65 63 69 61   pratt@Wo odSpecia
0120  6c 69 73 74 2e 63 6f 6d  3e 20 53 75 62 6a 65 63   list.com > Subjec
0130  74 3a 20 41 43 4d 45 2c  20 49 6e 63 20 49 6e 76   t: ACME,  Inc Inv
0140  6f 69 63 65 20 23 31 35  34 33 54 68 72 65 61 64   oice #15 43Thread

05d0  72 6d 61 6c 3e 3c 6f 3a  70 3e 26 6e 62 73 70 3b   rmal><o: p>&nbsp;
05e0  3c 2f 6f 3a 70 3e 3c 2f  70 3e 3c 70 20 63 6c 61   </o:p></ p><p cla
05f0  73 73 3d 4d 73 6f 4e 6f  72 6d 61 6c 3e 3c 6f 3a   ss=MsoNo rmal><o:
0600  70 3e 26 6e 62 73 70 3b  3c 2f 6f 3a 70 3e 3c 2f   p>&nbsp; </o:p></
0610  70 3e 3c 70 20 63 6c 61  73 73 3d 4d 73 6f 4e 6f   p><p cla ss=MsoNo
0620  72 6d 61 6c 3e 54 68 61  6e 6b 73 2c 3c 6f 3a 70   rmal>Tha nks,<o:p
0630  3e 3c 2f 6f 3a 70 3e 3c  2f 70 3e 3c 70 20 63 6c   ></o:p>< /p><p cl
0640  61 73 73 3d 4d 73 6f 4e  6f 72 6d 61 6c 3e 52 6f   ass=MsoN ormal>Ro
0650  62 65 72 74 20 53 63 61  6d 3c 6f 3a 70 3e 3c 2f   bert Sca m<o:p></
0660  6f 3a 70 3e 3c 2f 70 3e  3c 70 20 63 6c 61 73 73   o:p></p> <p class
0670  3d 4d 73 6f 4e 6f 72 6d  61 6c 3e 41 63 63 6f 75   =MsoNorm al>Accou
0680  6e 74 20 6d 61 6e 61 67  65 72 3c 6f 3a 70 3e 3c   nt manag er<o:p><
0690  2f 6f 3a 70 3e 3c 2f 70  3e 3c 2f 64 69 76 3e 3c   /o:p></p ></div><
06a0  2f 62 6f 64 79 3e 3c 2f  68 74 6d 6c 3e            /body></ html>
```

Ready to load or capture | Packets: 210 · Displayed: 1 (0%) | Profile: Default

○ fstone@rocks.com

● ~~lpratt@lowes.com~~

➡ ○ rscam@woodspecialist.com

○ rsmith@thehomedepot.com

Explanation

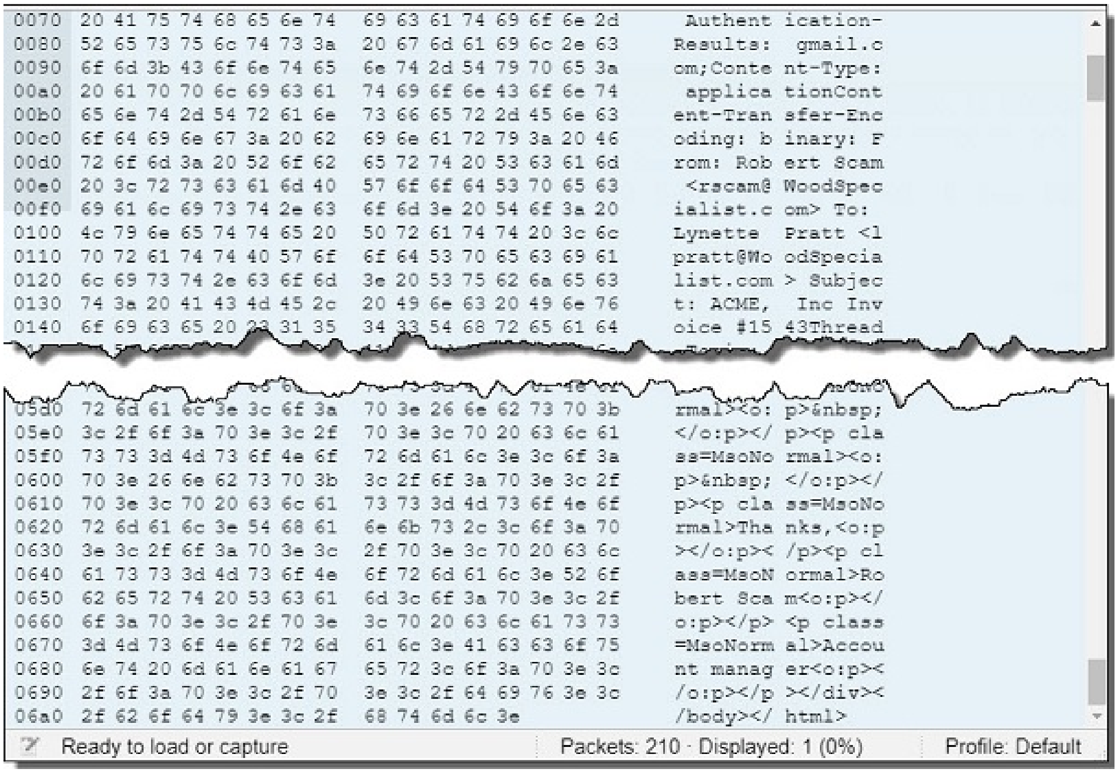
By looking at the beginning of the packet, you see that the email was sent from a person named Robert Scam, who has an email address of rscam@woodspecialist.com. Later in the packet, you see that the email was signed, "Thanks, Robert Scam - Account manager." Therefore, you know that the email address for the account manager is rscam@woodspecialist.com.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_WIRESHARK_SENSITIVE_DATA_01_EH1]

Question 12: Incorrect

You have been asked to perform a penetration test for a company to see if any sensitive information can be captured by a potential hacker. You have used Wireshark to capture a series of packets. Using the tcp contains Invoice filter, you have found one packet. Using the captured information shown, which of the following is the name of the company requesting payment?



```
0070  20 41 75 74 68 65 6e 74  69 63 61 74 69 6f 6e 2d    Authent ication-
0080  52 65 73 75 6c 74 73 3a  20 67 6d 61 69 6c 2e 63   Results:  gmail.c
0090  6f 6d 3b 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   om;Conte nt-Type:
00a0  20 61 70 70 6c 69 63 61  74 69 6f 6e 43 6f 6e 74    applica tionCont
00b0  65 6e 74 2d 54 72 61 6e  73 66 65 72 2d 45 6e 63   ent-Tran sfer-Enc
00c0  6f 64 69 6e 67 3a 20 62  69 6e 61 72 79 3a 20 46   oding: b inary: F
00d0  72 6f 6d 3a 20 52 6f 62  65 72 74 20 53 63 61 6d   rom: Rob ert Scam
00e0  20 3c 72 73 63 61 6d 40  57 6f 6f 64 53 70 65 63    <rscam@ WoodSpec
00f0  69 61 6c 69 73 74 2e 63  6f 6d 3e 20 54 6f 3a 20   ialist.c om> To:
0100  4c 79 6e 65 74 74 65 20  50 72 61 74 74 20 3c 6c   Lynette  Pratt <l
0110  70 72 61 74 74 40 57 6f  6f 64 53 70 65 63 69 61   pratt@Wo odSpecia
0120  6c 69 73 74 2e 63 6f 6d  3e 20 53 75 62 6a 65 63   list.com > Subjec
0130  74 3a 20 41 43 4d 45 2c  20 49 6e 63 20 49 6e 76   t: ACME,  Inc Inv
0140  6f 69 63 65 20 23 31 35  34 33 54 68 72 65 61 64   oice #15 43Thread

05d0  72 6d 61 6c 3e 3c 6f 3a  70 3e 26 6e 62 73 70 3b   rmal><o: p>&nbsp;
05e0  3c 2f 6f 3a 70 3e 3c 2f  70 3e 3c 70 20 63 6c 61   </o:p></ p><p cla
05f0  73 73 3d 4d 73 6f 4e 6f  72 6d 61 6c 3e 3c 6f 3a   ss=MsoNo rmal><o:
0600  70 3e 26 6e 62 73 70 3b  3c 2f 6f 3a 70 3e 3c 2f   p>&nbsp; </o:p></
0610  70 3e 3c 70 20 63 6c 61  73 73 3d 4d 73 6f 4e 6f   p><p cla ss=MsoNo
0620  72 6d 61 6c 3e 54 68 61  6e 6b 73 2c 3c 6f 3a 70   rmal>Tha nks,<o:p
0630  3e 3c 2f 6f 3a 70 3e 3c  2f 70 3e 3c 70 20 63 6c   ></o:p>< /p><p cl
0640  61 73 73 3d 4d 73 6f 4e  6f 72 6d 61 6c 3e 52 6f   ass=MsoN ormal>Ro
0650  62 65 72 74 20 53 63 61  6d 3c 6f 3a 70 3e 3c 2f   bert Sca m<o:p></
0660  6f 3a 70 3e 3c 2f 70 3e  3c 70 20 63 6c 61 73 73   o:p></p> <p class
0670  3d 4d 73 6f 4e 6f 72 6d  61 6c 3e 41 63 63 6f 75   =MsoNorm al>Accou
0680  6e 74 20 6d 61 6e 61 67  65 72 3c 6f 3a 70 3e 3c   nt manag er<o:p><
0690  2f 6f 3a 70 3e 3c 2f 70  3e 3c 2f 64 69 76 3e 3c   /o:p></p ></div><
06a0  2f 62 6f 64 79 3e 3c 2f  68 74 6d 6c 3e             /body></ html>
```

➡ ○ ACME, Inc

○ Lowes

● ~~The Home Depot~~

○ Wood Specialist

Explanation

By looking at the beginning of the packet, you see that Robert Scam is sending an email with a subject line of *ACME, Inc Invoice #1543*. Therefore, you now know that the name of the company requesting payment is ACME, Inc.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFER_WIRESHARK_SENSITIVE_DATA_02_EH1]

Question 13: Incorrect

Using sniffers has become one way for an attacker to view and gather network traffic. If an attacker overcomes your defenses and obtains network traffic, which of the following is the best countermeasure for securing the captured network traffic?

○ Eliminate unnecessary system applications.

○ Use intrusion detection countermeasures.

➡ ○ Use encryption for all sensitive traffic.

● ~~Implement acceptable use policies.~~

Explanation

Using encryption methods is the best practice to secure network traffic in this scenario. It becomes one of the last lines of defense. If the encryption method used is strong enough, it will take the attacker too long to decrypt the obtained encrypted traffic to be worth the effort.

An IDS is used to detect intrusion and to alert network administrators of attacks. These systems can search for anomalies in network traffic. They send an alert when an intrusion is detected and are not used as a countermeasure to secure network traffic that has already been obtained by an attacker.

Implementing policies and promoting network security awareness training are good countermeasures, but they will not protect the data that has been obtained by an attacker.

Closing unnecessary ports associated with known attacks and only allowing necessary applications to run lessens the attack arena and are good network attack countermeasures. These countermeasures do not secure network traffic already obtained.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFING_COUNTER_NETWORK_TRAFFIC_01_EH1]

▼ **Question 14:** Incorrect

Your network administrator is configuring settings so the switch shuts down a port when the max number of MAC addresses is reached. What is the network administrator taking countermeasures against?

○ Filtering

○ Hijacking

● ~~Spoofing~~

➡ ○ Sniffing

Explanation

Switched networks provide a natural barrier for an attacker using a sniffer. Be sure to configure settings so the switch shuts down a port when the max number of MAC addresses is reached, so MAC flooding isn't possible.

Session hijacking is the process of taking over an established connection between a host and a user.

DNS spoofing, also known as DNS cache poisoning, targets Active Directory or other DNS-reliant networks.

Packet filtering firewalls look at a packet's header information to determine legitimate traffic.

References

TestOut Ethical Hacker Pro - 10.1 Sniffing
[e_sniffing_eh1.exam.xml Q_SNIFFING_COUNTER_SWITCH_NETWORK_01_EH1]