Midterm – CS6823 – Network Security – Fall 2018

David Ho Dh2487

1a. [3 pts] How much does it cost to “Hack into Database” by “Obtain Admin Password” with no special tools?

**With no special tools, it is not possible to “Hack into Database” by “Obtain Admin Password” as you’d have to “Install Malware on a Computer” which requires a special tool.**

1b. [3 pts] If the attacker had access to Special Tools, what is the cheapest method to “Steal Credit Cards from MySQL Database”? (Special Tools includes ST and NST.)

**The cheapest method is to “Obtain Physical Access” which requires you to “Break into Server Room” for 50k and “Bribe Guard” for 20k.**

**Total of 70k.**

1c. [4 pts] Suppose due to a vulnerability, “Install malware on a computer” is now Free. How does that change the answers 1a and 1b?

**For 1a, even though it is now free, it depends on whether you still need “Special Tools”. Because free could mean no charge but still require special tools. If it does still require special tools, then there is no change, but if it now no longer does, then it costs 200k for 1a.**

**My assumption is that even though it is free, installing malware will require special tools or skills so it would not change.**

**It does not change for 1b.**

2. [10 pts] Suppose Trudy, the bad guy, installed a secret tftp server on a UDP port on the host 10.10.111.101. You know there’s a tftp server, but don’t know which port. Explain in detail how would you figure that out? Explain if it’s easy or hard.

**Since you know that the tftp server is on a UDP port, you would have to scan all the UDP ports. Getting a response shows that the port is open, an unreachable error means that its closed, and no response means that there is a firewall, but since it’s your system this would not be a problem other than the server. UDP port scanning is “hard” in the sense that it takes significantly longer than for TCP ports, though the actual check itself is relatively easy.**

3. Risk Assessment. ACME Corporation has a MySQL database that contains credit card numbers. The company does not have good security patch management and takes over 120 days to patch Windows after Patch Tuesday. Suppose the Windows 2016 Server that hosts the MySQL database has a probability of being compromised once in 24 months and each time it’s compromised, it loses 1 million CC numbers. Suppose ACME will be fined $1 per CC number lost and $100k one-time marketing fee to repair ACME’s reputation.

3a. [3 pts] What’s the Single Loss Expectancy (SLE)?

**Single Loss Expectancy is 1.1million dollars for the first incident.**

**Single Loss Expectancy is 1million dollars after the first.**

3b. [2 pts] What’s the Annualized Rate of Occurrence (ARO)?

**Annualized Rate of Occurrence is 0.5**

3c. [2 pts] What’s the Annualized Loss Expectancy (ALE)?

**Annualized Loss Expectancy for the first two years is 550k**

**Annualized Loss Expectancy afterwards is 500k**

3d. [3 pts] Would hiring a team of Cybersecurity professionals which costs $300k/year be worth it if the specialist can stop all attacks? Why or why not?

**Yes it would be worth it because it is cheaper to hire the professionals than to repeatedly pay the fine every time the database is compromised.**

4. DNS. Suppose Trudy was able to install malware on a host in nyu.edu, and now Trudy wants to establish a covert channel for two-way communications. NYU requires that all DNS traffic to go through the NYU Primary DNS Server; everything else is blocked by the firewall. Answer the following questions using only the DNS protocol. 4a. [4 pts] How would Trudy send a one kilobyte (1024 bytes) file to her server, evil.com?

**The file would still have to go through the NYU Primary DNS Server so it would have to be hidden in the data field.**

4b. [4 pts] How would Trudy be able to send commands to the malware on the host?

**You can send commands by hiding the commands in the sequence number or data field or even through timing of sending the requests.**

4c. [4 pts] What are two ways nyu.edu can detect and stop these two covert channels?

**NYU could check the data fields for unusual files or text. NYU Could also check the sequence numbers to make sure there are not patterns or repeats. Also turn off DNS Zone Transfer.**

5. Explain in detail the purpose of each scapy code fragment. Also specify how many packets are expected to be sent out for each.

5a. [4 pts] sr1(IP(dst=”10.10.10.10”)/TCP(dport=80,flags=”S”))

**Sending out one TCP Syn packet to 10.10.10.10 on port 80. SR1 is send and receive, so you are waiting for a response**

5b. [4 pts] Ether(dst="ff:ff:ff:ff:ff:ff")/IP(dst=[“10.10.10.11”,”10.10.10.12"],ttl=(1,9))/UDP()

**Sending out 18 UDP packets, 9 to 10.10.10.11 and 9 to 10.10.10.12, with a ttl range of 1 to 9. (ping)**

5c. [4 pts] ans, unans = sr(IP(dst=“10.10.10.13",ttl=(1,10))/TCP(dport=53,flags="S"))

**Sr gives both answered and unanswered packets. So you are setting variables for both. You are sending out 10 TCP Syn packet to 10.10.10.13 on port 53. Time to Live is a range 1 through 10.**

6. [10 pts] Compute 567 mod 15 (five raised to the sixty-seven mod fifteen) without a calculator. Write out your calculations.

**5 mod 15 = 5**

**52 mod 15 = (5mod15 \* 5mod15)mod 15 = 25mod15 = 10**

**54mod 15 = (10 \* 10) mod 15 = 10**

**58mod 15 = (10 \* 10) mod 15 = 10**

**516 mod 15 = (10 \* 10) mod 15 = 10**

**532 mod 15 = (10 \* 10) mod 15 = 10**

**564 mod 15 = (10 \* 10) mod 15 = 10**

**566 mod 15 = (10 \* 10) mod 15 = 10**

**567 mod 15 = (5\*10) mod 15 = 5**

**ANSWER: 5**

7. Perform RSA key generation. Suppose p=5 and n=115. Note: you must show work for any modular mathematics. 7a. [2 pts] What would be the value of q?

**n = p \* q**

**115 = 5q**

**q = 23**

7b. [1 pt] Compute φ

**φ = (p-1)\*(q-1) = 4 \* 22 = 88**

7c. [2 pts] Find the five smallest possible values for public (encryption) exponent e

**e and φ must be relatively prime.**

**e = 3,5,7,9,13**

7d. [3 pts] Using the smallest e from 7c, choose a private (decryption) exponent d

**edmod φ = 1**

**d = 39**

7e. [3 pts] Encrypt m=5

**c = me mod n**

**53 mod 115**

**51 mod 115 = 5**

**52 mod 115 = (5\*5) mod 115 = 25**

**53 mod 115 = (25 \* 5) mod 115 = 125 mod 115 = 10**

**c = 10**

7g. [3 pts] List and explain one positive and one negative for using RSA encryption.

**A positive use of RSA encryption is that it is extremely difficult to crack as finding p and q from n is difficult to match the parameters. Therefore, it is relatively safe to use RSA encryption to encrypt smaller messages.**

**A negative use of RSA encryption is that it takes a relatively long time (~5 sec per) so it is not good at encrypting and decrypting long messages.**

8. Basic Cryptography. 8a. [3 pts] Decrypt “KNWJBFQQ” with Julius Caesar’s Cipher of key +5 (positive five).

**FIREWALL**

8b. [4 pts] Using the standard Vigenere (Poly-alphabetic Encryption) table, encrypt the message HELLO using the key FED.

**MIOQS**

8c. [3 pts] Use the following substitution cipher to encrypt “NETWORK” Plaintext: abcdefghijklmnopqrstuvwxyz Ciphertext: mnbvcxzasdfghjklpoiuytrewq

**JCURKOF**

9a. [3 pts] If Trudy intercepted Ciphertext 100100100100 from Alice to Bob and knows that CFB is used, can she easily figure out that blocks are repeating?

**No, CFB is used so that repeated plaintext does not produce repeated ciphertext.**

9b. [6 pts] Encrypt Ciphertext 100 100 100 100 using CFB and IV=111

**E(IV) XOR PT1 = E(111) XOR 100 = 010 XOR 100 = 110**

**E(CT1) XOR PT2 = E(110) XOR 100 = 001 XOR 100 = 101**

**E(CT2) XOR PT3 = E(101) XOR 100 = 000 XOR 100 = 100**

**E(CT3) XOR PT4 = E(100) XOR 100 = 011 XOR 100 = 111**

**110 101 100 111**

9c. [3 pts] Verify your work by decrypting the message in 9b.

**E(IV) XOR CT1 = E(111) XOR 110 = 010 XOR 110 = 100**

**E(CT1) XOR CT2 = E(110) XOR 101 = 001 XOR 101 = 100**

**E(CT2) XOR CT3 = E(101) XOR 100 = 000 XOR 100 = 100**

**E(CT3) XOR CT4 = E(100) XOR 111 = 011 XOR 111 = 100**

**100 100 100 100**