[redacted] Exam 2 Athinav Fall 2013

NAME: Vivek Sribalusu (421901480) **SCORE:** 100

1. (10 pts) Which do you think is a greater security threat in the web, Server side executables or client side executables and why?

I think that Server Side executables possess a greater threat when compared with client side executables as the attacks like hijacking sessions and phishing can impact a lot of clients which use the server whereas an attack like a downloadable javascript file into the client system may steal the data from the client in which only the client system is affected.

2. (10 pts) What is the primary security vulnerability of each of the following and how can it be mitigated:

A. FTP

The FTP protocol uses unencrypted and unauthenticated TCP connection, eavesdrop to catch passwords or other sensitive information is possible. It is also possible to hijack connections. This can be addressed by applying software quality measures by maintaining consistency between server settings and wanted security level.

B. Telnet

Telnet allows incoming connections that does not have the ability to encrypt data. This can be then used to spoof or exploit valid protocols. A vigilant SysAdmin could comb the logs and subsequently disallow connections from sites or domains that no one should be connecting from.

C. rlogin

The primary vulnerability of rlogin is that if an /etc/hosts.equiv file exists on the system or the user has a .rhosts file, then no password is needed for the user. This can be mitigated by wrapping all of our r- commands started in /etc/inetd.conf with a wrapper and discourage the use .rhosts, maybe even setting up a script to prune .rhosts files from the system on an hourly basis.

3. (10 pts) Which category of the taxonomy does PGP mitigate that is not mitigated by just encrypting the SMTP traffic between MTAs?

PGP can be used to mitigate Authentication based which is not mitigated by just encrypting the SMTP traffic between MTAs. PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

4. (10 pts) What type of information about the browser or browser's computer is provided to a web server by the browser using the HTTP protocol?

HTTP protocol can send cookies to the server from the browser along the information of the user's previous activity on that website.

a. What security problems can this cause?

- Abuse of Server for Information
- Transfer of Sensitive Information

b. How could you stop a server from getting your information?

We can stop a server from getting our information by encoding sensitive information in URL's. Clients should not include a Referer header file in a non secure HTTP request if the referring page was transferred with a secure protocol. Authors of services which use HTTP protocol should not use GET based forms for submission of sensitive data.

5. (20 pts) Describe what each network mitigation device is used for and which categories of the taxonomy they can mitigate

A. Firewall

- Firewall is a software or hardware based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining they should be allowed or not. It eliminates traffic based attacks.

B. IDS

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious or policy violations and produces reports to a management station. It can mitigate authentication based attacks.

C. Web filter

Web filter monitors HTTP traffic on your network to monitor user behaviour and block inappropriate content. It can mitigate traffic (authentication based attacks.

D. Email virus filter

Email virus filter scans the emails for any virus which may be present in them and filters it accordingly. It helps in mitigating viruses which can use any type of taxonomy for its attack.

6. (20 pts) Describe how to defeat the following email security mechanisms

a. White listing

It can be defeated with techniques like Sniffing on the traffic between the network. IP address can be obtained. This can be used to send spam emails.

b. Grey listing

Grey listing can be defeated by sending messages multiple times such that it recognizes the server and does not mark it as spam.

c. Spam filter

By using images and text that does not look like spam messages.

d. Black listing

It can be defeated by spoofing address to non-blacklisted addresses.

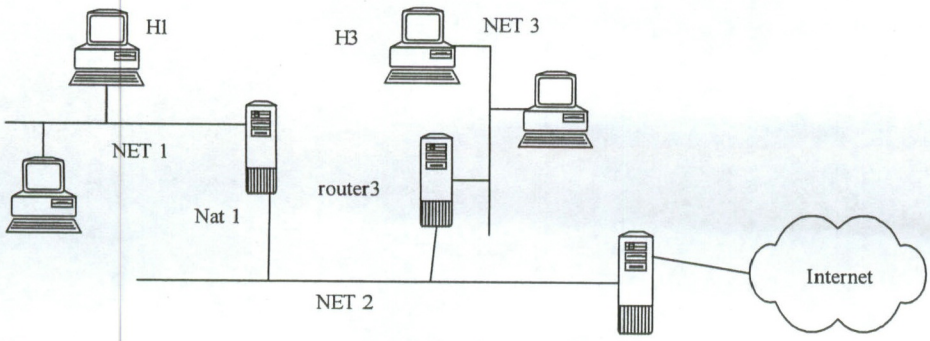
e. PGP

- It can be defeated by hijacking the network during the key registration phase. However, it is very difficult.

7. (5 pts) Comment on the course and the text book

The course and the textbook act as a great introduction for the course - network security with all the basic types of attacks and security mechanisms used for countering these attacks in a generic sense. Although, I feel that giving more real life examples for various attacks will help in understanding the importance of network security.

8. (15 pts) Using the figure below answer the following questions



Assume the following addresses:

H1 192.168.1.15
H3 129.186.10.5
Router 3 129.186.4.253 (for NET 2)
Router 3 129.186.10.254 (the NET 3)
Nat 1 192.168.1.254 (for the NET 1)
Nat 1 129.186.4.1 (for the NET 2)
Router 1 129.186.4.254 (for the NET 2)
Router 1 10.0.0.5 (for the internet side)

Assume the NAT is a dynamic NAT and that 192.168.1.0/24 is the internal network.

Assume the following request packet is delivered to the IP layer from the TCP layer on host H1 with an intended destination of H3. (Assume the other TCP header values are correct)

TCP source port = 7466
TCP destination port = 80
500 bytes of data

Assume all ARP and DNS tables are current.
For each of the points in the network listed below show the values for the following fields in the packets. (Assume the initial value of the time to live field is 100 when the packet is sent by either host H1 or H3) (If the value for a field is not specified you can assume a value) Show the fields in the reply packet at each of the points in the network.

	Request			Reply		
	Net 1	Net 2	Net 3	Net 1	Net 2	Net 3
TCP Layer:						
Source port	7466	NAT	NAT	80	80	80
Dest port	80	80	80	7466	NAT	NAT
IP Layer:						
TTL	99	98	97	99	98	97
SRC IP addr	H1	129.186.4.[illegible]	129.186.4.[illegible]	H3	H3	H3
Dest IP addr	H3	H3	H3	[illegible] H1	129.186.4.[illegible]	129.186.4.[illegible]