Homework #1 – CS6823 – Network Security

Directions: Keep your answers as short as possible. Most subquestion should be answered in no more one sentence. This assignment is based on Lecture 1 and 2 (which includes week 1, 2, and part of 3.) Do cite your sources if you use other than the lecture slides.

1. [6 pts] Describe the steps in the TCP 3-way handshake, including SEQ and ACK numbers.

The client sends a SYN packet to the server to establish communication including a sequence number. The server responds with a SYN/ACK packet with another sequence number and an acknowledgment number of the original sequence number plus one. Finally the client responds with an ACK packet with the received sequence number plus one.

1. [8 pts] What are the four possible responses to a TCP SYN packet, and the meaning of each?

2.1 A TCP SYN/Ack means that port is open.

2.2 A RST/ACK packet means port is closed or there is a firewall

2.3 An ICMP is unreachable means firewall is rejecting packet or networkr problem.

2.4 No response means that firewall is dropping packet or network issue.

1. [6 pts] What are the three possible responses to a UDP packet, and the meanings of each?

3.1 A UDP packet is sent back means its open

3.2 ICMP unreachable means that port is closed

3.3 No response can mean packet was misformatted, firewall blocked, or packet ddropped

1. [8 pts] What’s the difference between:

**Risk** and **Threat**

A risk is a potential for loss while a threat is something or someone that can exploit you.

**Vulnerability** and **Exploit**

Vulnerability is a weakness or gap in a security system while an exploit is acting on the vulnerability.

1. [10 pts] On lecture 1, slide 34 titled “Mitigating Risk”, what mitigation would you recommend to bring the risk #1 to the green zone? What’s the final residual risk level?

I would recommend reducing the consequence as much as possible. The residual risk level can vary depending on the severity of the consequences.

1. [6 pts] Suppose a credit card company gets compromised once every four years and two million credit cards numbers each time. The cost of replacing credit cards, charge-back fraud, and fraud is ten million dollars. How much can the credit card company spend each year on prevention of being compromised if it guarantees the company won’t be hacked anymore?

The annual rate of occurrence is .25 and the single loss expectancy is $10m making allowing the company to spend up to $2.5m a year on cyber security.

1. [6 pts] In the lecture 1 slide 45 titled “Cost of an Attack” (attack trees) what is the most expensive attack(s)? What is the cheapest attack(s)?

The cheapest attack is cutting the safe open. The most expensive are installing the safe improperly or a bribe.

1. [6 pts] List **three** Google hacking keywords with an example of each.

a. search keyterm within give site `site:itp.nyu.edu mark lam`

b. inurl searches sites with a given domain `inurl:itp mark lam`

c. intext finds pages with a certain word in the content `intext:itp mark lam

1. [6 pts] Describe **three technical** and **three non-technical** ways to perform reconnaissance on a company.

Non-technical ways you can perform reconnaissance is to do google hacking, call the company, and visit the physical location

Technical ways can involve doing a whois lookup, a dns lookup, and network mappipng.

1. [6 pts] Describe what each of the following DNS records are:
   1. A Record – Maps domain to IP address
   2. AAAA Record – map ipv6 ipaddress to domain
   3. NS Record – Domain name servers which serve domain
   4. MX Record – IP address that handles mail service
   5. TXT Record – free space for human readable text
   6. DNSKEY Record – holds a public signing key (https://www.cloudflare.com/learning/dns/dns-records/dnskey-ds-records/)
2. [9 pts] Describe in detail what each of the following DNS terms are:
3. DNS Zone Transfer

DNS Zone transfer is used to transfer dns names called a zone file from one server to another dns server.

1. Brute Force Forward DNS

This is to lookup various subdomains to see if they resolve to an ip address.

i.e. ping test.example.com test1.example.com mail.example.com etc...

1. Split DNS

This is when you have multiple dns servers. One for internal and external uses. Used as a security measure.

1. [5 pts] What’s the mailing address (snail mail) registered with the domain name amazon.com? How did you find it?

Admin Street: P.O. Box 8102   
Admin City: Reno   
Admin State/Province: NV   
Admin Postal Code: 89507   
Admin Country: US  
  
I did a whois lookup on amazon.com

1. [6 pts] What’s the MX record associated with the amazon.com? How did you find it?

|  |  |  |
| --- | --- | --- |
| 5 | [amazon-smtp.amazon.com](https://mxtoolbox.com/SuperTool.aspx?action=a%3Aamazon.com&run=toolpage) | [207.171.188.180](https://mxtoolbox.com/SuperTool.aspx?action=a%3Aamazon.com&run=toolpage) |

I used mxtoolbox.com

1. [6 pts] According to ARIN, what entity is the IP address 192.76.177.1 allocated to? Explain.

I used whois to lookup the ip address. It responded that NYU owns the 192.76.177.0 – 192.76.177.255 block of ip address.

1. [6 pts] Describe the kind of information can be expected to be obtained from using DNS services only.

You can get various ip addresses that are associated with a domain such as:

* 1. A Record – Maps domain to IP address
  2. AAAA Record – map ipv6 ipaddress to domain
  3. NS Record – Domain name servers which serve domain
  4. MX Record – IP address that handles mail service
  5. TXT Record – free space for human readable text

DNSKEY Record – holds a public signing key