Chapter 4

Enumeration

Theory

Ethical Hacking

Enumeration

Enumeration is the process of establishing an active connection to the target host to discover potential attack vectors in the computer system, information gained at this phase can be used for further exploitation of the system. It is often considered as a critical phase because few pieces of information gathered in this phase can help us directly exploit the target computer.

Information gathered in this phase

1. Usernames, Group names
2. Hostnames
3. Network shares and services
4. IPtables and routing tables
5. Service settings and Audit configurations
6. Application and banners
7. SNMP and DNS Details

NetBIOS enumeration

NetBIOS stands for Network Basic Input Output System. It allows computers to communicate over a LAN to share files and devices like printers. NetBIOS names are used to identify network devices over TCP/IP.

NetBIOS Name List:

Name	NetBIOS code	NetBIOS code	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<user name>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the PDC for that domain

Benefits of NetBIOS Enumeration:

1. Information related to computers that belong to a domain.
2. Details related to shares on computers in the network.
3. Extracting policies and passwords.

SMB Enumeration

SMB stands for Server Message Block. It is mainly used for providing shared access to files, printers and miscellaneous communications between nodes on a network. It also provides an authenticated inter-process communication mechanism.

DNS Enumeration

DNS enumeration retrieves information regarding all the DNS servers and their corresponding records related to an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

DNS - Domain Name Servers

The Internet equivalent of the phone book. They maintain the directory of domain names & translate them to internet protocol addresses.

DNS Records

The list of DNS records provides an overview of types of resource records stored in the zone files of the domain name system. The DNS implements a distributed, hierarchical and redundant database for information associated with internet domain names & addresses.

DNS record types and their uses

-A (Address) maps hostnames to IPv4 address.
-SOA (Start of Authority) identifies the DNS server responsible for the domain information.
-CNAME (Canonical Name) Provides additional names or aliases for the address.
-AAAA (Address) maps hostnames to IPv6 address.
-MX (Mail exchange) Identifies the mail server for the domain
-SRV (Service) Identifies services such as directory services

-PTR (Pointer) Maps IP address to hostnames
-NS (Nameserver) Identifies other name servers for the domain

DNS Zone Transfer

- Used to replicate DNS data across some DNS Servers or to backup DNS files. A user or server will perform a specific zone transfer request from a name server.
- DNS servers should not permit zone transfers towards any IP address from the Internet.
- Since zone files contain complete information about domain names, subdomains and IP addresses configured on the target name server, finding this information is useful for increasing your attack surface and for better understanding the internal structure of the target company.
- We can identify hidden subdomains, development servers information, and internal IP addresses, etc.
- Information gathered from zone files can be useful for attackers to implement various attacks against the target company, like targeting test or development servers which are less secure.

NTP Enumeration

NTP (Network Time Protocol) utilizes UDP port 123. Through NTP enumeration you can gather information such as a list of hosts connected to NTP server, IP addresses, system names, and operating systems running on the client system in a network. All this information can be enumerated by querying the server.

SNMP Enumeration

Simple Network Management Protocol is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs, switches and other network devices. SNMP is a popular protocol found enabled on a variety of operating systems like Windows Server, Linux & UNIX servers as well as network devices.

SMTP Enumeration

SMTP enumeration allows us to determine valid users on the SMTP server. With the help of built-in SMTP commands, we can gather useful information.

1. VRFY - Is used for validating users.
2. EXPN – Reveals the actual delivery address of mailing lists.
3. RCPT TO - It defines the recipients of the message.

Countermeasures

- Install IDS & IPS to detect and stop Enumerating attacks done on any ports.
- Install honeypot application in a proxy server to give false information to the hacker.
- Upload robots.txt file in the website to stop Footprinting of directories.
- Enable DNSSec option in server OS to avoid information leakage through DNS server.
- Hosts can be locked down and securely configured and patched. Limit services to only those needed.
- Network services can be locked down and made not to give up as much useful information to a hacker.
- Changing default security configuration is very important.
- Block ports to unknown hosts.
- Turn off file and print sharing services in windows.
- Prevent DNS zone transfers to unknown hosts.