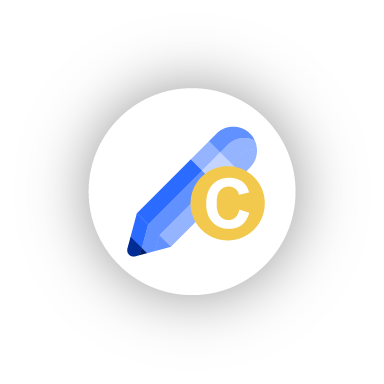
Otis Smith

**Footprinting (Core)**

**Learning Objectives:**

* Apply Nmap and RustScan in footprinting.

In this lab, you will perform the following tasks needed for any Pentest. The target machine is your metasploitable3 Linux machine:

1. Open Kali Linux.

Logged into **kali**, opened a new terminal.

Kali Machine

A screenshot of a computer

Description automatically generated

Did the command “**ifconfig**” to locate the IP address on this kali machine.

A screenshot of a computer

Description automatically generated

Powered up the Metasploitable3 Linux machine targeted machine.

Metasploitable Linux machine A screenshot of a computer

Description automatically generated

1. Scan all ports of your Metasploitable Linux machine.

Did the command “**nmap 10.0.2.1-254**” and found the Metasploitable Linux machine ip address of “10.0.2.15”.

A screenshot of a computer

Description automatically generated

1. Find the versions of each service running on ALL open ports using Nmap (use -A switch).

**Nmap scan report for 10.0.2.15**

**Host is up (0.0014s latency).**

**Not shown: 65524 filtered tcp ports (no-response)**

**PORT STATE SERVICE VERSION**

**21/tcp open ftp ProFTPD 1.3.5**

**22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)**

**| ssh-hostkey:**

**| 1024 2b2e1fa454268776122659580dda3b04 (DSA)**

**| 2048 c9ac70eff8de8ba3a344ab3d320a5c6a (RSA)**

**| 256 c049cc187b27a4070d2a0dbb424c3617 (ECDSA)**

**|\_ 256 a076f376f8f0704d09cae110fda9cc0a (ED25519)**

**80/tcp open http Apache httpd 2.4.7 ((Ubuntu))**

**|\_http-server-header: Apache/2.4.7 (Ubuntu)**

**|\_http-title: Index of /**

**| http-ls: Volume /**

**| SIZE TIME FILENAME**

**| - 2020-10-29 19:37 chat/**

**| - 2011-07-27 20:17 drupal/**

**| 1.7K 2020-10-29 19:37 payroll\_app.php**

**| - 2013-04-08 12:06 phpmyadmin/**

**|\_**

**445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)**

**631/tcp open ipp CUPS 1.7**

**|\_http-server-header: CUPS/1.7 IPP/2.1**

**| http-robots.txt: 1 disallowed entry**

**|\_/**

**| http-methods:**

**|\_ Potentially risky methods: PUT**

**|\_http-title: Home - CUPS 1.7.2**

**3000/tcp closed ppp**

**3306/tcp open mysql MySQL (unauthorized)**

**3500/tcp open http WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))**

**| http-robots.txt: 1 disallowed entry**

**|\_/**

**|\_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)**

**|\_http-title: Ruby on Rails: Welcome aboard**

**6697/tcp open irc UnrealIRCd**

**8080/tcp open http Jetty 8.1.7.v20120910**

**|\_http-server-header: Jetty(8.1.7.v20120910)**

**|\_http-title: Error 404 - Not Found**

**8181/tcp closed intermapper**

**Service Info: Hosts: METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel**

**Host script results:**

**| smb2-security-mode:**

**| 311:**

**|\_ Message signing enabled but not required**

**|\_clock-skew: mean: -1s, deviation: 2s, median: -3s**

**| smb2-time:**

**| date: 2023-10-20T22:25:14**

**|\_ start\_date: N/A**

**| smb-os-discovery:**

**| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)**

**| Computer name: metasploitable3-ub1404**

**| NetBIOS computer name: METASPLOITABLE3-UB1404\x00**

**| Domain name: \x00**

**| FQDN: metasploitable3-ub1404**

**|\_ System time: 2023-10-20T22:25:13+00:00**

**| smb-security-mode:**

**| account\_used: guest**

**| authentication\_level: user**

**| challenge\_response: supported**

**|\_ message\_signing: disabled (dangerous, but default)**

**Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .**

**Nmap done: 1 IP address (1 host up) scanned in 153.67 seconds**

A screenshot of a computer program

Description automatically generated A screenshot of a computer

Description automatically generated

1. Perform similar scans using another tool called [RustScan](https://github.com/RustScan/RustScan/releases" \t "_blank) (which is an alternative to NMAP) and report your findings on the usability of this new tool. This is the link “https://github.com/RustScan/RustScan/releases” . Click on the link “**RustScan**” listed above by holding the **ctrl key + click with my mouse** which opened this page. Also used this youtube video link”**<https://www.youtube.com/watch?v=_JozcegJL84&ab_channel=NethaxStark>**” to assist with the installation.

A screenshot of a video game

Description automatically generated

I removed the “releases” from the end to get to this link “https://github.com/RustScan/RustScan/” to get to the installation guide section

A screenshot of a computer

Description automatically generated

Scroll down to locate the installation guide section.

A screenshot of a computer

Description automatically generated

Clicked on the “**Installation Guide**” link which provided this page.

A screenshot of a computer

Description automatically generated

Moved down to the “**Debian / Kali**” section and clicked on this link “<https://github.com/RustScan/RustScan/releases>” A screenshot of a computer

Description automatically generated

After clicking the link, this page displayed. A screenshot of a computer

Description automatically generated

Moved down to the “**Fixing Cargo Lock**” section and then clicked on the arrow next to “Assets” to download the “**rustscan\_2.0.1\_amd64.deb**” A screenshot of a computer

Description automatically generated

The file has been downloaded.

A screenshot of a computer

Description automatically generated

Did the command “**cd Downloads**” and then “**ls**” to locate the “**rustscan\_2\_0\_1\_amd64.deb**” file. In the

(kali㉿kali)-[~/Downloads] directory. A screenshot of a computer

Description automatically generated

Ran this command “**sudo dpkg -i rustscan\_2.0.1\_amd64.deb**” and entered the password “kali” to start the installation.

A screenshot of a computer

Description automatically generated

The installation has been completed. Use the command “ip route” to display the following ip addresses A screenshot of a computer program

Description automatically generated

Ran the command “**rustscan -h**” for help to view the different switch options available. A screenshot of a computer

Description automatically generated

Run the command “**rustscan -a 10.0.2.15 -- -sV -r**” to find the versions of each service running on all open ports. Below is the outcome.

A screenshot of a computer program

Description automatically generated A screenshot of a computer program

Description automatically generated

**Mitigation:**

1. **Nmap Scan:**
   * *Observations:*
     + Identified Metasploitable Linux machine IP address: 10.0.2.15.
     + Detected open ports and services running on each port.
   * *Mitigation:*
     + Regularly update and patch services to fix known vulnerabilities.
     + Implement network segmentation to minimize the impact of potential breaches.
2. **RustScan Installation:**
   * *Observations:*
     + Successfully installed RustScan after following a YouTube tutorial and RustScan's official GitHub page.
   * *Mitigation:*
     + Always download software from official sources to avoid potential security risks.
     + Verify downloaded files using checksums when available.
3. **Nmap Service Versions:**
   * *Observations:*
     + Identified service versions on open ports using Nmap.
   * *Mitigation:*
     + Disable unnecessary services to reduce the attack surface.
     + Regularly audit and update software to mitigate known vulnerabilities.
4. **RustScan Service Versions:**
   * *Observations:*
     + Successfully used RustScan to find service versions on open ports.
   * *Mitigation:*
     + Diversify scanning tools to enhance detection capabilities.
     + Keep scanning tools updated to support the latest protocols and services.
5. **Overall Recommendations:**
   * Regularly conduct vulnerability assessments and penetration tests.
   * Establish a robust patch management process to address known vulnerabilities.
   * Educate users on secure practices and conduct regular security awareness training.
   * Employ network monitoring tools to detect and respond to suspicious activities.
   * Collaborate with IT and security teams to ensure a proactive and comprehensive security posture.

In conclusion, my practical experience in footprinting, combined with a commitment to ongoing learning and adherence to best security practices, positions me as a capable and security-conscious professional. I am eager to contribute my skills to a dynamic Cyber Security role and actively contribute to safeguarding digital assets.