Quiz 1

1. **The Kevin Mitnick Attack**

   : Which o the following movies is based on a hacker's true story?

   a. Titanic
   b. The Shawshark Redemption
   [✓ c. Track Down]
   d. Forrest Gump
   e. Pearl Gump
   f. La La Harbor
   g. Alpha Dog
   h. Catch me if you can

2. **The Kevin Mitnick Arrack**

   : In the process of hacking into Shimomura's server, Kevin Mitnick used a technique called ip spoofing. IP spoofing is a technique in which an attacker creates IP packets with a false destination IP address so as to conceal its identity or impersonate another computer system, true or false?

   a. True
   [✓ b. false]

3. **DoS Arrack**

   : In cybersecurity, DoS stands for Denial-of-service

4. **SYN Flooding Attack**

   : SYN flooding attack is a type of DoS attack, true or false?

   [✓ a. True]
   b. False

5. **SYN Flooding Attack**

   : An attacker launches a SYN flooding attack against the telnet server on a target machine. This particular telnet server listens to two ports, port 23 and port 8023. This attack is only targeting the default telnet port 23. When the attack is undergoing can people still be able to telnet to the server using port 8023?

   [✓ a. Yes]
   b. No

6. **TCP Reset Attack**

   : Describe a scenario where the TCP Reset Attack can be used as a prank?

7. **TCP Reset Attack**

   : Which of the following flag bits need to be set when performing a TCP Reset Attack?

   a. URG
   b. ACK
   c. PSH
   [✓ d. RST]
   e. SYN
   f. FIN

8. **TCP Session Hijack Attack**

   : Which of the following two attacks requires the attacker to know the sequence number 1.TCP Reset Attack 2. TCP Session Hijack Attack

   a. Only 1
   b. Only 2
   c. Both 1 and 2
   d. Neither 1 nor 2

9. **TCP Connection**

   : Typically, how many computers are involved in TCP-3 way handshake?

   a. 1
   b. 2
   c. 3
   d. 4
   e. 5

10. **TCP Connection**

    : Typically, how many packets need to be exchanged between two computers in order to establish a TCP connection?

    a. 1
    b. 2
    c. 3
    d. 4
    e. 5

Quiz 2

1. **TCP Session Hijack Attack**

   : TCP session hijack attack can be performed even if the connection is encrypted, true or false?

   a. True
   b. false

2. **Packet Sniffing**

   : You are in a starbucks coffee shop using its free wifi to access website http://cs.boisestate.edu viayour browser – there is no encryption in http traffic. Jidong is sitting in the same coffee shop and using this same wifi network. T or F: By using wireshark, Jidong would be able to sniff the packets you send to cs.boisestate.edu

   a. True
   b. false

3. **Traceroute**

   : In computer networks, TTL stands for Time-To-Live

4. **Traceroute**

   : ICMP messages are used in traceroute, true or false?

   a. True
   b. false

5. **OSI Model**

: Computers in the same network talk to each other using their MAC addresses, yet human beings usually only knows IP addresses. When you use an IP address to ping some other computer, your computer needs a way to translate that IP address into its MAC address. Which of the following protocols will be used so that your computer would know the destination's MAC address?

a. ARP
b. TCP
c. IP
d. ICMP

6. **OSI Model**

: ICMP messages are used in traceroute, true or false?

Application, Presentation, Session, Transport, Network, Data Link, Physical

7. **Packet Spoofing**

: President Trump is accessing twitter over a TCP connection. A hacker in Russia wants to hijack this TCP session. Let's suppose the hacker somehow knows President Trump's IP address (i.e.. source IP address). Now, he needs some other information so that he can send spoofed packets to Twitter. Which of the following is the Hardest for the hacker to spoof?

a. Destination IP address
b. Source port number
c. Destination port number
d. Sequence number

8. **Firewall**

: Which one of the following statements is true?

a. Firewall is software only
b. Firewall is hardware only
c. Firewall can be a combination of both software and hardware
d. None of the above is true

9. **Subnet**

: An ipv 4 address typically consists of two parts: network section and host section. To split the IP address into these two sections, we use the netmask (also known as subnet mask). Which one of the following is the network section of IP address 172.16.228.1? (Suppose the netmask is 255.255.255.0

a. 172.0.0.0
b. 172.16.0.0
c. 172.16.228.0
d. 172.16.228.1

10. **Firewall**

: To protect your network from being attached by foreign attackers, your firewall needs to have ingress filtering or egress filtering?

a. Ingress filtering
b. Egress filtering

Quiz 3

1. **DNS hierarchy**
   a. An inverted tree structure
2. **DNS Queries**
   : There are two types of DNS queries: recursive query and iterative query. Determine in the following situation, the query is a recursive query or an iterative query. You send a DNS query to a DNS server, and the server does not now the answer, but the answer refers you to some other DNS servers.
   a. Recursive query
   b. Iterative query
3. **DNS Term**
   : In DNS, TLD stands for Top-level Domain
4. **Hide the real IP address**
   : In the song "Good Old Days", Kesha sings "You'll miss the magic of these good old days". Indeed, in the old days, people were honest. Websites were honest about their IP addresses, and they didn't hide their IP addresses. Now, most famous websites hide their IP addresses. Even Kesha's official website hides its IP address. If you ping www.keshaofficial.com, it tells you the IP address is 104.16.202.94, but when you type 104.16.202.94 in your browser, you will only see an error page instead of the main page of the Kesha's official website. Is the following statement true or false? In the above scenario, hiding its IP address is an approach to protect the website from DDoS attack.
   a. True
   b. False (not sure)
5. **Learn Computer Security from Taylor Swift – DNS TTL**
   : Zayn and Taylor Swift recorded the song "I don't wanna live forever" for the film "Fifty shades darker". From DNS security perspective, this title makes perfect sense, and you shouldn't let your DNS records live forever. More specifically, in the DNS database, each DNS record has a TTL value, which tells your local DNS server how long a DNS record should be kept. Once the TTL runs out, your local DNS server will send a query again to the authoritative DNS server so as to get the latest record. From a security perspective, reducing the TTL value is a typical approach to defeat one of the following DNS attacks. Which one it would be?
   a. DNS spoofing
   b. DNS cache poison
   c. DNS pharming
   d. DNS amplification attack
6. **DNS spoofing**
   : During which of the following situation can a DNS spoofing attack take place?
   a. Client-server message exchanges
   b. Server-server message exchanges
   c. Neither of the above
   d. Both client-server message exchanges and server-server message exchanges

7. **Learn Computer Security from Taylor Swift – Virtual Hosting**
   : In Taylor Swift's "Delicate", the lyric goes "I don't want to share". From computer security perspective, this makes perfect sense. In computer security, sharing resource is the root cause of many security problems. However, in the virtual hosting situation, sometimes sharing resources actually can reduce your website's security risk. In a name-based virtual hosting situation, if two websites are hosted on the same physical machine, will they share domain name: and/or IP address?
   a. Domain name will be shared, ip address will also be shared
   b. Domain name will not be shared, ip address will not be shared
   c. Domain name will be shared, ip address will not be shared
   d. Domain name will not be shared, ip address will be shared
8. **DNS Attacks**
   : In the 2004 presidential debate between John Edward and the vice president Dick Cherney. Cherney said the following. Well, the reason they keep mentioning Haliburton is because they're trying to throw up a smoke-screen. They know the charges are false. They know that if you go, for example, to FactCheck.com, an independent website sponsored by the University of Pennsylvania, you can get the specific details with respect to Halliburton. The debate was broadcasted live on TV Within a few minutes, the website of FactCheck.com received a tremendous amount of traffic. Unfortunately for Cheney, the actual website should be FactCheck.org, a politically neutral website, not FactCheck.com. George Soros, who does not like president Bush, immediately capitalized on this mistakes by somehow redirecting all the FackCheck.com bound traffic to his own website, where the top item is an article by Soros entitled "Why we must not Re-Elect President Bush". If you were an attacker, and George Soros hired you to redirect all the FackCheck.com bound traffic to his website, which of the following attacks, if successful, could make this happen?
   a. DNS spoofing
   b. DNS cache poison
   c. DNS pharming
   d. DNS amplification attack
9. **DNS Attacks**
   : Which of the following DNS attacks is a type of DoS attack?
   a. DNS spoofing
   b. DNS cache poison
   c. DNS pharming
   d. DNS amplification attack
10. **DNSSEC**
    : DNSSEC is a set of extensions to DNS, it makes DNS systems more secure. Is the following statement true or false. Digital signatures are introduced in DNSSEC, and by checking the digital signature, we can verify if a DNS response is legitimate or fake.
    a. True
    b. False

Quiz 4

1. **Remote DNS cache poisoning attack**
   : The remote DNS cache poisoning attack we learned in this class was originally proposed/presented by _______________.
   a. Kobe Bryant
   b. Dennis Bergkamp
   c. Kevin Mitrick
   d. Britney Spears
   e. Lee Min-ho
   f. Ryan Gosling
   g. Justin Timberlake
   h. Lady Gaga
   i. Dan Kaminsky (not sure)
   j. Shawn Mendes
2. **DNS Source Port Randomization**
   : Randomizing source port number makes remote DNS cache poisoning attack easier or harder?
   a. easier
   b. harder
3. **Subdomain**
   : Which is the following statements is correct
   a. www.fakenews.com is a subdomain of cnn.com
   b. My.boisestate.edu is a subdomain of www.boisestate.edu
   c. www.boisestate.edu is a subdomain of boisestate.edu
   d. Boisestate.edu is a subdomain of www.boisestate.edu
   e. www.gmail.com is a subdomain of www.google.com
   f. Store.brunomars.com is a subdomain of www.brunomars.com
4. **Learn Computer Security from Adele – DNS Cache Poisoning**
   : In Adele's song "Set Fire To The Rain", the lyric goes "All the things you'd way, they were never true, never true" From security's perspective, if you want to perform DNS cache poisoning attack, you need to "say" something that is not true. More specifically, if you want to poison a DNS server so that the DNS server believes Yellowstone.boisestate.edu is the DNS server responsible for maroon5.com, you need to inject a fake record, and this record will be a/an _____________.
   a. CNAME record
   b. NS record
   c. AAAA record
   d. MX record
5. **Learn Computer Security from Adele – DNS Cache Poisoning**
   : In Adele's song, "Set Fire To The Rain", the lyric goes "And the games you play, you would always win, always win". From security's perspective, if you, as an attacker, want to successfully perform the remote DNS cache poisoning attack, you need to win a competition. The competition is

a. Your fake response needs to reach the victim DNS server earlier than the authoritative name server's response.
b. Your fake response needs to reach the victim DNS server later than the authoritative name server's response.
c. Your fake request needs to reach the victim DNS server earlier than the authoritative name server's request
d. Your fake request needs to reach the victim DNS server later than the authoritative name server's request.

6. **VPN**

: True or False. VPN requires a dedicated line between the client and the server
a. True
b. False

7. **Private IP address**

: Which of the following is NOT a private IP address.
a. 10.0.2.3
b. 172.16.228.165
c. 132.178.28.16
d. 192.168.25.224

8. **VPN**

: When you use your laptop to connect to Boise State's VPN service from your home. Is this connection a client-to-site connection or a site-to-site connection?
e. Client-to-site connection
f. Site-to-site connection

9. **VPN Term**

: In computer networks, VPN stands for Virtual Private Network

10. **VPN**

: In "House of Cards" season 2, episode 2, the secret service agent disconnects Vice President Frank. Underwood's video game console from the Internet because "It's not a secure connection". Imagine you were the secret service agent, if Frank Underwood really wants to play that online game from security's perspective you could let him use VPN. Explain why VPN would make his connection secure.

Encapsulation (Private IP address not routable on the Internet. Enclose a packet within another packet that has a different IP source and destination information), Encryption, Authentication

Quiz 5

11. **Certificate Authority**

: Which of the following is NOT a well known Certificate Authority company?
k. Comodo
l. Symantec

m. GoDaddy
n. GoMommy
o. DigiCert
p. GlobalSign

12. **Heartbleed**

: The heartbleed vulnerability was identified in the implementation of which protocol?

c. TCP
d. DNS
e. ARP
f. SSL/TLS
g. IP

13. **Encryption**

: Using the same key to encrypt and decrypt data is called _______________

g. Symmetric encryption
h. Asymmetric encryption

14. **Public/Private Key Pair**

: Nowadays most well known websites have deployed HTTPS, in which data is encrypted during transmission. Even CNN is using HTTPS, which is weird, because some people don't understand why encryption is needed when the only thing they transmit is fake news. More specifically, a pair of public key and private key is used for this encryption/decryption procedure, and which of the following statements is correct?

e. A private key will be used to encrypt a message, and a public key will be used to decrypt a message
f. A public key will be used to encrypt a message, and a private key will be used to decrypt a message
g. A private key will be used to encrypt and decrypt a message
h. A public key will be used to encrypt and decrypt a message

15. **Digital Signature**

: A public key certificate normally includes a public key, the identity of the owner, and a digital signature. Normally certificate authorities sign a certificate with their digital signature and everyone else can verify if the signature of this certificate is valid or not. Which of following statement correctly describes this signing and verifying procedure?

e. A private key will be used to sign a certificate, and a public key will be used to verify a certificate
f. A public key will be used to sign a certificate, and a private key will be used to verify a certificate
g. A private key will be used to sign a certificate and verify a certificate
h. A public key will be used to sign a certificate and verify a certificate.

16. **Digital Signature**

: From Wikipedia: "A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity)". True or false: Digital signature is based on public key cryptography.

c. True

d. false

17. PKI

: In computer cryptography. PIK stands for Public Key Infrastructure

18. MITM Attack

: 2018 has truly been a year of great loss for a lot of us. Like, Jidong just lost 3 HTTP packets. It turns out there is an attacker sits in between Jidong and the web server he was trying to access, and the attacker simply dropped some of Jidong's HTTP packets. In computer security, this type of attack is called MITM attack. And what does MITM stand for?

Man in the middle Attack

19. PIK

: Which of the following MITM attacks can be defeated by PKI?

g. Attacker forwards the authentic certificate

h. Attacker creates a fake certificate

i. Attacker sends its own certificate

j. All of the above

20. SSL/TLS

: The SSL/TLS protocol sits in between which two layers of the OSI model?

a. Application layer and Transport layer

b. Application layer and Presentation layer

c. Transport layer and Physical layer

d. Transport layer and Data link layer

e. Network layer and Physical layer.

Final Exam

1. **DNS: knowing the dig command**
2. **DNS: knowing the basics of the Dan Kaminsky attack**
   : DNS cache poisoning vulnerability. Discovered by Dan Kaminsky in 2008. Root cause: DNS transaction ID: only 2 to the 16 (65536) possibilities. Target non-existing sibling subdomains – bypass cache effect or TTL defense.
3. **DNS: understanding various DNS attacks described in he slides.**
   a. DNS spoofing
      - impact: temporary
      - Answering DNS request that intended for another server(a real DNS server)
      - Spoofs the DNS server's answer by answering with the DNS server's IP address in the DNS server's IP address in the packets source-address field
      - Client-server exchange or server-server exchange

   b. DNS cache poison
      - impact: permanent (or until ttl expires)
      - Making a DNS server cache false information
      - Try to make the ns.defense.gov DNS to answer with the IP of the hacker's computer to any query about the IP of telnetaccess.dense.gov

   c. DNS pharming
      - impact: permanent
      - Change the DNS server setting on a victim's computer
      - Change the DNS server setting on the DHCP server.
      - DHCP: Dynamic Host Configuration Protocal

   d. DNS amplification/reflection
      - impact: temporary
      - A type of DoS attack
      - Forgeability of source addresses of DNS messages.
      - Availability of open resolvers: A DNS resolver is open if it provides recursive name resolution For clients outside of its administrative domain.
      - Asymmetry of DNS requests and responses.
4. **DNS: knowing the basic idea of DNNSEC**
   : Domain Name System Security Extension. Digital signatures are introduced into DNS responses – checks the digital signature to verify if it's a valid or fake response. Deploy DNSSEC takes time due to practical issues.
5. **DNS: knowing the different types of DNS queries**
   : Recursive queries: the DNS client requires that the DNS server respond to the client with either the requested resource record or an error message stating that the record or domain name does not exist. The DNS server cannot just refer the DNS client to a different DNS server. If a DNS server does not have the requested information when it receives a recursive query, it queries other servers until it gets the information, or until the name query fails.

Iterative queries: when a DNS client allows the DNS server to return the best answer it can give based on its cache or data. If the queried DNS server does not have an exact match for the queried name, the best possible information it can return is a referral.

6. **DNS: understanding the meaning of various types of DNS records**
   : DNS resource record(RR), A record: address record, AAAA record: IPv6 address record, CNAME record: alias, NX record: Mail exchanging record, NS record: Name server record
7. **DNS: understand private IP addresses vs public IP addresses**
   :
8. **VPN: the basic idea**
   : Virtual Private Network
   IP addresses reserved for organizations to use, not routable on the Internet. (10.0.0.0 ~ 10.255.255.255, 172.16.0.0 ~ 172.31.255.255, 192.168.0.0 ~ 192.168.255.255)
   Connect two or more private networks in a secure way. Hid your identity and IP address.
   VPN does not use a dedicated line, rather, it uses the same public Internet connections that millions of people use.
9. **VPN: the core activities in included in VPN**
   : Encapsulation (Private IP address not routable on the Internet. Enclose a packet within another packet that has a different IP source and destination information), Encryption, Authentication
10. **Subdomain: meaning of subdomain**
11. **Subdomain: how to tell if one domain is the subdomain of another domain**
12. **Knowing how digital signature is signed and verified**
    : Based on public key cryptography: signed with the signer's private key, verified by anybody who has the signer's public key. Once a message is signed, altering the content of the message would make the signature invalid.
    Public key certificate : consists of a public key, identity of the owner, signature of a trusted party. Recipient can verify the signature to ensure the integrity of a certificate.
    Certificate Authority Market Share (Comodo, IdenTrust, Symantec, GoDaddy, GlobalSign, DigiCert)
13. **Understanding Heartbleed**
    : You can get the information with Heartbleed attack (passwords, credit card numbers, medical records, contents of private email or social media messages, server's private encryption key)
    - SSL/TLS : secure sockets layer/ transport layer security. A protocol used for establishing an encrypted link between a server and a client (typically a web server and a browser). TLS is the successor of SSL.
    - HTTPS : A protocol for secure communication over a computer network. HTTPS consists of communication over HTTP within a connection encrypted by SSL/TLS: The webpage you are viewing is transmitted to you in an encrypted form, default port 443.
14. **Understanding Shellshock**
    : a security bug in bash (bash shell). Bash executes some commands contained in environment variables.
    - Shell: Command-line interpreter in operating systems. Reads cmd from console and execute them.
    - Environment Variables: A set of named values that affect the way a process behaves
    - CGI: Common Gateway Interface: Utilized by web servers to run executable programs that dynamically generate web pages.

- Two conditions to trigger shellshock: invocations of bash, passing of user data as environment variables.

15. **Understanding Buffer overflow vulnerabilities**
    - Buffer Overflow: during memory copying, more data copied to the destination buffer than the amount of allocated space. Consequence: program crash, or arbitrary code execution – logic of the program will be different from the original one.
    - Stack: used for storing local variables defined inside functions, as well as storing data related to function calls, such as return address, arguments
    - Stack Frame: When a function is called, a block of memory space will be allocated on the top of the stack, and it is called stack frame.
    - Return address: the address following the call instruction. When a function finishes and hits the return instruction, it needs to know where it returns to
16. **Acronyms: can be anything covered in the slides (except those we learned before DNS security)**
17. **Knowing the difference between HTTPS and HTTP**
18. **Knowing the basic idea of public key cryptography**
19. **Public key infrastructure: what the major problem existing in asymmetric encryption and what's the major technique introduced in Public key infrastructure so as to address this challenge, how public key infrastructure can defeat all the three situations mentioned in the slides.**
    - Symmetric Encryption
        - Use one key to encrypt information, use the same key to decrypt information
    - Asymmetric Encryption
        - Known as public key encryption, or public key cryptography. Use a public key to encrypt information, use a private key to decrypt information. More secure than symmetric encryption.
    - Main-in-the-middle Attack (MITM attack)
        - Happens when someone else is intercepting the traffic between two devices.
        - If PKI is used, Attacker forwards the authentic certificate, Attacker creates a fake certificate, Attacker sends its own certificate
20. **Buffer overflow: Understanding and being able to explain various defenses against buffer overflow**
    - Address Space Layout Randomization (ASLR)

```
- #include <stdio.h>
- #include <stdlib.h>
-
- void main()
- {
-   char x[12];
-   char *y = malloc(sizeof(char)*12);
-
-   printf("Address of buffer x (on stack): 0x%x\n", x);
-   printf("Address of buffer y (on heap): 0x%x\n", y);
- }
```

- Write XOR execute (in Windows, this is called Data Extension Prevention or DEP).
- StackGuard