Chapter 6
Scanning and Enumeration Phase

ABSTRACT

In ethical hacking, the reconnaissance phase is followed by the scanning and enumeration phase where the information collected from reconnaissance phase is used to examine the target or target network further for getting specific details such as computer names, IP addresses, open ports, user accounts, running services, OS details, system architecture, vulnerabilities, etc. This chapter introduces different scanning and enumeration tools used in the scanning phase of the ethical hacking process in detail. One may use scanning and enumeration tools and techniques involving packet crafting tools, packet analyzers, port scanners, network mappers, sweepers, and vulnerability scanners during this phase. The chapter introduces tools like Hping3, NMAP security scanner, Colasoft packet builder to create custom packets, vulnerability scanners such as Nessus, Netbios enumeration technique, Hyena, remote administration of network devices using advanced IP scanner, global network inventory, network mapping using the dude network monitor, banner grabbing using ID serve, SNMP enumeration technique, creating NetBIOS null session to enumerate, etc. The chapter also provides the details of maintaining privacy and anonymity while carrying out such scanning and enumeration attacks.

PACKET CRAFTING (HACKINGARTICLES, 2018)

Packet crafting techniques involve manually generating packets in order to test the network and network devices for their performance. It does not use existing network traffic but creates its own network traffic. These techniques can allow hackers to probe firewall/IDS rule-sets, TCP/IP stack, router and open ports in order to determine entry points into a target system or network (Samineni, Barbhuiya, & Nandi, 2012). These packet generating tools allows to carry out the settings for specific options/flags/changing payload size in the packet. Packet editing tools like Colasoft or Scapy can be used. For analyzing the response packets, tools like Wireshark (GUI based and offers more user friendliness), Tcpcdump (command line based), or Windump (command line based for windows) can be used.

DOI: 10.4018/978-1-5225-7628-0.ch006
Colasoft Packet Builder to Create Custom Packets (COLASOFT, 2018)

Colasoft Packet Builder provides powerful editing features in order to create custom network packets (Ethernet Packet, ARP Packet, IP Packet, TCP Packet and UDP Packet etc.) for testing the network. The decoding editor allows us to edit specific protocol field value/parameters easily. We can save the created packets to files on hard disk. Try to add/insert/send/edit/save packet using colasoft.

First install colasoft packet builder on windows host machine or guest VM. Next select adapter (use ipconfig/all command to get details of the Ethernet adapter) and click on add/create packet tab as shown in Figure 1. Select ARP packet template as shown in Figure 2 with delta time = 0.1 seconds setting. Select view in decode/hex editor. Click send all with burst mode seeing as shown in Figure 3 and click close tab. Now, ARP packet will be broadcasted on network. All active machines in the network will send reply to these ARP packets. To view the response ARP packets, start Wireshark prior to sending ARP packets and capture the response packets in Wireshark with ARP typed in filtering command section for further analysis as shown in Figure 4. You can also save or export the created/captured packets in any file on hard disk.

You can also craft TCP packets with different options, flag (SYN, RST, PSH, URG, ACK, FIN) settings, different source/destination address and send packets. Figure 6 and 7 shows the sample TCP packet with SYN flag set sent over the network and corresponding output observed in the Wireshark respectively.

NMAP SCANNING TECHNIQUES (NMAP, 2018)

Gordon Lyon’s NMAP security scanner can also be used to send specially crafted packets to the target host. The tool also analyzes the responses which can be used to discover hosts and services on a computer network. This helps us building a map of existing computer network. Zenmap is the official Nmap Security Scanner GUI and also supports tasks like host discovery, port scanning, version or OS detection, Scriptable interaction with the target using Nmap Scripting Engine (NSE) and Lua programming language, Auditing the security of a device or firewall etc. Install it from nmap website (Sun-young, Shin, Yeol, & Byeong-hee, 2016, & Mandal, & Jadhav, 2016). Figure 7 shows the interface of Zenmap, where, we can select target and scan or type the command with required/available scanning options in the command window.

For e.g. type: nmap -T4 -O -v scanme.nmap.org

Where,

-O refers to OS detection,
-v means verbose mode and,
-T4 states to use the aggressive timing template. Nmap offers six timing templates using
-T option followed by the number (0–5) such as template paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5).

The first two less noisy templates are used for IDS evasion due to slow scanning. Normal mode is the default mode hence not necessary to state explicitly. Aggressive/insane modes assume the network as fast and reliable and speeds the scans but are very noisy.

Nmap output states the port states in one of the following states as:
Related Content

A Novel Approach for Computer-Aided Diagnosis for Distinction Between Benign and Malignant of Lung Nodules Based on Machine Learning Techniques

An Efficient, Anonymous and Unlinkable Incentives Scheme
[www.igi-global.com/article/an-efficient-anonymous-and-unlinkable-incentives-scheme/148300?camid=4v1a](www.igi-global.com/article/an-efficient-anonymous-and-unlinkable-incentives-scheme/148300?camid=4v1a)

A Secure and Trustful e-Ordering Architecture (TOES) for Small and Medium Size Enterprises (SMEs)
[www.igi-global.com/chapter/secure-trustful-ordering-architecture-toes/45817?camid=4v1a](www.igi-global.com/chapter/secure-trustful-ordering-architecture-toes/45817?camid=4v1a)

A Keystroke Biometric System for Long-Text Input
[www.igi-global.com/article/keystroke-biometric-system-for-long-text/43056?camid=4v1a](www.igi-global.com/article/keystroke-biometric-system-for-long-text/43056?camid=4v1a)