Kang-Wei Chang
kwc305
Network Security HW1

1.
Confidentiality is prevent unauthorized reading of information.
Integrity is prevent unauthorized writing of information.
Availability: Data is available in a timely manner when needed
Authenticity is determining the origin of data – Type of Integrity
Non-Repudiation: proving the integrity and origin – Type of Integrity

2.
a.
A risk consists of something of value (an “asset” at risk) which may lose value if a negative event occurs.
A threat to a system is any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system.
b.
A vulnerability of a system is some characteristic that makes it possible for a threat to occur.
An attack (exploit) on a system is some action that involves exploitation of some vulnerability in order to cause an existing threat to occur.

3.
1 billion(SLE) multiple 1/5(ARO) = 200 million dollar.

4.
Install improperly—100k and Blackmail—100k

5.
Non-technical:
Dumpster Diving
Social Engineering
Educate your users about giving out sensitive or confidential information over the phone. Caller-id DOES NOT provide authentication
Physical Break in
You can have the best, multimillion dollar security system on the market but it will be useless if you don’t lock the front door.

Technical:
Nmap
Scanning:
IDLE Scan
Firewalk

6.
Arecord:address record. Describe the IP address that a given node has
AAAA Record: AAAA records are IPv6 address records which map a host name to an IPv6 address

NS Record: NAME SERVER. DOMAIN NAME SERVERS WHICH SERVE THIS DOMAIN NAME
MX: Mail exchange, IP address of the server, which handle the mails for the domain.
TXT Record: Originally for human readable information. But now used for things such as domain-keys
DNSKEY Record: The key record used in DNSSEC. Uses the same format as the KEY record.

7.
DNS Zone Transfer: It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers
Brute Force Forward DNS: basically brute-force common names of hosts via DNS query and based on response from DNS server it identify if the host exist or not.
Split DNS: is an implementation in which separate DNS servers are provided for internal and external networks as a means of security and privacy management.

8.

```
Registrant:
   New York University
   ITS Communications Operations Services
   7 East 12th Street, 5th Floor
   New York, NY 10003
   UNITED STATES
```

I type the following command: whois nyu.edu

9.

```
Administrative Contact:

   NYU Network Operations Admin Role Account
   New York University, ITS C&CS
   7 East 12th Street
   5th Floor
   New York, NY 10003
   UNITED STATES
   (212) 998-3431
   domreg.admin@nyu.edu
```

I also use the same command with Q.8

10.
TCP Connect scan - This type of scan is the most reliable, although it is also the most detectable. It is easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK, whereas closed ports respond with an RST/ACK.
TCP SYN scan - This type of scan is known as half open because a full TCP three-way connection is not established. This type of scan was originally developed to be stealthy and evade IDS systems although most now detect it. Open ports reply with a SYN/ACK, whereas closed ports respond with a RST/ACK.

Nmap is more reliable and easier to be detected by host, however, SYN scan just send SYN packet, the connection is not Establish.

11.
a. It means that the port is open
b. It means that the port is close
c. In the port scan, if get an ICMP message, it may because ICMP destination unreachable.
d. It means port not exist
12.
a. It means that the port is close
b. It means port not exist

13.
IDLE scan

Attacker first picks the machine which will be “framed” for the attack.

Attacker sends a SYN packet to the “framed” machine

Attacker gets back a SYN-ACK which will include the IP header with IP ID value of X which is remembered by the attacker.

Next step is the attacker selects the port to be scanned and sends a spoofed SYN packet to the target with the “framed” machine’s ip.

If listening the target will send a SYN-ACK back to the framed machine

When the “framed” machine receives a SYN-ACK from the target which was never requested it will send a RESET. The IP ID field on the “framed” machine will be X+1

Attacker now “measures” the IP ID field on the “framed” machine. Sends SYN. If gets IP ID value of X+2 then port is open. If IP ID is X+1 then it is closed

14.
FTP bounce scanning
Use Hping
Use IDLE scan

15.
Ingress filtering checks the source IP field of IP packets it receives, and drops packets if the packets don't have an IP address in the IP address block that the interface is connected to. However, if in same IP field, there are many IP, it means that one IP can spoof as another IP in the same field.

16.

Denial of Service
Insertion
Evasion

17.
If SYN-flood attack with spoofed IP address, there is no ACK comes back to B for connection. If the server then receives a subsequent ACK response from the client, the server is able to reconstruct the SYN queue entry using information encoded in the TCP sequence number. So, B is not waiting for an ACK

18.
Both two method are use Spoof source IP address = victim's IP, so after NTP/DoS bot get request, both of them will send reply to the victim, which crash the victim.

19.
If trudy wants to poison the DNS, he needs to send a dans lookup request, and if the cache already have record for amazom.com, it would be not able to poison, because it already have record, so Trudy need to clean the cache first, and than send a request for amazon's ip address, before local dans get the real ip address, send the reply to local dans server with fake ip address.

20.
Inline – Shellcode to be executed is delivered in one block. Single payload stage. Disadvantage is that it might be too big to deliver in a single stage.
Staged – The first payload is just a small stub which then grabs the reset of the shellcode.
Reverse – Instead of the attacker connecting to the payload on the exploited host. The payload on the exploited host connects back to the attack. Good for inside firewalls.