
ATTACK
DEFENSE
by PentesterAcademy

Name	SSH Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=526
Type	Network Recon : SSH Servers

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. What is the version of SSH server.

Answer: OpenSSH 7.2p2 Ubuntu 4ubuntu2.6

Command: nmap -sV 192.201.39.3

```
root@attackdefense:~# nmap -sV 192.201.39.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 12:22 UTC
Nmap scan report for ak3il9uxk8nv237myolo6i8a4.temp-network_a-201-39 (192.201.39.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:C9:27:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
root@attackdefense:~#
```

Q2. Fetch the banner using netcat and check the version of SSH server.

Answer: OpenSSH 7.2p2 Ubuntu 4ubuntu2.6

Command: nc 192.201.39.3

```
root@attackdefense:~# nc 192.201.39.3 22
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.6
```

Q3. Fetch pre-login SSH banner.

Answer: Welcome to attack defense ssh recon lab!!

Command: ssh root@192.201.39.3

```
root@attackdefense:~# ssh root@192.201.39.3
The authenticity of host '192.201.39.3 (192.201.39.3)' can't be established.
ECDSA key fingerprint is SHA256:dxlBXgBb0Iv5/LmemZ2Eikb5+GLl9CSLf/B854fUeV8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.201.39.3' (ECDSA) to the list of known hosts.
Welcome to attack defense ssh recon lab!!
root@192.201.39.3's password:
```

Q4. How many “encryption_algorithms” are supported by the SSH server.

Answer: 6

Command: nmap --script ssh2-enum-algos 192.201.39.3

```
root@attackdefense:~# nmap --script ssh2-enum-algos 192.201.39.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 12:29 UTC
Nmap scan report for ak3il9uxk8nv237myolo6i8a4.temp-network_a-201-39 (192.201.39.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (6)
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       ssh-rsa
|       rsa-sha2-512
|       rsa-sha2-256
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
```

Q5. What is the ssh-rsa host key being used by the SSH server.

Answer:

AAAAB3NzaC1yc2EAAAADAQABAAABAQC1fkJK7F8yxf3vewEcLYHljBnKTAiRqzFxkFo6lqyew73ATL2Abyh6at/oOmBSlPI90rtAMA6jQGJ+0HlHgf7mkjz5+CBo9j2VPu1bejYtcxpqpHcL5Bp12wgey1zup74fgd+yOzILjtgbnDOw1+HSkXqN79d+4BnK0QF6T9YnkHvBhZyjzIDmjonDy92yVBAIoB6Rdp0w7nzFz3aN9gzB5MW/nSmgc4qp7R6xtzGaqZKp1H3W3McZO3RELjGzvHOdRkAKL7n2kyVAraSUrR0Oo5m5e/sXrITYi9y0X6p2PTUfYiYvgkv/3xUF+5YDDA33AJvv8BblnRcRRZ74BxaD

Command: nmap --script ssh-hostkey --script-args ssh_hostkey=full 192.201.39.3

```
root@attackdefense:~# nmap --script ssh-hostkey --script-args ssh_hostkey=full 192.201.39.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 12:31 UTC
Nmap scan report for ak3il9uxk8nv237myolo6i8a4.temp-network_a-201-39 (192.201.39.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC1fkJK7F8yxf3vewEcLYHljBnKTAiRqzFxkFo6lqyew73ATL2Abyh6at/oOmBSlPI90rtAMA6jQGJ+0HlHgf7mkjz5+
CBo9j2VPu1bejYtcxpqpHcL5Bp12wgey1zup74fgd+yOzILjtgbnDOw1+HSkXqN79d+4BnK0QF6T9YnkHvBhZyjzIDmjonDy92yVBAIoB6Rdp0w7nzFz3aN9gzB5MW/nSmgc4
qp7R6xtzGaqZKp1H3W3McZO3RELjGzvHOdRkAKL7n2kyVAraSUrR0Oo5m5e/sXrITYi9y0X6p2PTUfYiYvgkv/3xUF+5YDDA33AJvv8BblnRcRRZ74BxaD
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBB0cJ/kSOXBWVIBA2QH4UB6r7nFL5l7FwHubbSZ9dIs2JSmn/oIgvvQvx
mI5YJxkdxRkQlF01KLDmVgESYXyDT4=
|_  ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAAIKuZlCFfTgeaMC79zla20ZM2q64mjqWhKPw/2UzyQ2W/
MAC Address: 02:42:C0:C9:27:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
root@attackdefense:~#
```

Q6. Which authentication method is being used by the SSH server for user “student”.

Answer: none_auth

Command: nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" 192.201.39.3

```
root@attackdefense:~# nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" 192.201.39.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 12:37 UTC
Nmap scan report for ak3il9uxk8nv237myolo6i8a4.temp-network_a-201-39 (192.201.39.3)
Host is up (0.000064s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|_  Supported authentication methods: none_auth
MAC Address: 02:42:C0:C9:27:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
root@attackdefense:~#
```

Q7. Which authentication method is being used by the SSH server for user “admin”.

Answer: publickey, password

Command: nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=admin" 192.201.39.3

```
root@attackdefense:~# nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=admin" 192.201.39.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 12:44 UTC
Nmap scan report for ak3il9uxk8nv237myolo6i8a4.temp-network_a-201-39 (192.201.39.3)
Host is up (0.000059s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: 02:42:C0:C9:27:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
root@attackdefense:~#
```

Q8. Fetch the flag from /home/student/FLAG by using nmap ssh-run script.

Answer: e1e3c0c9d409f594afdb18fe9ce0ffec

Command: nmap -p 22 --script=ssh-run --script-args="ssh-run.cmd=cat /home/student/FLAG, ssh-run.username=student,ssh-run.password=" 192.201.39.3

```
root@attackdefense:~# nmap -p 22 --script=ssh-run --script-args="ssh-run.cmd=cat /home/student/FLAG, ssh-run.username=student,ssh-run
.password=" 192.201.39.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 12:45 UTC
NSE: [ssh-run] Authenticated
NSE: [ssh-run] Running command: cat /home/student/FLAG
NSE: [ssh-run] Output of command: e1e3c0c9d409f594afdb18fe9ce0ffec

Nmap scan report for ak3il9uxk8nv237myolo6i8a4.temp-network_a-201-39 (192.201.39.3)
Host is up (0.000057s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-run:
|   output:
|_    e1e3c0c9d409f594afdb18fe9ce0ffec\x0D
MAC Address: 02:42:C0:C9:27:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
root@attackdefense:~#
```

References:

1. OpenSSH Server (https://www.openssh.com/)
2. Nmap Script: ssh2-enum-algos (https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html)
3. Nmap Script: ssh-hostkey (https://nmap.org/nsedoc/scripts/ssh-hostkey)
4. Nmap Script: ssh-auth-methods (https://nmap.org/nsedoc/scripts/ssh-auth-methods.html)
5. Nmap Script: ssh-run (https://nmap.org/nsedoc/scripts/ssh-run.html)