## Tests & Quizzes

# Final Exam Spring 2020

Return to Assessment List

Part 1 of 1 - 95.0/ 100.0 Points

Question 1 of 18

Which of the iPv6 Addresses below are valid? Can be more than one correct answer. 0.0/ 5.0 Points

- ✖ ☐ **A.** 2031::130F::9C0:876A:130B
- ☐ **B.** 2001:0DB8:0:130H:87C:140B
- ☐ **C.** 2001:0DB8:0000:130F:0000:0000:08GC:140B
- ✔ ☐ **D.** 2001:0DB8:130F::140B

**Answer Key:** C, D

**Feedback:** 2031::130F::9C0:876A:130B - not valid as there are two :: which is not allowed 2001:0DB8:0:130H:87C:140B - Only 6 fields without a :: Other two are valid

Question 2 of 18

Which of the following is not a valid default chain type in IP Tables Filter Table? 5.0/ 5.0 Points

- ✔ ○ **A. FORWARD**
- ✔ ○ **B. INPUT**

- ✔ ○ **C. OUTPUT**
- ✔ ○ **D. REJECT**

**Answer Key:** D

Question 3 of 18

5.0/ 5.0 Points

As a network security engineer you need a mechanism to log and monitor application level traffic leaving your corporate network. What would be the BEST choice of a control to perform this function?

- ✔ ○ **A. Proxy**
- ✔ ○ **B. Packet Filtering Firewall**
- ✔ ○ **C. IPS**
- ✔ ○ **D. VPN**

**Answer Key:** A

Question 4 of 18

5.0/ 5.0 Points

On an OS X machine you observe the following output when typing ifconfig:

```
en6: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=b<RXCSUM,TXCSUM,VLAN_HWTAGGING>
ether ec:1a:59:3d:03:f1
inet6 fe80::ee1a:59ff:fe3d:3f1%en6 prefixlen 64 scopeid 0x4
inet6 2001:420:2481:e:ee1a:59ff:fe3d:3f1 prefixlen 64 autoconf
inet6 2001:420:2481:e:258c:a4e0:9bed:339d prefixlen 64 autoconf temporary
inet 10.117.92.24 netmask 0xffffff0 broadcast 10.117.92.31
```

```
media: autoselect (100baseTX <full-duplex>)
status: active
```

The addresses in bold are IN ORDER from top to botom:

- ✔ ○ **A. Link Local Address, Global Unicast Address, Privacy Extension Address**
- ✔ ○ **B. Multicast Address, Global Unicast Address, Privacy Extension Address**
- ✔ ○ **C. Anycast Address, Global Unicast Address, Privacy Extension Address**
- ✔ ○ **D. Link Local Address, Global Unicast Address, Broadcast Address**

**Answer Key:** A

Question 5 of 18

5.0/ 5.0 Points

In layer 2 switching devices there exists a component called Content Addressable Memory (CAM). How could it be abused to allow for unlimited sniffing of traffic on a layer 2 switch which normally only forwards broadcast and multicast traffic to all switch ports.

- ✔ ○ **A. Overflow the CAM table with entries**
- ✔ ○ **B. Insure the CAM table can't interact with routing tables.**
- ✔ ○ **C. Insure that the CAM table doesn't interact with spanning tree bringing**
- ✔ ○ **D. Perform a row hammer attack on the CAM memory**

**Answer Key:** A

**Feedback:** Overflowing the CAM table with ARP mapping is the most effective way to put a switch into a mode where it

effectively operated as a hub. None of the other answer make sense.

Question 6 of 18

5.0/ 5.0 Points

You are troubleshooting an intermittent connectivity issue with a web server. After examining the logs, you identify repeated connection attempts from various IP addresses. You realize these connection attempts are overloading the server, preventing it from responding to other connections. Which of the following is MOST likely occurring?

- ✔ **A. Smurf Attack**
- ✔ **B. DOS Attack**
- ✔ **C. DDoS Attack**
- ✔ **D. Salting Attack**

**Answer Key:** C

Question 7 of 18

5.0/ 5.0 Points

What is DHCP snooping?

- ✔ **A. Encryption of the DHCP server requests**
- ✔ **B. A technique used to prevent rogue DHCP servers**
- ✔ **C. Algorithm which is part of DHCP operation**
- ✔ **D. None of the above**

**Answer Key:** B

Question 8 of 18

5.0/ 5.0 Points

Within WPA and WPA2 there are various methods of providing authentication to the wireless infrastructure. Which of the below is NOT a valid authentication type in WPA/WPA2:

- ✔ ◯ **A. EAP-TTLS**
- ✔ ◯ **B. PSK**
- ✔ ◯ **C. EAP-PEAP**
- ✔ ◯ **D. AES-256**

**Answer Key:** D

Question 9 of 18

5.0/ 5.0 Points

There exists a concept called the Base Rate Fallacy. The Base Rate Fallacy presents a problem when designing an IDS/IPS because:

- ✔ ◯ **A. The processing power required to perform signature detection outpaces modern processor architecture**
- ✔ ◯ **B. When intrusion rates are small compared to normal traffic patterns the IDS will produce more than expected false positives.**
- ✔ ◯ **C. It impacts the ability of the IDS/IPS to perform fragmentation reassembly which can be used by an attacker for evasion.**
- ✔ ◯ **D. Memory exhaustion of the IDS system can occur due to the addition state implied with the Base Rate Fallacy**

**Answer Key:** B

Question 10 of 18

A method that is NOT effective for an attacker to evade a signature based IDS/IPS is : 5.0/ 5.0 Points

- ✔ A. Manipulation of attack data
- ✔ B. Fragmentation of traffic
- ✔ C. Attacker performs testing of attack code with offline IDS to insure signatures are not "fired"
- ✔ D. Perform rapid port scanning using NMAP

**Answer Key:** D

Question 11 of 18

Something set up on a separate network (or in DMZ) to attract hackers and lure them away from the real network; it logs keystrokes, provides other information about an attacker, and also provides warning that someone is trying to attack your network. 5.0/ 5.0 Points

- ✔ A. Proxy Server
- ✔ B. Firewall
- ✔ C. Honeypot
- ✔ D. IDS

**Answer Key:** C

Question 12 of 18

All of the following are true statements about Cipher Block Chaining EXCEPT: 5.0/ 5.0 Points

- ✔ A. The IV used in CBC does not have to be secret

- ✔ ○ **B. Provides for unique ciphertext even if the plaintext is repeated**
- ✔ ○ **C. Is implemented in the form of a block cipher**
- ✔ ○ **D. The ciphertext block output is independent of the previous CBC stages.**

**Answer Key:** D

Question 13 of 18

ARP poisoning is an attack technique which: 5.0/ 5.0 Points

- ✔ ○ **A. Sends spoofed IP addresses onto a LAN with the aim of mapping a MAC address to a different IP address.**
- ✔ ○ **B. Sends spoofed ARP messages onto a LAN with the aim of mapping an IP address to a different host MAC address**
- ✔ ○ **C. Remapping of DNS entries to different ip addresses**
- ✔ ○ **D. Remapping of reverse DNS entries to different host names**

**Answer Key:** B

Question 14 of 18

IDS systems can potentially be evaded by all of the following methods EXCEPT 5.0/ 5.0 Points

- ✔ ○ **A. Slowing down the transmission of attack packets**
- ✔ ○ **B. Fragmenting the attack packets**
- ✔ ○ **C. Sending a EIGRP routing update to the IDS system**
- ✔ ○ **D. Encrypting the payload of the attack packet**

**Answer Key:** C

Question 15 of 18

In firewalling and perimeter security, at the end of every filtering rule should be: 5.0/ 5.0 Points

- ✔ ○ **A. Implicit permit all**
- ✔ ○ **B. Implicit deny all**
- ✔ ○ **C. Implicit per ICMP**
- ✔ ○ **D. Implicit deny ICMP**

**Answer Key:** B

Question 16 of 18

If an attacker compromised a DHCP server on a network he/she can do all of the following EXCEPT: 5.0/ 5.0 Points

- ✔ ○ **A. Provide an incorrect default gateway which can be actually be an attacker machine.**
- ✔ ○ **B. Incorrect DNS server. The DNS server can be the attackers DNS and hand out malicious DNS responses.**
- ✔ ○ **C. Incorrect IP addresses which can result in a denial of service condition on the network.**
- ✔ ○ **D. Becoming the DHCP server will initiate ARP poisoning attacks on the local network and can be used for malicious ARP/IP bindings.**

**Answer Key:** D

Question 17 of 18

10.0/ 10.0 Points

Open wireless networks are common in coffee shops, airports and hotels. In these networks there is no encryption and typically no authentication aside from a web page with legal terms of service. If an attackers goal is to perform a man in the middle attack on such a network what would be a feasible way to get in the middle of the conversation between a client wishing to connect to such a wireless network and the Internet. You don't have to describe specific tools. Rather describe the characteristics of open wireless networks that could be exploited for an attacker to inject themselves in the middle of the wireless traffic.

The person can implement an evil twin access (AP) point, a fake wireless access point. The attacker can send wireless frame packets to the the main AP to make it down form frame exhaustion , the attacker now on his machine run the evil twin and copy the same information of the the real APand start broadcasting itself as the fake AP. Other clients will connect to the evil thinking it is the real access point to the internet but actuality your connecting to that machine. the attacker can now able to monitor packets coming from connected devices and the attackers can set up a DNS to reroute to the attackers websever and to create social media login page to simply steal their credentials.

Question 18 of 18

10.0/ 10.0 Points

A common method of exploitation is a "man in the middle attack" where the attacking machine maliciously assumes the position of the default gateway in an IPv4 environment instead of the real default gateway. Now consider how you would perform this same "Man in the Middle" attack if the environment were IPv6. Specifically identify the method IPv6 uses in place of ARP and how this and other characteristics of IPv6 can be used for an attacker to insert themselves in the middle of a conversation.

With my machine I would send a Router Solicement (RS) , it will broadcast to every machine on the network. IPv6 routers task is to s send a router advertisement and advertise itself as the router for that network to later provide entries such as DNS, IP addresses and default gateway. Now I know what IP and DNS is in the router and create spoof the routers IP and add my DNS info whenever a client request a IP address within the network by sniffing any RS coming through the network. With that I can record the devices requesting of for IP, and have routing control from the fake DNS I provided.

Timezone: America/New_York

- Terms of Use
- Send feedback to the NYU Classes Team

## Change Profile Picture

Error removing image
Error uploading image
Upload Choose File No file chosen

Save Cancel Connections ✖ Remove

Search for people ...
View More

My Connections | Pending Connections

You don't have any connnections yet. Search for people above to get started.
You have no pending connections.
←Back to My Connections
Search for people ...
$({cmLoader.getString("connection_manager_no_results")}

Done