J. A. “Drew” Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Enumeration

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Chapter Outline

- **Definition and Techniques**
- **Enumeration on Windows and Linux**
- **LDAP, NTP, and SMTP**

Definition and Techniques

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

What is Enumeration

- Enumeration is the process of extracting information from the target’s system through active connections.
- This is a crucial step and is where the attacker has the greatest chance of being detected.
- Types of information:
  - Network resources and shares
  - Users and groups
  - Routing tables
  - Auditing and service settings
  - Machine names
  - SNMP and DNS details

Enumeration Techniques

- **Extracting information through email IDs**
  - – **Obtain email credentials through the targets email address.**
- **Obtaining information through default passwords**
  - – **Using default settings or passwords to gain access to a system.**
- **Brute force attacks on directory services**
  - – **A directory service has information used to administer a network. It is an ideal target to gain extensive information on the network environment.**
- **Exploiting SNMP**
  - – **Simple Network Management Protocol can be used to gain usernames.**

Enumeration Techniques

- Exploiting SMTP
  - Simple Mail Transport Protocol can be connected to in order to steal credentials and other information.
- DNS zone transfers
  - A zone transfer is used to update a DNS server with newer data. This transfer could contain information to help map out the network.
- Capturing User Groups
  - Determining whether a session account is in a specific group.
- Retrieving system policy settings
  - Finding the security policies in place for a network environment.

Enumeration on Windows and Linux

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Enumeration on Windows

- Users
  - Users are most responsible for controlling access to a system. By default windows has at least two user accounts, the administrator and guest account.
  - Prior to Windows Vista the admin account was the default account and admin rights were enabled by default.
- Groups
  - A group contains multiple users and helps to simplify user rights/ management.
  - You can assign rights to one group rather than having to do this task for each user.

Enumeration on Windows

- Default Windows groups
  - Anonymous logon
  - Batch
  - Creator group
  - Creator owner
  - Everyone
  - Interactive
  - Network
  - Restricted
  - Self
  - Service
  - System
  - Terminal server user

Enumeration on Windows

- Security Identifiers (SID) is a number by the operating system to uniquely identify specific users, groups, and devices.
- Decoding SID numbers
  - All SID numbers follow the pattern of S-1-5-21
  - Administrator accounts end with 500
  - Guest accounts end with 501
  - S-1-0-0 is used when the SID value is unknown or a group has no members.
  - S-1-1-0 is used for the group world, which consists of every user.
  - S-1-2-0 is used for the group local, which are users who are logged in through the local terminal.

Enumeration on Windows

- SID storage
  - The Security Account Manager (SAM) is used to store SID information and associated passwords.
  - Passwords are stored encrypted in Lan Manager (LM) hash format and NTLM hash format.
  - SAM is apart of the windows registry and it is located at \windows\system32\config\

Enumeration on Windows

- Commonly exploited services
  - NetBIOS was originally intended to help with system resource accessibility on a local area network.
    - User 16 character names where the first 15 identify the machine with the last character identifying the service.
  - If port 139 is open then attackers can attempt to view or access information. This port is usually associated with NetBIOS.
- Null Session
  - This is when a connection is made to Windows without any credentials being provided.
    - This is supposed to be used to assist with the sharing of information between devices. Consequently anyone can create this session to gain information on a Windows service.

Enumeration on Linux

- Similar to Windows, Linux has users that require the following information
  - Username and user ID (UID)
    - The UID is usually above 500 for users and below 100 for system accounts
  - Password
    - Passwords are stored at etc/passwd file or shadow file
    - Each user account has their own password the this format

      username:password:UID:GID:name directory:shell
  - Primary group name and group ID (GID)
  - Secondary group name and GID
  - Location of the home directory
  - Preferred shell

Significant Linux Ports & Uses

Port	Connection	Use
21	TCP	FTP
23	TCP	Telnet
25	TCP	SMTP
53	TCP/ UDP	DNS
80	TCP	HTTP
135	TCP	RPC
137	TCP	NetBIOS
139	TCP	NetBIOS
445	TCP	SMB
161, 162	UDP	SNMP
389	TCP/ UDP	LDAP
3268	TCP/ UDP	Global Catalog Service

Helpful Linux Commands

- finger
  - Returns information about a user on a given system.
- rpcinfo
  - Uses the Remote Procedure Call (RPC) gain information.
- showmount
  - Identifies the shared directories on a system and any clients who have remotely mounted a file system.
- enum4linux
  - Allows for extraction of data through Samba software.

LDAP, NTP, and SMTP

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

LDAP Enumeration

- **Offensive**
  - **There are several free tools available to gain information from an LDAP and directory service.**
    - **JXplorer, LDAP Admin Tool, LEX, and LDAP Search.**
    - **Can store usernames, passwords, and emails.**
- **Defensive**
  - **A good way to filter LDAP enumeration is to close ports or filter traffic over the LDAP port (389).**

NTP and SMTP Enumeration

- NTP is used to synchronize the clocks across multiple hosts on a network.
  - Ntpdate, ntptrace, ntpdc, and ntpq are commands that can be used to view NTP data.
- SMTP is a protocol to send messages between servers that are used to send and receive emails.
  - VRFY
    - This is a command that is used to verify valid accounts on the server.
  - EXPN
    - Similar to VRFY, but instead of returning one user it returns all users on a distribution list.