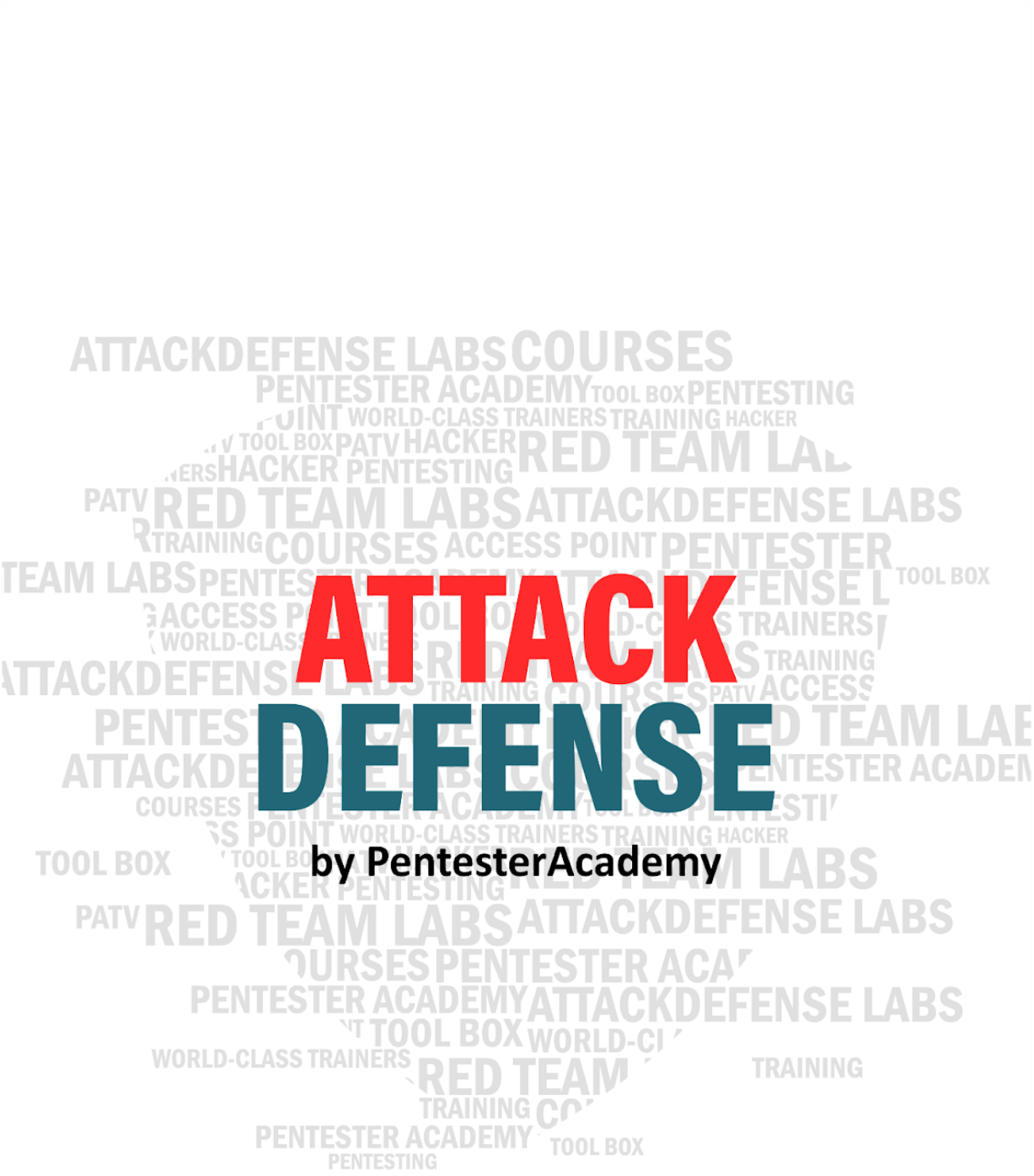
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows Recon: Nmap Host Discovery
URL	https://attackdefense.com/challengedetails?cid=2219
Type	Windows Reconnaissance: SMB

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.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the "**target**" file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.30.43
root@attackdefense:~#
```

Step 2: Ping the target machine to see if it's alive or not.

Command: ping -c 5 10.0.30.43

```
root@attackdefense:~# ping -c 5 10.0.30.43
PING 10.0.30.43 (10.0.30.43) 56(84) bytes of data.

--- 10.0.30.43 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4077ms

root@attackdefense:~#
```

We can observe that the target is not responding to the ping requests, so this does not confirm if it's alive or down.

Step 3: Run a Nmap scan against the target IP.

Command: nmap 10.0.30.43

```
root@attackdefense:~# nmap 10.0.30.43
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-26 17:38 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds
root@attackdefense:~#
```

Nmap also could not detect the host, it's up or not. Many security tools first ping the host before it starts scanning or exploiting the target. In that case, one has to use advanced Nmap options i.e -A or -T5, etc. in order to get the correct output.

In the nmap there is one option i.e **-Pn** (Treat all hosts as online -- skip host discovery) this option will force the scanning even if it has detected the target as down in host discovery.

Step 4: Running Nmap using the -Pn option to discover all alive ports.

Command: nmap -Pn 10.0.30.43

```
root@attackdefense:~# nmap -Pn 10.0.30.43
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-26 17:43 IST
Nmap scan report for ip-10-0-30-43.ap-southeast-1.compute.internal (10.0.30.43)
Host is up (0.0014s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
49155/tcp open  unknown
49163/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
root@attackdefense:~#
```

We will scan any random port which isn't open. In this case scan port 443. If the port is not open we would receive "filtered" as an output to that port.

Command: nmap -Pn -p 443 10.0.30.43

```
root@attackdefense:~# nmap -Pn -p 443 10.0.30.43
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-26 17:44 IST
Nmap scan report for ip-10-0-30-43.ap-southeast-1.compute.internal (10.0.30.43)
Host is up.

PORT    STATE    SERVICE
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
root@attackdefense:~#
```

We can observe, in the Nmap output that the host is up but port 443 is filtered.

About Filtered port:

“Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.”

Source: https://nmap.org/book/man-port-scanning-basics.html

Step 5: Similarly, if we want to discover the running application on port 80 we could use option -sV and this option is used to determine the application version information.

Command: nmap -Pn -sV -p 80 10.0.30.43

The above command skipped the host discovery and forced version information discovery to port 80 only.

```
root@attackdefense:~# nmap -Pn -sV -p 80 10.0.30.43
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-26 17:51 IST
Nmap scan report for ip-10-0-30-43.ap-southeast-1.compute.internal (10.0.30.43)
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.40 seconds
root@attackdefense:~#
```

This is one of the ways where we can discover a machine that is behind a firewall and forcing tools for scanning.

Note: This is a standard method to discover hosts using Nmap which is behind a firewall.

There are plenty of tools that do the same thing.

The target is running Windows Server 2012 and running a Windows Firewall.

References:

1. Nmap (https://nmap.org/)