Homework #1 – CS6823 – Network Security

Directions: Keep your answers as short as possible. Most subquestion should be answered in no more one sentence.

1. [5 pts] Define these terms: **Confidentiality**, **Integrity**, **Availability**, **Authenticity**, and **Non-Repudiation**.
2. [4 pts] What’s the difference between:

**Risk** and **Threat**

**Vulnerability** and **Exploit**

1. [8 pts] Suppose a credit card company gets compromised once every five years and loses millions of credit cards numbers each time. The cost of replacing credit cards, charge-back fraud, and fraud is one billion 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?
2. [4 pts] In the lecture 1 slide titled “Cost of an Attack” (attack trees) what is the most expensive attack(s).
3. [6 pts] Describe **three technical** and **three non-technical** ways to perform reconnaissance on a company.
4. [6 pts] Describe what each of the following DNS terms are:
   1. A Record
   2. AAAA Record
   3. NS Record
   4. MX Record
   5. TXT Record
   6. DNSKEY Record
5. [6 pts] Describe in detail what each of the following DNS terms are:
6. DNS Zone Transfer
7. Brute Force Forward DNS
8. Split DNS
9. [4 pts] What’s the registrant mailing address (snail mail) registered with the domain name nyu.edu? How did you find it?
10. [4 pts] What’s the e-mail server (electronic mail) associated with the domain name nyu.edu? How did you find it?
11. [4 pts] What’s the difference between the nmap Connect scan and SYN Scan?
12. [4 pts] When performing an nmap **SYN** scan of a target, what does one meaning when the target responds with:
    1. SYN/ACK
    2. RST/ACK
    3. Some ICMP response
    4. No response
13. [4 pts] When performing an nmap **ACK** scan of a target, what does one meaning when the target responds with:
    1. RST/ACK
    2. No response
14. [4 pts] Which nmap scan type takes advantage of the flaw in the IP ID field? Explain how this attack works.
15. [6 pts] What are **three ways** to perform a port scan of a target without the target seeing the IP address of the attacker?
16. [5 pts] Define ingress filtering and explain why it’s difficult to implement ingress filtering to stop IP source spoofing.
17. [6 pts] Suppose Trudy is trying to hijack a telnet session between Alice and Bob. In order to successfully impersonate Alice, Trudy must stop Alice from communicating. What are **three ways** that Trudy can achieve that?
18. [4 pts] How does SYN cookies protect against SYN floods?
19. [4 pts] How is DNS amplification attack similar to NTP amplification attack?
20. [6 pts] If Alice and Trudy were on the same local network (e.g., 10.11.110.0/24), explain how difficult it would be for Trudy to poison Alice’s DNS cache to amazon.com
21. [6 pts] What’s the difference between the metasploit **inline**, **staged**, and **reverse** payloads?