

CMSCI 358 Exam 2 (Due 11/6/20)

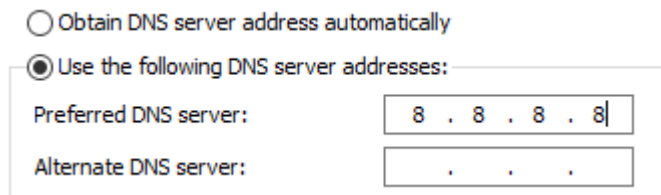
Directions: This is a take-home test. Take as much time as you need for test, as long as it is in by the due date. You may use any resources you like as long as they don't involve another human helping you. For instance, you can use books, class notes, websites, and calculators. But you must not get assistance in any form from anyone in class, any professor, any family member, anybody on the internet, etc. The only exception is you can ask me for clarifications on what a problem is asking.

You can either do your work on the test itself or on a separate sheet. Be sure to show all work.

1. Please write or type a statement in your own words saying that you did not receive assistance on this test, that you did not give anyone assistance, and that this is 100% your own work. **This problem is not optional.**

2. Which of these is the address of a server on the internet that is accessible from most places?
(a) 10.44.57.121 (b) 52.14.144.171 (c) 192.168.22.202 (d) 265.144.97.17

3. Show below is a network setting in Windows being changed in a very particular way. What will doing this help with?



The image shows a Windows network settings window. The 'Use the following DNS server addresses' option is selected. The 'Preferred DNS server' field contains '8 . 8 . 8 . 8'. The 'Alternate DNS server' field is empty.

- (a) It protects against someone intercepting your DNS requests and sending bogus answers.
 - (b) It protects against people sniffing network traffic to see which sites you're visiting.
 - (c) It protects against your ISP's DNS resolver or an evil twin AP's DNS resolver sending you bogus answers to your DNS queries.
 - (d) It protects in case your hosts file has become corrupted.
-
4. One big problem with WEP is
(a) its beacon frames contain the access point's MAC address
(b) it doesn't allow for SSID hiding
(c) it uses a stream cipher in which reusing a keystream is very likely
(d) it uses an insecure scheme to check PINs by breaking into two groups of 4

 5. In NTP amplification, the attacker sends a query to a misconfigured NTP server. The source and destination addresses are
(a) src=attacker, dst=target
(b) src=attacker, dst=NTP server
(c) src=target, dst=NTP server
(d) src=target, dst=attacker

6. The Mitnick-Shimomura attack wouldn't work anymore because
 - (a) TCP initial sequence numbers are randomized.
 - (b) DNSSEC would prevent Mitnick from finding a trusted server.
 - (c) TCP uses a different three-way handshake than it did in the 1990s.
 - (d) Servers are programmed not to send back SYN-ACKs when the source address is spoofed.
7. Port scans are typically performed with which of the following tools?
 - (a) nmap (b) ping (c) traceroute (d) all of these
8. A router queries a network asking which machine on the network has the IP address 10.0.0.7. You reply with your own MAC address, even though you don't have that IP. What type of attack is this?
 - (a) ARP spoofing (b) DNS cache poisoning (c) IP address spoofing (d) MAC address spoofing
9. When someone sets up an evil twin access point, they get people to join their network by
 - (a) giving it a more enticing SSID than the real network
 - (b) periodically varying their network's MAC address
 - (c) making sure their network's beacons are more frequent than the real network's beacons
 - (d) spoofing a deauthentication packet to knock users off the real network and then making sure their network has a higher power than the real network
10. If you send a ping to 255.255.255.255, it won't get through because
 - (a) that's not a real ip address
 - (b) that's a common vector for the ping of death attack
 - (c) pings don't have port numbers
 - (d) pings to that address are blocked to prevent smurf attacks
11. MAC addresses are randomized by some devices because
 - (a) it makes it easier for firewalls to block sites based on MAC addresses
 - (b) it helps prevent certain types of tracking
 - (c) it's required by the TCP specification
 - (d) it helps prevent ARP spoofing
12. ARP spoofing allows an attacker to
 - (a) read the traffic destined for others on a network
 - (b) prevent a host on the network from getting traffic
 - (c) modify the traffic destined for others on a network
 - (d) all of these
13. If you make a request to a web site, that site will *not* see your computer's IP
 - (a) if you're using a VPN
 - (b) if you're behind a NAT
 - (c) both
 - (d) neither

14. If I want to access a computer in my office at MSM using SSH from my computer at home,
- (a) I could look up its IP via DNS and send a request to port 22
 - (b) I could use my Mount VPN access to get onto the Mount's network and access the computer
 - (c) I could not do this because firewalls don't allow SSH access from behind a NAT
 - (d) I could not do this because I can't get through the NAT that my home router uses
15. Which of the following is something an application layer firewall can do that a packet filter cannot?
- (a) Block all traffic to ports 80 and 443
 - (b) Block all traffic containing the word "football"
 - (c) Block all outgoing traffic to IP addresses associated with known malware
 - (d) Trick question. Packet filters can do all of this.
16. Suppose you are on the Mount's network and your friend is on MIT's network. Your friend says her IP address is 10.83.101.25 and her MAC is 23-48-AF-98-88-15. If you send Packet #1 to that IP address and you send Packet #2 to that MAC address, which will your friend get?
- (a) Packet #1 only (b) Packet #2 only (c) Both (d) Neither
17. Why is SHA-1 not recommended for hashing passwords?
- (a) It's not an encryption technique
 - (b) It's too easy for attackers to create other passwords with the same hash
 - (c) It's too fast
 - (d) It's too slow
18. If a TCP port is closed and there is no firewall intercepting things, then a port scanner will typically receive which of these?
- (a) SYN (b) SYN-ACK (c) ACK (d) ACK-ACK (e) RST (f) FIN-ACK
19. Which of these attacks usually involves IP address spoofing? Choose all that apply.
- (a) Echo-charge (b) SYN flood (c) UDP scan (d) HTTP flood
20. Which of the following attacks are considerably easier for attackers on the same network as their target versus being on a different network?
- (a) TCP session hijacking (b) DNS cache poisoning (c) ARP spoofing (d) all of them
21. Which of the following domains are sites that are not part of the Mount's domain? Choose all that apply.
- (a) devices.msmay.edu.a.nl
 - (b) devices.msmay.edu
 - (c) a.nl.devices.msmay.edu
 - (d) msmay.devices.edu
 - (e) msmay.devices.a.nl.edu

22. Which of the following are things a novice hacker could easily do with freely available tools? Choose all that apply.

- (a) Send a packet with a spoofed IP address
- (b) Spoof their MAC address
- (c) BGP hijacking
- (d) Discovering a Wifi network if the administrator has disabled SSID broadcasts
- (e) Break WEP encryption
- (f) Read communication sent via the service that usually runs on port 443

23. True or False.

- (a) _____ The chop-chop attack relies on weaknesses in the algorithm that sees if a Wi-Fi frame has been corrupted in transit.
- (b) _____ The ping of death involves sending an excessive number of pings to flood a target.
- (c) _____ ARP is the system used to associate domain names to IP addresses.
- (d) _____ DNS lookups usually involve the user's web browser contacting at least three different name servers on the internet.
- (e) _____ If someone hacked all the TLD name servers and replaced the resource records with bogus ones, then most of the world would have trouble accessing web sites.
- (f) _____ Malware can block access to antivirus sites by putting 0.0.0.0 entries for those sites into the victim's hosts file.
- (g) _____ When you contact a machine over TCP, the initial response you get back from it will have both the SYN and ACK flags set.
- (h) _____ If a network administrator sends out an ARP query for the address 10.1.2.3, which is not an actual address on the network, and they get a reply, then the person replying is most likely performing ARP spoofing.
- (i) _____ If you don't change the default username and password on your router, attackers can change your router's DNS resolver settings.
- (j) _____ One limitation of denial of service attacks is that the attacking machines cannot cause more traffic at the target than the combined total of their bandwidths.
- (k) _____ The devices with MAC addresses aa:bb:12:34:56:78 and cc:dd:12:34:56:78 are produced by the same manufacturer.
- (l) _____ UDP port scans usually give more conclusive information than TCP scans.
- (m) _____ Egress filtering stops many DDoS attacks because they limit the IP addresses that a site is allowed to contact.
- (n) _____ BGP hijacking is used to redirect traffic destined for certain IP addresses to an attacker.
- (o) _____ WPA2 is the strongest security for Wi-Fi that is widely available.
- (p) _____ Hashing passwords is only recommended if encryption is not possible.
- (q) _____ Rainbow tables for all 10-character passwords of random typeable characters are not available because they would be too large.

24. Below are some rules for a firewall. Answer the questions that follow.

```
iptables -A myfirewall.rules -p icmp --icmp-type any -j ACCEPT
iptables -A myfirewall.rules -p tcp --destination-port 443 -j ACCEPT
iptables -A myfirewall.rules -p all -j REJECT
```

- (a) _____ True/False. This is a blacklist.
- (b) _____ True/False. This server allows HTTP traffic.
- (c) _____ True/False. This server allows HTTPs traffic.
- (d) _____ True/False. This server allows pings.

25. Here is a part of the IP to MAC address mappings on my laptop. Which, if any, of the entries were obtained through ARP queries?

```
Interface: 192.168.1.127 --- 0xc
Internet Address    Physical Address    Type
192.168.1.1        c0-c1-c2-11-2c-d4   dynamic
192.168.1.116      00-11-f4a-8f-f0-3e   dynamic
192.168.1.123      6c-49-62-31-11-20   dynamic
192.168.1.124      db-dd-22-76-0f-f1   dynamic
```

26. For each of the following descriptions, give the specific name of the attack. Your answer needs to be as specific as possible (something like “denial of service” or “port scan” would be too vague).

- (a) An attacker starts a large number of TCP connections on a server with spoofed source IP addresses so that the connections will never be completed.
- (b) An employee working for a major ISP goes rogue and sends announcements to other ISP’s routers claiming to have IP addresses that the major ISP doesn’t really have.
- (c) An attacker instructs their botnet to make a large number of requests to web sites for web pages that require the site to make a lot of resource-consuming database queries.

27. What IDS technique can be defined as “noticing that attacks are happening based on the occurrence of sequences of bytes in packets”?

28. Suppose an attacker has already created a massive list of hashes of all combinations of lowercase letters up to 8 letters long. To stop this list’s effectiveness at breaking password hashes, what should we do?

29. Assuming a password-cracking program can check up to 10 billion passwords a second, how long will it take to crack a password that consists of four random lowercase letters followed by 4 digits? Show your work.