Introduction to ETHICAL HACKING

Topic

TCP Port Scanning using NMAP Tool

Dr. P. RAGHU VAMSI
JIIT University, Noida

Introduction to ETHICAL HACKING

Topic

NMAP Tool for Basic Network Scanning

Dr. P. RAGHU VAMSI
JIIT University, Noida

PRV's EduHub

View video at Dr. P. Raghu Vamsi YouTube Channel
https://www.youtube.com/channel/UC0oJO4o-UeMt5irLm6kxIWA

Basic ports for scanning

- Various applications uses the services that run based on TCP/IP, UDP, DCCP, and SCTP.
- Port numbers used by applications are
  - System Ports (0-1023)
  - User Ports (1024-49151)
  - Dynamic / Private Ports (49152-65535)

Service Name	Port Number
FTP	20, 21
SSH	22
Telnet	23
SMTP	25
DNS	53
DHCP	67, 68
TFTP	69
HTTP	80
POP3	110
NNTP	119
NTP	123
IMAP4	143
LDAP	389
HTTPS	443
IMAPS	993
RADIUS	1812
AIM	5190

Basic scanning with NMAP (Network Mapper Tool)

- **Installing NMAP**
  - Download the NMAP for Windows or Linux from https://nmap.org/download.html
  - NMAP is an in-built tool in Kali Linux
- **Using NMAP with ZENMAP**
  - NMAP is a command based tool
  - ZENMAP is GUI version of NMAP
    - It has three main configurable settings
      - Target: which IP to be scanned
      - Profile: using a scan profile
      - Command: nmap command that runs on the command prompt
- **Understanding the NMAP port states**
  - Open: system/application is actively listening connections
  - Closed: There is no application listening the connection
  - Filtered: Firewall or some hurdle monitoring the connection, NMAP is unable to decide is the port open or closed.
  - Unfiltered: In this, port responds to NMAP but it unable to decide they are open or closed.
  - Open/Filtered: The port is either opened or filtered and NMAP is not able to precisely determine the state.
  - Closed/Filtered: The port is either closed or filtered and NMAP is not able to precisely determine the state.

Conducting basic scanning with NMAP

- **Basic Scan on a Single IP**
  - **nmap -sn <target IP address>**
- **Basic Scan on an Entire Subnet**
  - **nmap -sn <target IP subnet>**
- **Scan Using an Input File**
  - **nmap -sn -iL <file path>**
- **Reason Scan**
  - **nmap --reason <target IP address>**
- **Supported Protocols**
  - **nmap -sO <target IP address>**
- **Firewall Probe**
  - **nmap -sA <target IP address>**
- **Drawing Topology in ZENMAP**
- **Quick TCP Scan**
  - **nmap -T4 -F<target IP address>**
- **UDP Port Scan**
  - **nmap -sU -p 1-1024 <target IP address>**
- **OS Detection**
  - **nmap -O <target IP address>**
- **Intense Scan**
  - **nmap -T4 -A -v <target IP address>**

TCP Scanning with NMAP (1)

- Full Open Scan
  - Completing full three way handshake with target.
  - It is a too noisy scan.
  - It detects all open ports, for open ports ACK will be replied, when closed ports are encountered nmap sends RST packet.
  - Use this scan only if all other scan fails, because this scan will be logged by firewalls and security devices present on target.
  - nmap –sT <target IP or range>
- Half open Scan (or Stealth Scan or SYN Scan)
  - It is less noisy as compared to Full open scan.
  - In this, RST will be sent by nmap if it received SYN-ACK from target.
  - This scan can not be logged by firewalls or other security devices
  - Nmap –sS <target IP or range>

TCP Scanning with NMAP (2)

- **XMAS Tree Scan**
  - In this numerous flags are set.
  - Unrelated combinations of TCP flags will be set.
  - URG, PSH and RST flags set on.
  - Modern OS will drop this kind of packets
  - Windows OS (Windows XP and later) does not have response mechanism to this setting.
  - Nmap –sX –v <target IP or range>
- **FIN Scan**
  - It is more reliable scan than SYN as FIN are less likely to filtered by firewalls.
  - The result will be similar to XMAS scan
  - If FIN received by open port, no response will be received.
  - If FIN received by closed port, the target replies with RST flag.
  - Nmap –sF <target IP or address>

TCP Scanning with NMAP (3)

- NULL Scan
  - In this, attacker sends the packet with no flag set.
  - The response is similar to XMAS and FIN scan.
  - Nmap –sN <target IP or range>
- Idle Scan
  - It is more complex scan as compared to other scan methods.
  - Refer: https://nmap.org/book/idlescan.html
  - Nmap –Pn –n- –sI <Zombine IP> <target IP>
- Evading firewall
  - Nmap –sS –T4 –A –f –v <target IP or range>

OS Fingerprinting

- Active fingerprinting
  - Uses crafted packets
  - Responses are compared to a known databases
  - High chance of detection by firewalls
  - Nmap –O <target IP>
- Passive fingerprinting
  - Uses sniffing technique to capture packets
  - Responses are analyzed
  - Low change of detection by firewalls as no crafted packets are sent.
  - By observing the TTL in the ICMP eco reply via ping.
  - Linux, Google customized Linux, Free BSD – Initial TTL is 64
  - Windows XP, 7, 2008, 10 – initial TTL is 128
  - CISCO routers – initial TTL 256

References

1. Sean-Philip Oriyano, "Certified Ethical Hacker Version 9 - Study Guide", EXAM 312-50, Sybex Wiely,2016.
2. Georgia Weidman, "Penetration testing A Hands-On Introduction to Hacking", No Scratch Press, 2014.
3. Raphaël Hertzog, Jim O'Gorman, and Mati AharoniKali, "Linux Revealed Mastering the Penetration Testing Distribution", OFFSEC Press, 2017
4. Corey P. Schultz, Bob Percianccante, "Kali Linux Cook Book", Second edition, Packet Publishing, 2017.
5. Lee Allen, Tedi Heriyanto, Shakeel Ali, "Kali Linux – Assuring Security by Penetration Testing, Packet Publishing, 2014.
6. James Corley, Kent Backman, and Michael T. Simpson, "Hands-On Ethical Hacking and Network Defense", 2006.
7. Willie L. Pritchett, David De Smet, "Kali Linux Cook book", Packet publishing, 2013.
8. Georgia Weidman, Penetration Testing - A Hands Introduction to hacking, No Starch press, 2014.
9. Jessey Bullock, Jeff T. Parker, Weireshark for security professionals using Wireshark and Metasploit Framework, Wiely, 2015.
10. Dejey, Murugan, "Cyber Forensics", Oxoford University Press, 2018.
11. Online material from https://www.ethicalhackx.com
12. Rahalkar, Sagar, Sagar Rahalkar, and Karkal. Quick Start Guide to Penetration Testing. Apress, 2019.