

1. Intrusion Detection and Firewalls

(a) Consider the following ipchain rule sets:

Rule Set A:

```
ipchains -P input ACCEPT
ipchains -P forward ACCEPT
ipchains -P output ACCEPT
ipchains -A input -i eth0 -s 0/0 -d 0/0 22 -p tcp -y -j ACCEPT
ipchains -A input -i eth0 -s 0/0 -d 0/0 -i lo -j ACCEPT
ipchains -A input -i eth0 -s 110.208.x.y 53 -d 0/0 -p udp -j ACCEPT
ipchains -A input -i eth0 -s 110.208.z.v 53 -d 0/0 -p udp -j ACCEPT
ipchains -A input -i eth0 -s 0/0 -d 0/0 -p tcp -y -j REJECT
ipchains -A input -i eth0 -s 0/0 -d 0/0 -p udp -j REJECT
```

Rule Set B:

```
ipchains -A input -i eth1 -s 10.10.10.23 -d 0/0 -j ACCEPT
ipchains -A input -i eth1 -s 10.10.15.0/24 -d 0/0 -j ACCEPT
ipchains -A input -i eth1 -s 10.0.0.0/8 80 -d 0/0 -p tcp -y -j ACCEPT
ipchains -A input -i eth1 -s 0/0 -d 0/0 -j REJECT
```

Rule Set C:

```
ipchains -A output -i eth1 -s 10.0.0.0 -d 0/0 -p tcp -j ACCEPT
ipchains -A output -i eth1 -p tcp -j REJECT
```

Answer the following questions:

- i. If a machine uses rule set A: (a) What kind of traffic can originate from this machine (i.e. ping, telnet, http.. etc)? (b) What kind of traffic can flow into this machine?
- ii. If a machine uses rule sets A and B: (a) What kind of traffic can originate from this machine (i.e. ping, telnet, http... etc)? (b) What kind of traffic can flow into this machine? (c) How many interfaces does this machine have? (d) How many networks is this machine connected to? (e) What kind of traffic can flow through this machine? You must say what direction is it flowing (i.e.network y -i eth1 -i eth0 -i network x and vise versa)
- iii. If a machine uses rule set A, C and B (note: rule set C is before rule set B): (a) What kind of traffic can flow through this machine?You must say what direction is it flowing (i.e. network y -i eth1-i eth0 -i network x and vise versa) b. Put yourself in an administrators seat and figure out why a whole bunch of users having 10.x.y.z IPs are having problems communicating with the other side of the firewall? Is there total blockade or partial blockade? Explain the problem in detail. (Hint: 10.x.y.z is in eth1 side the other side, eth0 is connected to the Internet. A total blockade means nothing can pass through, a partial blockade means one way communication)

- (b) Consider the following snort rules:

```
alert tcp any any -> 10.0.0.0/24 21 (msg:"EXPLOIT "; flags:A+;
flow:to_server; content: "SITE EXEC |25 30 32 30 64 7C 25 2E 66 25
2E 66 7C 0A|"; depth: 32; nocase; reference:cve,CVE-2000-0573;
reference:bugtraq,1387; reference:arachnids,453;
classtype:attempted-user; sid:338; rev:3;)
```

```
alert tcp any any -> 10.0.0.0/24 80 (msg:"Problem " ; dsize < 256)
```

- i. What would snort look for if a machine use only the above rules?
- ii. Now the your snort administrator complaints to you that there are a lot of alerts and he's unable to analyze them, due to its volume? Do you see any problem in the above rules?

2. Cryptography

- (a) With the aid of a diagram explain how the CBC and CFB modes of DES work?
- (b) Suppose you wanted to send to a friend an encrypted message containing a secret which the CIA, KGB, NSA, etc. would love to possess and they already suspect that you may have it!! Your friend lives far away and it is impossible for you to meet her in person. But you both have telephone and internet access. List the steps you would take to ensure that the message you send is as unreadable as the encryption guarantees. Give reasons for each of the steps. BE PARANOID. DO NOT ASSUME ANYTHING IS SAFE WITHOUT GOOD REASON.

3. VPN's and Remote Access

- (a) Because of the known risks of the UNIX password system, Sun OS 4.0 documentation recommends that the password file be removed and replaced with a publicly readable file called `/etc/publickey`. An entry in the file for user A consists of the user's identifier ID_A , the users public key KU_A , and the corresponding private key KR_A . This private key is encrypted using DES with a key derived from the user's login password P_A . When A logs in the system decrypts this encrypted private key to get KR_A . Explain how will the system verify that P_A was correctly supplied. Also, describe how an opponent can attack this system.
- (b) It is said that that longer key lengths would not help in fixing the problems of MS CHAP v1. Explain in detail why longer key lengths would not affect the complexity of a brute-force attack by a cryptanalyst.

4. IPSEC and SSL

- (a)
- (b) With reference to IPSEC answer the following:
 - i. How does ISAKMP/Oakley provide defense against denial of service attacks? Explain.
 - ii. One more.

- (c) Consider the following threats to Web security and describe how each is countered by a specific feature of SSL:
- Brute-force cryptanalytic attack.
 - Known-plaintext dictionary attack.
 - Replay attack.
 - Man-in-the-middle attack.
 - IP Spoofing.

5. Wireless Security and Anonymity

- (a) To address the weaknesses discovered in WEP it could be suggested that the key length be increased to 128 bits. Explain why increasing the key length would not help against some of the attacks that have been discovered. Clearly explain the attacks and explain why the increased key length would not help.
- (b) Either explain Onion routing or ATTACH YOUR CHEAT SHEETS TO YOUR ANSWER BOOK.