NET – 332

NETWORK SECURITY LAB

Lab 9. Operating Systems Finger printing & Scanning

OS Fingerprinting

- Process of determining the Operating System used by a host on a network.
  - Forensics Wiki
- What are the contents of an OS Fingerprint?
  - Just like human fingerprints have unique characteristics, OS fingerprints are unique too.
  - These characteristics are reflecting during communication.
  - By capturing and analyzing certain protocol flags and data packets, we can accurately establish the identity of the OS that relayed it.

How is it different than Scanning?

- Scanning is done against IP addresses of computers only such as mail servers, web servers or standalone PC’s.
- OS fingerprinting can be don all network based devices such as Routers, switches, printers, etc.,

Points to ponder about nMap

- nMap is a very noisy solution
- Raises a lot of alerts in IDS/IPS solutions while scanning.
- The trick is to use nMap with different switches smartly so that the scans remain less frequent yet result effective.
  - Usage of switches

Hands On – Lab Activity

- Download and install the nMap Utility from the Vdrive folder – Lab 9

Target

- To keep the scanning legal and ethical we will use the following url to scan.
- The url is provided freely by nMap to be scanned and exploited for practice purposes:
  - http://scanme.nmap.org

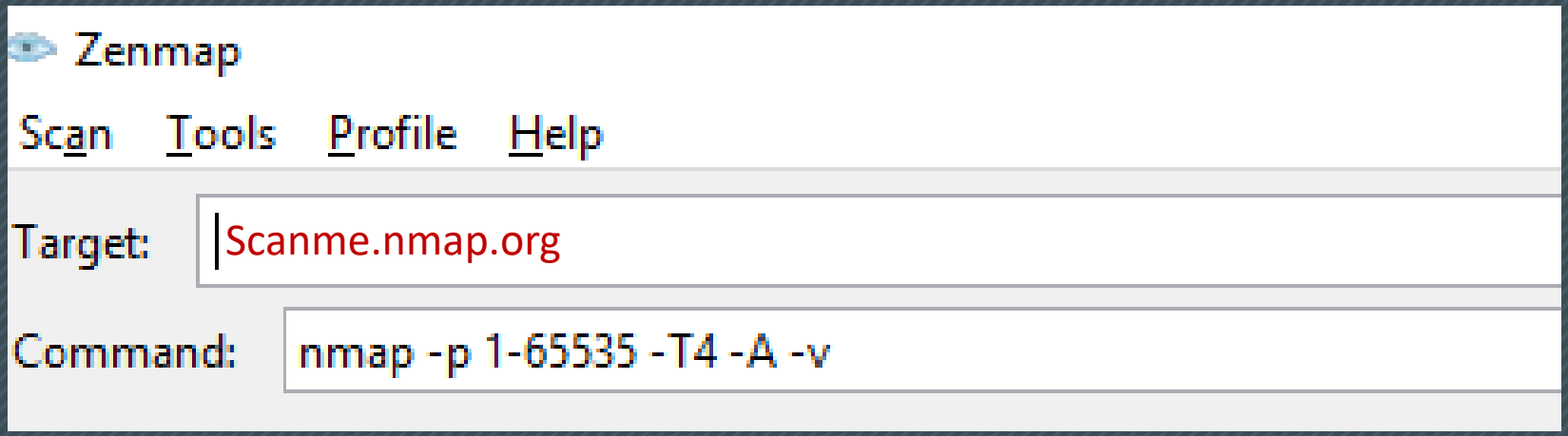
Switches to be used in nMap

- -v : returns the version number of the service you are hosting
- -a : Enables OS detection, version detection, script scanning
- -V 192.168.100.1/16 : passing a range of ip addresses to scan

- Using the nMap GUI run a scan against scanme.nmap.org

Objective

- To intense scan a network (system / server / router)
- Run the nMap utility in GUI Mode



Scanning through nMap

- nMap returns with results

```
Not shown: 991 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (EdDSA)
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 156515DA3C0F7DC6B2493BD5CE43F795
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
81/tcp    filtered hosts2-ns
85/tcp    filtered mit-ml-dev
119/tcp   filtered nntp
1025/tcp  filtered NFS-or-IIS
1080/tcp  filtered socks
9200/tcp  filtered wap-wsp
31337/tcp open     tcpwrapped
```

Scanning a target for specific ports

- Nmap –p <<port number>> 22 <<ssh port>> – target
- nMap –p 22 scanme.nmap.org

Aggressive Scanning using nMap

- nMap –A <<aggressive>> target
  - nMap –A scanme.nmap.org

  Gives the Operating System version of the target.

- nMap –F target
  - Fast scanning (100 ports) of the target

- nMap –open target
  - Runs a fast probe on target and retrieves only open ports on the target.

Report Work:

- Using nMap commands and switches provide the result for the following information:
  - Scan http://www.altoromutual.com using nMap to identify:
    - The version of the Operating System
    - The Services Running on the target
    - Search for ports 8080, 22 and 443 on the target
    - Use a fast scan on the target
    - Retrieve only the open ports on the target
- Provide the answers in the following format:

Command with switch
Result

Questions