The following questions are directly from the SEC502: Perimeter Protection In-Depth course material. If you are wondering if this course would help to enhance your skill set, taking this test is a great way to find out:

1) How many different techniques are available to sniff in a switched environment?

A) None. Switches block unicast traffic to all ports.
B) 2
C) 4
D) 6

2) You receive the ICMP packet shown below from a remote host. Which of the following is the most likely source of the packet?

15:52:50.129178 IP (tos 0x0, ttl 47, id 51389, offset 0, flags [none], proto: ICMP (1), length: 28)
1.2.3.4 > 172.30.2.10: ICMP echo request, id 18492, seq 21446

A) Ping run on a Windows system.
B) Ping run on a Linux system.
C) hping using the “-C 8” option.
D) nmap using the “-sP” option.

3) Which is the best way to discourage attackers from using your address space as part of a SYN flood attack?

A) Quietly drop all inbound SYN/ACK packets that are unsolicited.
B) Return an ICMP Admin Prohibited error packet for all inbound SYN/ACK traffic that is unsolicited.
C) Advertise all portions (even unused) of your IP address space via BGP.
D) Report all suspicious inbound traffic to the listed administrative contact of the source IP.

4) Which firewall product is susceptible to loose source route attacks?

A) Check Point
B) Cisco
C) Netscreen
D) None of the above

5) Which Libpcap filter would permit you to see potentially malicious IP fragments which could not have been generated by a normal topology MTU?

A) ip = frag and evil bit = enable
B) ip[12:2] = ip[16:2]
C) ip[2:2]<0x1F4 and ip[6]&32!=0
D) ip[8]<0x2A or ip[0]&0x0F>5

6) Which of the following techniques would permit an attacker to port scan your network without giving any indication of their true source IP address?

A) nmap “stealth” (-sS) scan.
B) nmap “idle” (-sI) scan.
C) nmap “decoy” (-D) scan.
D) Port scans require responses to stimulus so the true source IP cannot be completely hidden.

7) Which of the following best describes what happens when you surf to a Web site, see “HTTPS” in the URL, and the little lock icon on your Web browser is activated?

A) All data to and from the Web server is at least authenticated.
B) All data to and from the Web server is at least encrypted.
C) All data to and from the Web server is encrypted and the digital certificate is fully verified.
D) All data to and from the Web server is authenticated and encrypted.

8) You see the following packet leaving your Web server and headed to an IP address on the Internet. What is the most likely cause?

17:08:08.412172 IP (tos 0x0, ttl 128, id 18210, offset 0, flags [DF], proto: UDP (17), length: 33) 172.30.2.185.32851 > 1.2.3.4.69:

A) Problem with the firewall state table time-out being set too low.
B) Automatic update checking for new patches.
C) Attacker retrieving a toolkit.
D) A secure HTTPS session.

9) You see the following packet entering your network. Which answer gives the most accurate and likely possibility of what is going on?

19:22:17.631407 IP (tos 0x0, ttl 112, id 30435, offset 0, flags [DF], proto: TCP (6), length: 48) 1.2.3.4.4110 > 192.168.1.10.25: S, cksum 0xc25c (correct), 103504428:103504428(0) win 8192 <mss 1460,nop,nop,sackOK>

A) TCP transmission from a Windows system.
B) SMTP transmission from a Windows system.
C) Spam or Phishing attempt from a Windows system.
D) SMTP transmission from a Linux or UNIX system.

10) Given the following netstat output, which of the answers best describes the situation:

```
Proto  Local Address          Foreign Address        State           PID
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       2648
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       2292
```

```
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1204
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
```

A) The system has potentially been compromised.
B) The system needs a restart to install updated software.
C) The system is configured as a typical Windows desktop.
D) The system is configured as a typical Windows server.

11) Which of the following systems can potentially be taken over by a remote attacker?
A) A Web server exposed to Internet access.
B) A desktop with Internet access.
C) A firewall or Network Based Intrusion Prevention (NIPS) system.
D) All of the above.
E) None of the above.

12) A Network Based Intrusion Prevention System (NIPS) is simply a relabeled:
A) Proxy based firewall.
B) Stateful inspection based firewall.
C) Neither, it is its own unique technology.
D) A combination of both.

13) You see the following pattern in your firewall log. Which answer best describes what may be going on?

```
Jun  8 05:40:36 SRC= 1.2.3.4 DST=our_web_server LEN=40 TTL=2 ID=7831 PROTO=TCP
SPT=2023 DPT=80 WINDOW=1400 SYN
Jun  8 05:40:38 SRC= 1.2.3.4 DST=our_web_server LEN=40 TTL=44 ID=7832 PROTO=TCP
SPT=80 DPT=80 WINDOW=1400 SYN
Jun  8 05:40:40 SRC= 1.2.3.4 DST=our_web_server LEN=40 TTL=44 ID=7833 PROTO=TCP
SPT=2024 DPT=80 WINDOW=1400 ACK
Jun  8 05:40:45 SRC= 1.2.3.4 DST=our_dns_server LEN=38 TTL=44 ID=7834 PROTO=ICMP
TYPE=8 CODE=0 ID=47578 SEQ=5
Jun  8 05:40:50 SRC= 1.2.3.4 DST=our_dns_server LEN=58 TTL=44 ID=7835 PROTO=UDP
SPT=2025 DPT=53
Jun  8 05:40:52 SRC= 1.2.3.4 DST=our_dns_server LEN=58 TTL=44 ID=7836 PROTO=UDP
SPT=80 DPT=53
Jun  8 05:40:54 SRC= 1.2.3.4 DST=our_dns_server LEN=58 TTL=44 ID=7837 PROTO=TCP
SPT=2026 DPT=53 WINDOW=1400 SYN
Jun  8 05:40:59 SRC= 1.2.3.4 DST=our_dns_server LEN=58 TTL=44 ID=7838 PROTO=TCP
SPT=2026 DPT=53 WINDOW=1400 RST
```

A) Someone is fingerprinting which firewall product you are using.
B) A remote site is having connectivity issues connecting to our Web server.
C) The state table time-out value on our firewall is set too low.
D) This is normal and expected traffic to our servers.

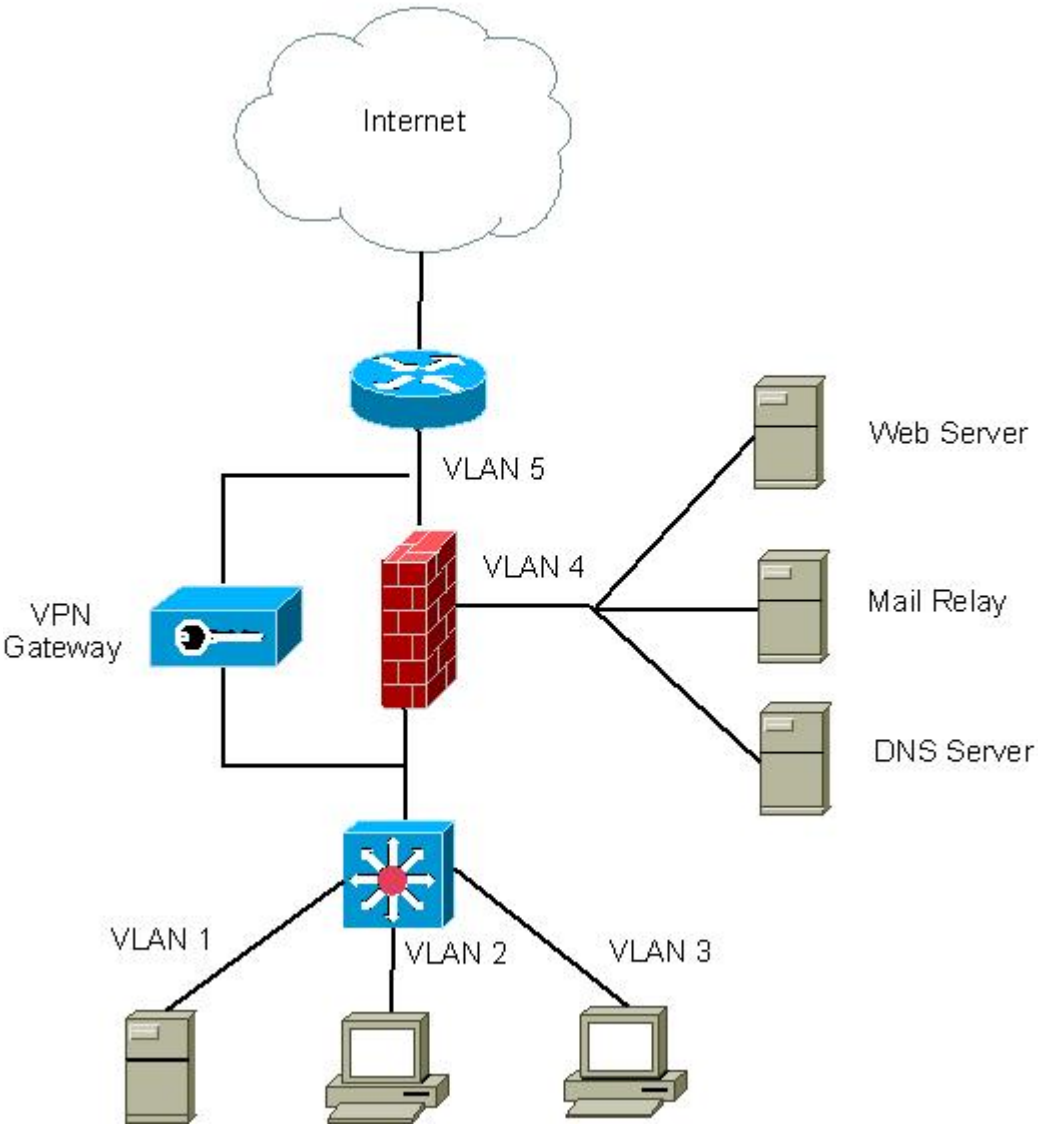
14) You see the following traffic pattern in your proxy log. What is the most likely cause?

```
192.168.1.22 [ 9/Jul/2009:10:42:55 +0000] "GET http:// 1.2.3.4/ HTTP/1.1" "-" "-"
192.168.1.22 [ 9/Jul/2009:10:42:55 +0000] "POST http:// 1.2.3.4/ HTTP/1.1" "-" "-"
192.168.1.22 [ 9/Jul/2009:10:43:20 +0000] "GET http:// 1.2.3.4/ HTTP/1.1" "-" "-"
```

```
192.168.1.22 [ 9/Jul/2009:10:43:20 +0000] "POST http:// 1.2.3.4/ HTTP/1.1" "-" "-"
192.168.1.22 [ 9/Jul/2009:10:43:45 +0000] "GET http:// 1.2.3.4/ HTTP/1.1" "-" "-"
192.168.1.22 [ 9/Jul/2009:10:43:45 +0000] "POST http:// 1.2.3.4/ HTTP/1.1" "-" "-"
```

A) 192.168.1.22 is performing normal Web browsing.
B) 192.168.1.22 is downloading patches.
C) Someone on 192.168.1.22 is running an nmap version scan against 1.2.3.4.
D) 192.168.1.22 has been compromised and is calling home.

15) Analyze the following network drawing. How many potential paths does an attacker have available in order to gain access to the internal network?



A) 1
B) 2
C) 3

D) 4

Don’t look below this point until you have answered all of the questions above.

Answers:
1) D
There are six different techniques that can be used to sniff in a switched environment. ARP cache poisoning, ARP cache flooding, DHCP spoofing, Port stealing, ICMP redirect attack and ICMP route discovery attack. High end vendor switches can be configured to block all of these except the ICMP redirect attack. That must be addressed on a per host level.

2) D
Ping on both Windows and Linux encapsulate data in the payload of their Echo-Request packets. The above packet has a length of 28, which is just an IP and ICMP header. When hping generates Echo-Request packets, it uses an initial sequence number of 0 and then increments by +256. The above sequence number of 21446 is not evenly divisible by 256. This makes nmap the most likely candidate as it generates empty payload Echo-Requests with random sequence numbers.

3) B
When your address space is spoofed as part of a SYN flood attack, you will see a high number of unsolicited SYN/ACK packets being sent to your network. Quietly dropping this traffic makes your address space highly attractive to attackers spoofing packets because it maximizes the amount of time their attacking SYN packets fill up the remote connection queue. By returning an ICMP error for these packets, your IP address space becomes less desirable as you are quickly removing the attacking SYN packets from the remote connection queue.

4) C
All three products prevent source route packets (both loose and strict) from being bounced off of the firewall itself. Netscreen however will pass loose source route packets targeting a host on the other side. So to be safe from redirection attacks in a Netscreen environment, you must ensure source routing is disabled on all exposed hosts.

5) C
The first portion of the filter, “ip[2:2]<0x1F4” checks to see if the packet is less than 500 bytes in size. The second portion of the filter, “ip[6]&32!=0” checks to see if the more fragment flag is turned on. So the complete filter will catch non-last fragments smaller than 500 bytes. All non-last fragments will express the smallest topology Maximum Transmission Unit (MTU) they pass through. The smallest LAN or WAN MTU used in the Internet is 512 bytes. So fragments smaller than 500 bytes are being crafted, most likely to obfuscate an attack pattern and avoid detection.

6) B
An idle scan leverages the predictable IP ID's being used by a secondary system in order to make it appear that all the scanning packets are originating from that host. Since all the scan packets use the spoofed IP address of this secondary host, the attacker's true IP address is not revealed to the host being targeted. nmap's stealth and decoy options still transmit packets using the attacker's true source IP

address.

7) A
The protocol HTTPS and the little lock icon being activated on a Web browser simply means that the SSL or TLS protocol is being used to secure the data stream. Both specifications require that every packet be authenticated. Both specifications make encryption an optional feature. So its possible to use either SSL or TLS to communicate without encrypting any of the data passing between the systems. The only way to prevent this is to disable these options in your browser. Further, digital certificates are typically checked against a locally stored public key, but the browser does not check to see if the certificate has been revoked. This can also be changed through the browser's options.

8) C
The traffic in question is an outbound attempt to connect to a TFTP server. Since Web servers do not use TFTP, this is not a problem with the firewall state table. Also, vendors do not make fixes available via TFTP, so this is not a check for new patches. The most likely candidate is that an attacker has compromised the system and is attempting to move their toolkit onto the box.

9) C
The TTL value in this packet is 112. Linux and UNIX use a starting TTL of 64, so this packet most likely did not come from one of these systems. Windows uses 128 as a starting TTL so this could likely be a Windows host located 16 hops away. This is a TCP packet headed to port 25, so it is most likely the start of an SMTP session. The system is using a very small window size (8192 bytes) and does not support the TCP windowing option (this would be listed in the output as "wscale" followed by a numeric value), which indicates that it is an older Windows desktop system. Since most organizations do not rely on old Windows desktops as their SMTP servers, this is most likely a compromised host transmitting spam or phishing attacks. A firewall such as pf or Netfilter would be able to filter these packets by passively identifying the source operating system.

10) A
Within a Linux or UNIX environment, ports can only be opened exclusively. This means that only one application can hold open a TCP or UDP listening port at any given time. While most Windows applications open ports exclusively as well, Windows permits applications to listen with non-exclusive access. The result is that one application will service most inbound sessions but if that port is busied out, connections are then passed to the second application. This can permit an attacker to open a back door on a system that is undetectable during port scans of the system.

11) D
The classic view is that only systems with open listening ports exposed to Internet access are susceptible to attack. The point of risk is in fact permitting unknown entities to interact with code running on the local system. All of the indicated systems permit some level of code interaction with untrusted IPs on the Internet. With this in mind, all can potentially be remotely compromised.

12) B
Network based intrusion prevention systems leverage stateful inspection technology to analyze both header and payload information, same as a stateful inspection based firewall. Sometimes NIPS provides more signatures to look for hostile patterns, but most high-end stateful inspection firewalls provide multiple signatures as well, but typically at a lower cost.

13) A

There are many suspicious patterns in these log entries. To start, the Time To Live (TTL) in the first packet is 2. Given modern OSs use a starting TTL of 64 or higher, and most systems are about 15 hops away from each other on the Internet, we should never see a TTL this low. Most likely this is someone running a TCPTraceroute variant to map our network through the firewall.

Look at the length of the first three TCP packets; its 40 bytes. This means no TCP options have been set. All modern day operating systems support some number of TCP options, so these looks like crafted packets. Also, the TTL of 44 is indicative of a Linux or UNIX variant, but the increment of the IP identification (ID) looks like a Windows system. The Echo Request recorded in log entry four is also suspicious, as a Linux/UNIX variant would use an initial Echo-Request sequence number of 0 or 1, not 5.

So what's going on? Look at the source port in the first two packets. Based on the response (if any) from these probes a smart attacker can tell what technology the firewall is based on (proxy, static filtering or stateful filtering). If you know which firewall products leverage each technology, its now just a matter of further reducing the possibilities.

The second packet would identify if the source port is being restricted, which is done by some firewall products but not others. The third packet would identify if an ACK can create a new state table entry, which again is done by some products but not others. The rest of the pattern is similar. Based on what replies come back from each of these probe packets a smart attacker may be able to identify what vendor firewall product we are running.

14) D
The log entries claim this is normal HTTP 1.1 traffic. The issue is that normal HTTP traffic would include additional fields of information such as the full URI visited (we just see the target IP address 1.2.3.4) and the host identification field (what OS is being used, name and version of the browser, etc.). Both of these pieces of information are missing, which makes the log entries very suspicious. The GET and POST nature of the traffic implies that an exchange of information is taking place. While we would want to confirm via additional investigation work, it is very likely our internal system (192.168.1.22) has been compromised and is calling home for instructions.

15) C
There are three potential paths into the internal network; through the firewall, through the VPN gateway and through the switch. The firewall may be attacked directly or via data replies from a malicious site. The VPN gateway has exposed ports with no trusted system to monitor them, so it is susceptible to direct attack. Finally, the switch is a potential path as it is VLANing across multiple security zones. Features like auto trunk negotiation may be leveraged to gain access to the internal network from the DMZ, thus bypassing the firewall's filtering capability between these two security zones.

So how did you do? If you knew the answers to 13 of the 15 questions, you are in pretty good shape. If not, you may find the 502 class useful for filling in holes in your knowledgebase.