Student Name:

Network Security
Midterm Examination 2

GENERAL INSTRUCTIONS

The midterm is out of a total of 200 points (with the possibility of scoring a 210 including the 10 extra credit points): 50 points of True/False and 150 points of short answer. You have one hour and 15 minutes for the entire exam plan accordingly. The questions are in no particular order of difficulty. Move on to easier ones if you find yourself stuck. You may answer questions in any order as long as they are clearly labeled. This exam is to be completed individually and is closed device, book and notes.

True False questions (50 points + 10 points extra credit)

Circle only one of the choices (10 points each).

1. **True** **False** Kerberos authentication protocol requires clock synchronization for the client to authenticate with the server.

2. **True** **False** Secure BGP would protect against some control plane routing attacks.

3. **True** **False** IPSec in Authentication Header (AH) mode provides confidentiality of IP packets.

4. **True** **False** SSL/TLS uses X509 certificates to provide replay attack protection.

5. **True** **False** DNSSEC provides integrity of domain name to IP resolutions.

6. **True** **False** An anomaly based IDS can detect previously unknown attacks

Short Answer (150 points)

1) **Authentication (50 points)**

a) What is the current Certificate Authority (CA) trust model for HTTPS in terms of the domain names that CAs included in the browser can validly sign certificates for? (15 Points)

Any CA that is trusted by a browser can sign a valid certificate for any domain name.

b) How does this Certificate Authority (CA) trust model differ from DNSSEC in terms of the scope of domain names that registrars can validly sign? (20 points)

For DNSSEC the '.' root CAs can sign valid domain name resolutions for any domain, but CAs lower down in the DNS hierarchy can only sign valid resolutions for domain names below them in the DNS naming hierarchy. This limits their scope of trust unlike HTTPS.

c) What is two-factor authentication and what are the advantages of using this in place of password authentication? (15 Points)

Two-factor authentication requires a user to validate his identity using two different form of authentication: Something you have, Something you know, Somewhere you are, or Something you are(biometrics). If a user is required to produce a password and an RFID tag then an attacker will need to know his password and have access to or be able to clone the tag. Two-factor authentication prevents an attacker from successfully authenticating unless they can compromise both types of authentication. Password authentications should be paired with another factor because they are susceptible to eavesdropping, insecure storage, and possibility of a successful guess.

2) Firewall (50 points)

Louis Reasoner has just discovered a new firewall program called Ipchairs, but he is so excited about Ipchairs' simple rule format that he neglects to read the entire manual. He installs the following rules on his firewall:

No	Action	Prot.	Source	Destination	Source port	Destination port
1	ACCEPT	TCP	0.0.0.0/0	129.174.1.10/32	*	22
2	ACCEPT	TCP	0.0.0.0/0	129.174.1.10/32	*	80
3	ACCEPT	ALL	0.0.0.0/0	129.174.1.10/32	*	53
4	DENY	ALL	*	192.0.0.1	*	1:2000
5	ALLOW	ALL	*	192.0.0.1	*	*

Louis' machine is 129.174.1.10. He wants ssh (TCP 22), web (TCP 80), and DNS (TCP/UDP 53) services running on his machine to be accessible to everybody, all other ports below 2000 blocked, and he doesn't care about ports above 2000. Later that day, Louis notices incoming traffic to port 135 is not being blocked.

(a) What was Louis' mistake? Show how he can fix his rules. (30 Points)

Louis set to destination to 192.0.0.1 instead of 129.174.1.10, change these two rules to fix it.

4 DENY ALL * 129.174.1.10 * 1:2000

5 ALLOW ALL * 129.174.1.10 * *

(b) How should Louis modify his rules if he installs a print daemon that only listens on port 7701? The print daemon should only be accessible to others on his local network, 129.174.1.0/24, and to his friend Max, whose computer is at 128.59.15.63. (20 Points)

1 ACCEPT TCP 0.0.0.0/0 129.174.1.10/32 * 22
2 ACCEPT TCP 0.0.0.0/0 129.174.1.10/32 * 80
3 ACCEPT ALL 0.0.0.0/0 129.174.1.10/32 * 53
4 ACCEPT TCP 129.174.1.0/24 129.174.1.10 * 7701
5 ACCEPT TCP 128.59.15.63 129.174.1.10 * 7701
6 DENY ALL * 129.174.1.10 * 1:2000
7 ALLOW ALL * 129.174.1.10 * *

3) **IDS (50 points)**

a) Wolf Security released an intrusion detection system that can detect Syn floods and SQL injection attacks. The boast a low false positive rate and high accuracy rate, rates are in the following table:

	How connection is classified		
Type of connection	Syn flood	SQL Injection	Normal
Syn flood	85%	5%	10%
SQL Injection	5%	90%	5%
Normal	5%	5%	90%

For example, when the IDS observes a Syn flood, it correctly classifies it as a Syn flood with probability 85%, misclassifies it as an SQL Injection attack with probability 5%, and misclassifies it as a normal connection with probability 10%.

For the purposes of this problem, assume that Syn floods are 3% of all connections, and that SQL Injection attacks are 1% of all connections, while 96% of traffic consists of normal connections.

Also assume that a connection cannot be both a Syn flood and an SQL injection attack at the same time.

When the IDS announces that it detected a Syn flood, what is the probability that the connection is, in fact, normal? Give your calculations. (40 points)

P(normal | Syn flood) = (P(Syn flood | normal) * P(normal)) / P(Syn flood) =

(P(Syn flood | normal) * P(normal))/ (P(Syn flood | normal) * P(normal) + P(Syn flood | SYN flood) * P(SYN flood) + P(Syn flood | SQL Injection) * P(SQL Injection))

(.05 * .96) / (.05 * .96 + .85 * .03 + .05 * .01) = .6486 =

65% chance that the traffic is normal.

b) Explain how an anomaly based IDS functions and what trade-off is makes in terms of false positive rates and detection of unknown attacks compared to a signature-based IDS. (10 points)

Any anomaly-based IDS uses a supervised statistical model based on network traffic features to determine what is normal and what is anomalous. This tends to result in higher false positive rates compared to signature-based IDSs. It also enables anomaly-based IDSs to detect previously unknown attacks that a signature-based IDS can't detect.