Gus-khawaja-pratical-web-penetration-testing.pdf
Service probing and enumeration In the preceding step, we used the Nmap script to quickly probe each service that we found. In this step, we will take this information to the next step and try to probe aggressively. The Nmap scripts that we will use in the following examples are both very aggressive and time-consuming:

Port TCP 21 – FTP: Nmap script probing: nmap -sV -p 21 -Pn -T5 --host-timeout 15m --script=ftp* -v [IP address]
Credential brute force: hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] ftp://[IP address]

Port TCP 22 – SSH: Nmap script probing: nmap -sV -p 22 -Pn -T5 --host-timeout 15m --script=ssh* -v [IP address]
Credential brute force: hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] ssh://[IP address]

Port TCP 23 – Telnet: Nmap script probing: nmap -sV -p 23 -Pn -T5 --host-timeout 15m --script=telnet* -v [IP address]
Credential brute force: hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] telnet://[IP address]

Port TCP 25 – SMTP: Nmap script probing: nmap -sV -p 25 -Pn -T5 --host-timeout 15m --script=smtp* -v [IP address]
Connect to the server and execute the VRFY command: telnet [IP] 25 Then execute the command once connected: VRFY [user] (e.g. VRFY John)

Port TCP/UDP 53 – DNS: Nmap script probing: nmap -sV -p 53 -Pn -T5 --host-timeout 15m --script=dns* -v [IP address]

Port TCP 80 – HTTP: Nmap script probing: nmap -sV -p 80 -Pn -T5 --host-timeout 200m --script=http* -v [IP address]

Probing using Nikto: nikto -host http://[IP address]
Probing using WhatWeb: whatweb [IP address]
Directory crawling: gobuster -u http://[IP address]-w /usr/share/wordlists/dirb/common.txt -s '200,204,301,302,307,403,500' -e

Port TCP 110 – POP3: Nmap script probing: nmap -sV -p 110 -Pn -T5 --host-timeout 15m --script=pop3* -v [IP address]

Ports UDP ports 137, 138 TCP ports 137, 139 – Netbios & TCP 445 –
Samba (SMB): Nmap script probing: nmap -sV -p 139,445 -Pn -T5 --host-timeout 200m --script=smb* -v [IP address]

Using Enum4Linux to probe SMB: enum4linux -a [IP address]
Using nmblookup to probe SMB: nmblookup -A [IP address]
Netbios probing using nbtscan: nbtscan -r [IP address]
Listing SMB shares: smbclient -L [IP address] -N Connecting to a shared directory: smbclient //[IP address]/[Shared directory]

Port UDP 161 – SNMP: Nmap script probing: nmap -sV -p 161 -Pn -T5 --host-timeout 15m --script=snmp* -v [IP address]
Enumerating the MIB tree: snmpwalk -c public -v1 [IP address]
Probing SNMP using the snmp-check tool: snmp-check -t [IP address]

Port TCP 389 – LDAP: Nmap script probing: nmap -sV -p 389 -Pn -T5 --host-timeout 15m --script=ldap* -v [IP address]

Port TCP 443 – HTTPS/SSL: Nmap script probing: nmap -sV -p 443 -Pn -T5 --host-timeout 15m --script=ssl* -v [IP address]

Port TCP 1433 – Microsoft SQL Server (MSSQL): Nmap script probing: nmap -sV -p 1433 -Pn -T5 --host-timeout 15m --script=ms-sql* -v [IP address]
Brute force for credentials: hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] mssql://[IP address]

Port TCP 3306 – MySQL: Nmap script probing: nmap -sV -p 3306 -Pn -T5 --host-timeout 15m --script=mysql* -v [IP address]
Brute force for credentials: hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] mysql://[IP address]

Port TCP/UDP 3389 – Remote Desktop Protocol (RDP): Nmap script probing: nmap -sV -p 3389 -Pn -T5 --host-timeout 15m --script=rdp* -v [IP address]
Brute force for credentials: hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] rdp://[IP address]