Information Gathering

담당교수 : 신원
대상 : 정보보호학과 3/4학년
과목 : 해킹 및 악성코드 대응
학기 : 2020년 1학기

Definition

- Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system

Objectives

- The major objectives of footprinting include collecting the target's network information, system information, and the organizational information.

Steps

1. Collect basic information about the target and its network
2. Determine the operating system used, platforms running, web server versions, etc.
3. Perform techniques such as Whois, DNS, network and organizational queries
4. Find vulnerabilities and exploits for launching attacks

Collect Network Information

- Domain name / Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites / private websites
- TCP and UDP services running
- Access control mechanisms and ACLs
- Networking protocols
- VPN points
- ACLs
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms
- System enumeration

Collect Organization's Information

- Employee details
- Organization's website
- Company directory
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles/press releases

Footprinting Threats

- Social Engineering
- System and Network Attacks
- Information Leakage
- Privacy Loss
- Corporate Espionage
- Business Loss

Footprinting Methodology

- Footprinting through Search Engine
- Website Footprinting
- E-Mail Footprinting
- Competitive Intelligence
- Footprinting using Google
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Definition

- Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network
- Network scanning is one of the components of intelligence gathering an attacker uses to create a profile of the target organization

Objectives

- Discovering live hosts, IP address, and open ports of live hosts running on the network
- Discovering open ports
- Discovering operating systems and system architecture of the targeted system
- Identifying the vulnerabilities and threats
- Detecting the associated network service of each port

Scanning Methodology

- Check for Live Systems
- Check for Open Ports
- Scanning Beyond IDS
- Banner Grabbing
- Scan for Vulnerability
- Draw Network Diagrams
- Prepare Proxies
- Scanning Pen Testing

Scanning Tools

- Nmap
  - Nmap is a security scanner for network exploration and hacking
  - It allows you to discover hosts and services on a computer network, thus creating a "map" of the network
  - Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime
  - Attackers use Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, operating systems, and OS versions
- Hping2 / Hping3
  - HPing2/HPing3 is a command-line-oriented TCP/IP packet assembler/analyzer that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols

Scanning Techniques

- TCP Connect / Full Open Scan
- Stealth Scans: SYN Scan (Half-open Scan); XMAS Scan, FIN Scan, NULL Scan
- IDLE Scan
- ICMP Echo Scanning / List Scan
- SYN / FIN Scanning Using IP Fragments
- UDP Scanning
- Inverse TCP Flag Scanning
- ACK Flag Scanning

Definition

- Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system
- In the enumeration phase, the attacker creates active connections to the system and performs directed queries to gain more information about the target

Information Enumerated by Intruders

- Network resources and shares
- Users and groups
- Routing tables
- Auditing and service settings
- Machine names
- Applications and banners
- SNMP and DNS details

Techniques for Enumeration

- Extract user names using E-mail IDs
- Extract user names using SNMP
- Extract user groups for Windows
- Extract information using the default passwords
- Brute force Active Directory
- Extract information using DNS Zone Transfer

Services and Ports to Enumerate

- TCP 23 : Telnet Protocol
- TCP 25 : Simple Mail Transfer Protocol (SMTP)
- TCP 53 : DNS zone transfer
- TCP 80 : Hyper-text Transfer Protocol (HTTP)
- TCP 135 : Microsoft RPC Endpoint Mapper
- TCP 137 : NetBIOS Name Service (NBNS)
- TCP 139 : NetBIOS Session Service (SMB over NetBIOS)
- UDP 161 : Simple Network Management Protocol (SNMP)
- TCP/UDP 389 : Lightweight Directory Access Protocol (LDAP)
- TCP 445 : SMB over TCP (Direct Host)
- TCP/UDP 3368 : Global Catalog Service
- TCP 3389 : Remote Desktop Protocol (RDP)
- TCP 5800/5900 : Virtual Network Computing (VNC)