Port Scanning and TCP

Premise

- Users scan the Windows attack host using NMAP and find that there is a certain port open, they are then urged to poke and prod at this port until they find a way into the exposed service.
  - NIST:

Questions

- What *port* is the exposed network service running on
- What is the *command* used to gain access to this network service
- What is the *name* of the file that holds the encrypted password
- What kind of *password hashing* method was used
- What is the result of the cracked password
- What message is displayed when the buffer is overflowed

FILE

- TcpListenServer (On windows machine)

Recommended tools

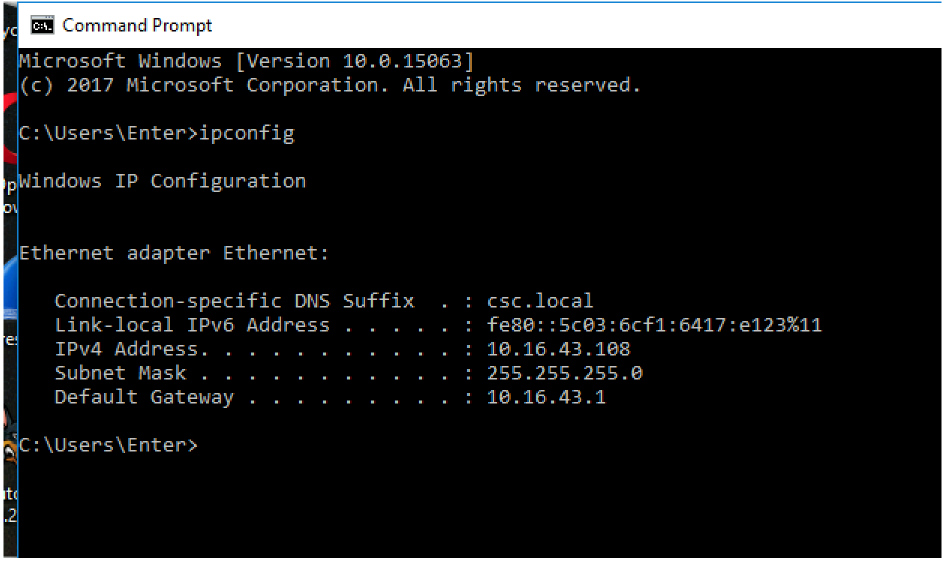
- Nmap
- Netcat

Answers

- What *port* is the exposed network service running on
  - 259
- What is the *command* used to gain access to this network service
  - nc <IP_ADDR> 259 ~or~ netcat <IP_ADDR> 259
- What is the *name* of the file that holds the encrypted password
  - passwd.enc
- What kind of *password hashing* method was used
  - SHA1
- What is the result of the cracked password
  - changeme
- What message is displayed when the buffer is overflowed
  - BUFFER OVERFLOW: 0x135017C

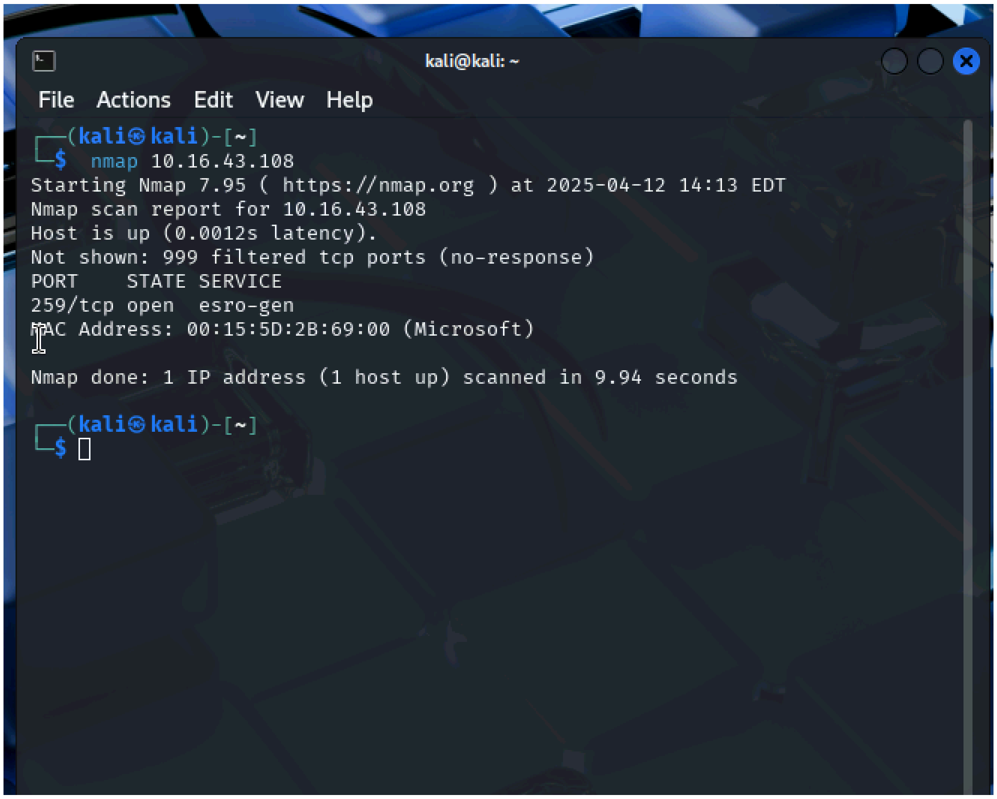
Walkthrough

- Get the IP address of the Windows attack target by opening **cmd** and tying in *ipconfig*

- 

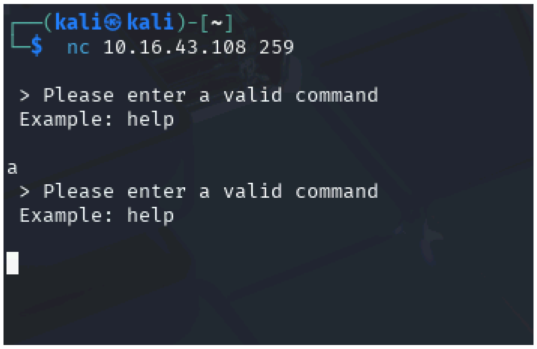
```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Enter>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : csc.local
   Link-local IPv6 Address . . . . . : fe80::5c03:6cf1:6417:e123%11
   IPv4 Address. . . . . . . . . . . : 10.16.43.108
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.16.43.1

C:\Users\Enter>
```

- Load into a **Linux** machine and open a terminal, type *nmap <HOST_WINDOWS_IP*
  - This will scan the first 1000 most often used ports on the target machine, the target process will be running on port **259**



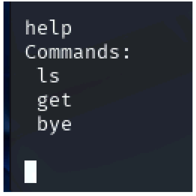
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.16.43.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-12 14:13 EDT
Nmap scan report for 10.16.43.108
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE
259/tcp open  esro-gen
MAC Address: 00:15:5D:2B:69:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 9.94 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- This is the port that will be used for the attack
- In the same terminal type *nc <WINDOWS_IP_ADDR> 259*, this will attach you to the TCP listen server that is running on the attack target

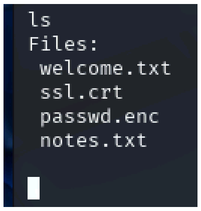


```
┌──(kali㉿kali)-[~]
└─$ nc 10.16.43.108 259

 > Please enter a valid command
 Example: help

a
 > Please enter a valid command
 Example: help

```

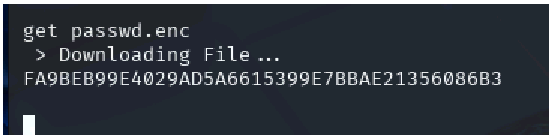
- Type any input to prompt the help dialogue
- Entering *help* will show all available commands on the TCP server, these commands are all that is needed to complete the TCP server segment of the challenge

- 

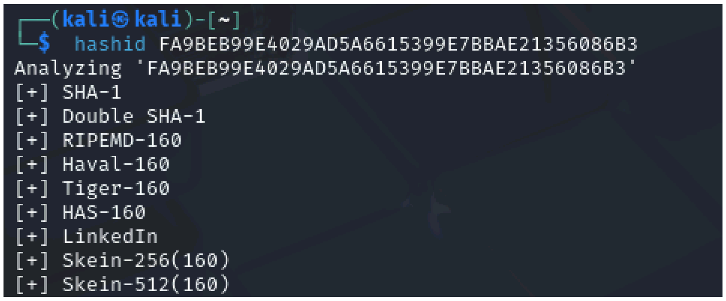
  ```
  help
  Commands:
   ls
   get
   bye
  ```

- Use *ls* on the server to list out all the files
  - 

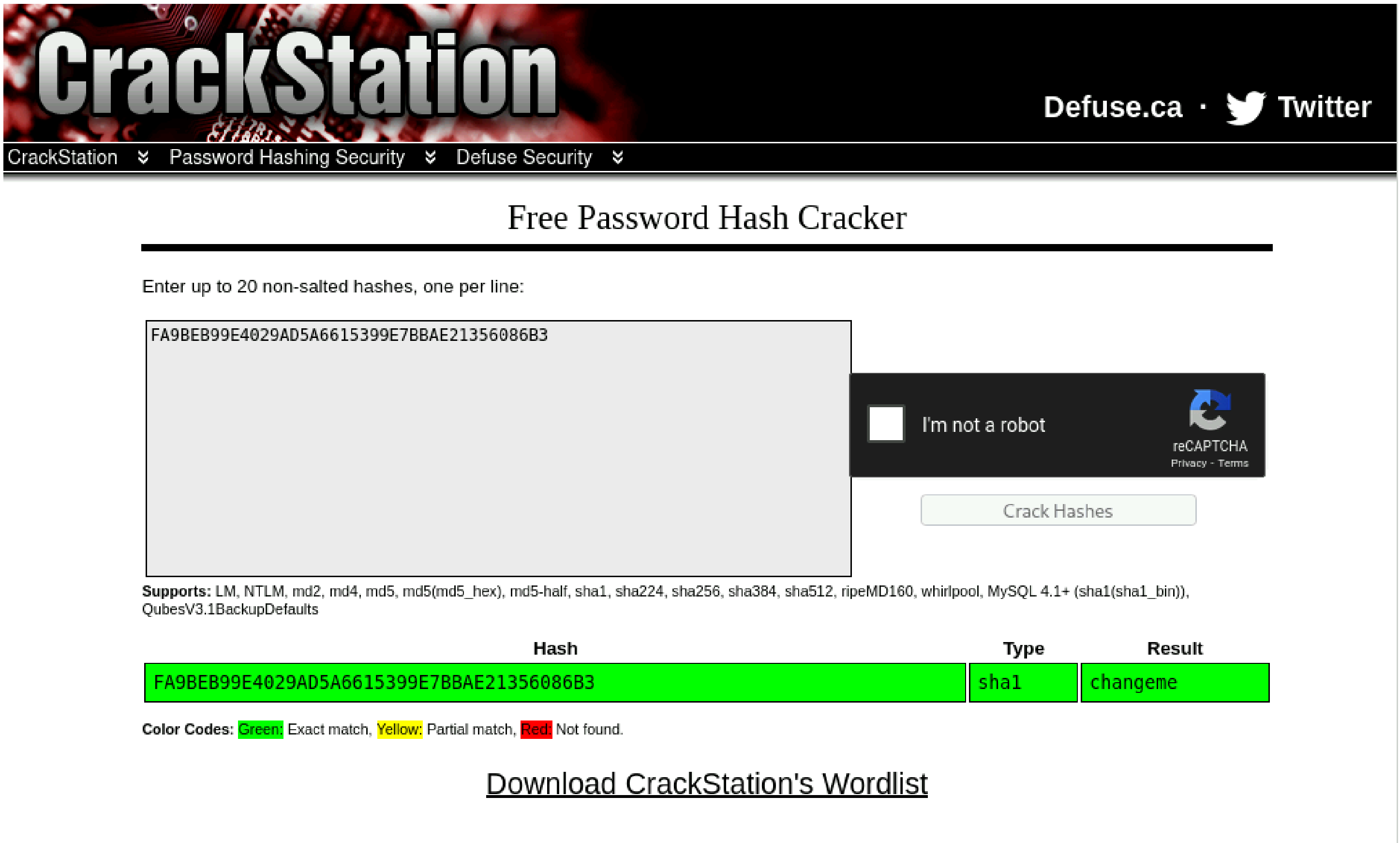
    ```
    ls
    Files:
     welcome.txt
     ssl.crt
     passwd.enc
     notes.txt
    ```

  - Note the file names, especially *passwd.enc*
- Use the *get* command to get the contents of the file on the server
  - *get passwd.enc*
  - 

    ```
    get passwd.enc
     > Downloading File...
    FA9BEB99E4029AD5A6615399E7BBAE21356086B3
    ```

  - This will dump the file contents of the *passwd.enc* file
- Use a utility like *hashid* to get the type of password hash that was used
  - 

    ```
    ┌──(kali㉿kali)-[~]
    └─$ hashid FA9BEB99E4029AD5A6615399E7BBAE21356086B3
    Analyzing 'FA9BEB99E4029AD5A6615399E7BBAE21356086B3'
    [+] SHA-1
    [+] Double SHA-1
    [+] RIPEMD-160
    [+] Haval-160
    [+] Tiger-160
    [+] HAS-160
    [+] LinkedIn
    [+] Skein-256(160)
    [+] Skein-512(160)
    ```

  - SHA-1 is mentioned multiple times, as that is the actual hashing algorithm
- The password can either be cracked with *hashcat* on the VM, or as it is SHA-1 and very weak, websites can be used to look up the hash and see if it has already been solved
  - 

    Free Password Hash Cracker

    Enter up to 20 non-salted hashes, one per line:

    ```
    FA9BEB99E4029AD5A6615399E7BBAE21356086B3
    ```

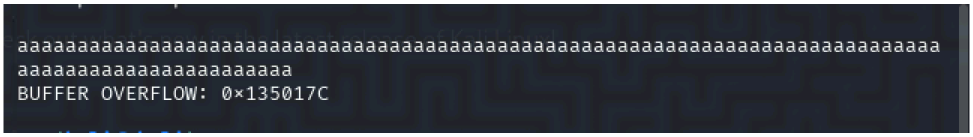
    Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
FA9BEB99E4029AD5A6615399E7BBAE21356086B3	sha1	changeme

    Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

  - Using crackstation, the password is decrypted to *changeme*

- To Trigger a "Buffer Overflow" on the exposed network service, the input buffer needs to be exploited. This means testing a prodding the buffer bu sending in arbitrary amounts of characters, symbols, or other UNICODE/ASCII values.
- In this case the buffer has been preprogrammed to only hold 50 values, any number over 50 will result in a "Buffer Overflow" on the server



```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaa
BUFFER OVERFLOW: 0×135017C
```