Part1 ---- For each pcap, discuss what kind of traffic communication is going on and anything you learned about the communication.

(1) lab3-1.pcap:

UserA (gurpartap@patriots.in) is sending emails to

UserB(raj_deol2002in@yahoo.co.in), he wants to send smtp pcap files to user B.

Totally, he sends a lot of versions, from 4.9.5.1 to 4.9.9.1, which the later ones have updated many bugs from the previous ones.

We could also infer that password of User A is: punjab@123, the protocols here mainly are TCP, SMTP etc.

(2) lab3-2.pcap:

User(fake) login on OpenBSD/i386 (oof) (ttyp2)<unix-like operating system>, his password is: user. He pings to www.yahoo.com. All of his 6 packets have been received. He lists all his files (. .. .cshrc .login .mailrc .profile .rhosts) in /sbin and exit OpenBSD/i386 (oof) (ttyp2).The protocols here mainly are TCP, TELENT etc.

(3) lab3-3.pcap:

X11 is the certain type of protocol that requests a remote control to its client. All X11 protocol is SSH security encrypted. So we are not able to find any information of this part if we don't use any specific tool to dig it out. User A(131.151.32.129) is sending remote control request to client B(131.151.32.21), and successfully get the control permission of client B after several communication requests.The protocols here mainly are X11,IPX,TCP etc.

(4) lab3-4.pcap:

UserA(192.168.1.3) use ARP to get the control of UserB(192.168.1.1), eventually he gets UserC(192.168.1.2) control permission. Then he uses "dir" to display all the files in "C://" and use "ls –la", which is not recognized by that operating system.He exits and then goes to http://www.goals365.com, try to download the /images/empty.gif from http://www.goals365.com/feed/soccer/, which is a soccer

website for watching and betting for the soccer. The protocols here mainly are ARP,DNS,TCP etc.

Part3 ---- Domain Analysis

(1) What kind of information does dig return and what was different about facebook.com--profile---notifybpdblfpbccfj.e-ticket.pt?

First, dig will return target domain name, global options, QUERY status & id, AUTHORITY SECTION, ADDITIONAL SECTION, Query time, SERVER, MSG SIZE etc. Google.com and Gmail.com both have similar number of authorities (4), plus the additional ones (9) and dig time message size is around 300.Also, their servers are similar as well since they are from the same company.

Facebook.com will return number of authorities (2), plus the additional ones (5) and dig time message size is around 180.

While, the facebook.com--profile---notifybpdblfpbccfj.e-ticket.pt are authorities (2), plus the additional ones (3) and dig message size is around 185.

(2) Can you think of any reason why someone would set up DNS records like that?

We can use the dig command to perform a reverse DNS lookup, that is we can query an IP address and find the domain name that it points to by querying the PTR record.

From facebook.com--profile---notifybpdblfpbccfj.e-ticket.pt, we have:

ANSWER SECTION:

facebook.com--profile---notifybpdblfpbccfj.e-ticket.pt. 10 IN A 130.185.81.169

ADDITIONAL SECTION:

ns1.skainteractive.com. 886 IN A 94.46.135.240

ns2.skainteractive.com. 886 IN A 130.185.82.240

First thing might be he login in a fake website that seems to have the facebook.com domain but it's a fake one.

Another thing might be a virtual machine or VPN, DNS return the ip address which with the encryption one which will cause the results not same.

(3) What were you able to discover about our server with nmap?

yuxuanz6@yzcmf:~$ nmap 192.168.200.5

Starting Nmap 7.70 (https://nmap.org) at 2019-02-11 01:26 UTC

Nmap scan report for 192.168.200.5

Host is up (0.00019s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp open ssh

993/tcp open imaps

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

From the picture, we can know that the target host is up and there are 998 ports are closed, and 2 opened ports are 22/tcp(we could use ssh to access), 993/tcp(we could use imaps to access)

Part 4 - Find the Flag

The attack used to obtain the flag was covered in lecture. What was it? What was going on? Are there other ways to perform this attack? If so, how are they different?

ARP address spoofing. Client (192.168.200.62) communicates with Server (192.168.200.5), then we make arpspoof -t 192.168.200.62 192.168.200.5, let client think I'm the server; arpspoof -t 192.168.200.5 192.168.200.62, let server think I'm the client; echo 1 > /proc/sys/net/ipv4/ip_forward, forward all the

packages I've received. tcpdump -XX src 192.168.200.62, print all the data packets from src 192.168.200.62(server). The flag will be in the data packet from the server.

For the spoofing, we could also do IP spoofing. We could make a fake ip address as it is the target ip address in one of our machines. ARP is mainly from the router tables reflections while the ip address fake spoofing is making fake ip address machine.

However, we could also use ssh attack and find the password of the client and server. Since they both use ssh in port23. That will be cool if we know their password.