Enumeration

TOPICS

- What is Enumeration
- Banner Grabbing
- Commonly Enumerated Services
  - FTP
  - SMTP
  - HTTP
  - TFTP
  - NetBIOS
- Countermeasures

RECALL – PHASES OF HACKING

WHAT IS ENUMERATION?

- Attacker creates active connections to targets and performs directed queries to gain more information
  - Identify system attack points
  - Perform future password attacks
- Conducted in an intranet environment
- Retrieves
  - user accounts
  - resource shares
  - known vulnerabilities of software versions

BANNER GRABBING

- Examining banners can sometimes give clues about the software servicing a particular port

SOME COMMON NETWORK SERVICE SOFTWARE

HTTP/S	Mail	FTP
• Apache • Microsoft IIS • Nginx	• Microsoft Exchange • Sendmail • PostFix • Eudora • Lotus Notes	• Microsoft IIS • Filezilla • vsftpd

ENUMERATING COMMON NETWORK SERVICES

- FTP
- SMTP
- TFTP
- HTTP
- NetBIOS

FTP ENUMERATION

- Uses TCP port 21 for control
- Many FTP servers allow anonymous login
- Googling for FTP Servers

  Search for intitle:"Index of ftp://”

SMTP ENUMERATION

- Allows you to test for valid users on an SMTP server
- Useful built-in SMTP commands:
  - VRFY – for validating users
  - EXPN – asks for actual delivery address of aliases
  - RCPT TO – defines recipients of an email
- SMTP server responses can be used as basis to know if a user exists or not
- Connection to the SMTP server can use a telnet utility set to connect through port 25
- smtp-user-enum for smtp user enumeration

SMTP ENUMERATION

Using VRFY

```
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
HELO
502 5.5.2 Error: command not recognized
HELO x
250 metasploitable.localdomain
VRFY alice
252 2.0.0 alice
VRFY anna
550 5.1.1 <anna>: Recipient address rejected: User unknown in
local recipient table
```

SMTP ENUMERATION

Using RCPT TO

```
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
HELO
502 5.5.2 Error: command not recognized
HELO x
MAIL FROM:hacker@hacme.om
250 2.1.0 Ok
RCPT TO:bob
250 2.1.5 Ok
RCPT TO:brenda
550 5.1.1 <brenda>: Recipient address rejected: User unknown in local recipient table
```

SMTP ENUMERATION

Using smtp-user-enum

Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.

smtp-user-enum -M VRFY -U /usr/share/wordlists/fern-wifi/common.txt -t 192.168.46.134

```
┌──(kali㉿kali)-[~]
└─$ smtp-user-enum -M VRFY -U /usr/share/wordlists/fern-wifi/common.txt -t 192.168.46.134
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/wordlists/fern-wifi/common.txt
Target count ............. 1
Username count ........... 478
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sun Oct  9 11:19:51 2022 #########
 exists.46.134: lp
 exists.46.134: root
 exists.46.134: service
 exists.46.134: sys
 exists.46.134: user
 exists.46.134: MAIL
 exists.46.134: Root
 exists.46.134: SERVICE
 exists.46.134: SYS
 exists.46.134: Service
 exists.46.134: User
######## Scan completed at Sun Oct  9 11:19:53 2022 #########
11 results.

478 queries in 2 seconds (239.0 queries / sec)
```

TFTP ENUMERATION

- Runs on UDP port 69
- No authentication so anyone can grab a file
- Use a tftp client for this
- Can be useful in getting system user account and password files
  - /etc/passwd.bak and shadow.bak in Linux

WEB DIRECTORY ENUMERATION

- There is essentially no way for a user to know which files are found in which directories on a web-server, unless the whole server has directory listing by default. So what the attacker can do is to brute force hidden files and directories, by sequentially visiting pages defined in a wordlist. The attack is of course very noisy and will show up fast in the logs.

WEB DIRECTORY ENUMERATION

dirb

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses.

```
dirb http://<ip address>/ /usr/share/wordlists/dirb/common.txt
dirb http://<ip address>/ /usr/share/wordlists/dirb/common.txt -X .php
dirb http://<ip address> /usr/share/wordlists/dirb/common.txt -N 302
```

WEB DIRECTORY ENUMERATION

gobuster

Gobuster is a tool used to brute-force URIs including directories and files as well as DNS subdomains.

```
gobuster -e -u http://<ip address>/ -w /usr/share/wordlists/dirb/common.txt
```

NETBIOS ENUMERATION

- NetBIOS is used to facilitate access of LAN resources by client software
- NetBIOS name is a 16-char ASCII string
- Uses TCP 137 and 139
- Typically needs a connection to the local network segment
- Allows enumeration of Windows domains and computers

NETBIOS ENUMERATION TOOLS: WINDOWS

- List computers in a domain

  net view /domain:<*domainname*>

- Extract system name, domain and logged-on users of remote computer

  nbtstat –a/-A <name/ipaddress>

- View NetBIOS cache on local computer

  nbtstat –c

NETBIOS ENUMERATION TOOLS: LINUX

- **nbtscan** queries for the NetBIOS name of a Windows computer IP address

  nbtscan <ip address>

- NMAP **nbstat script** – equivalent of the Windows nbtstat tool

  nmap –script=nbstat <ip address>

NETBIOS SESSIONS

- NetBIOS Null session
  - an unauthenticated connection to a Windows machine
  - considered by some as the biggest security vulnerability in Windows history
  - Turned on by default in Win NT/2000 but with restrictions by default in succeeding OS
- Can allow users to view and access shared resources on a remote computer through the SMB protocol

SMB OVER NETBIOS ENUMERATION

- SMB (Server Message Block) is an application layer protocol that provides access to shared folders, files, printers, etc over the network
- Can run on top of NetBIOS via ports TCP 137 and 139
- Easily accessed for enumeration if the target Windows computer allows null sessions
  - User accounts and groups
  - Logged in user
  - Shared folders

SMB OVER NETBIOS ENUMERATION

smbmap

SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands. This tool was designed with pen testing in mind, and is intended to simplify searching for potentially sensitive data across large networks.

smbmap -u <username> -p <passwords> -H <ip address>

SMB OVER NETBIOS ENUMERATION

enum4linux

- Enum4linux is a tool for enumerating information from Windows and Samba systems. It attempts to offer similar functionality to enum.exe formerly available from www.bindview.com.
- It is written in PERL and is basically a wrapper around the Samba tools smbclient, rpclient, net and nmblookup. The samba package is therefore a dependency.

enum4linux –a <ip address>

SMB OVER NETBIOS ENUMERATION

- NMAP has several built-in scanning scripts for Windows SMB.

  nmap --script=<script-name> <ip address>

- Script list
  - smb-enum-users
  - smb-enum-sessions
  - smb-enum-groups
  - smb-enum-shares

COUNTERMEASURES

- FTP – require log ins
- SMTP – configure server to ignore nonexistent addresses
- Other services – turn off if unnecessary, limit banner information
- NetBIOS
  - limit ports 137, 139 and 445
  - restrict anonymous user – set registry entry

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous = 1 or 2**