PENETRATION TESTING

What is enumeration? [updated 2021]

January 22, 2021 by Raghu Chakravartula

Share:

Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.

Enumeration is used to gather the following:

- Usernames, group names
- Hostnames
- Network shares and services
- IP tables and routing tables
- Service settings and audit configurations
- Application and banners
- SNMP and DNS details

Significance of enumeration

Enumeration is often considered as a critical phase in penetration testing, as the outcome of enumeration can be used directly for exploiting the system.

Enumeration classification

Enumeration can be performed on the following.

1. NetBios enumeration

In this Series

What is enumeration? [updated 2021]

Red Teaming: Taking advantage of Certify to attack AD networks

How ethical hacking and pentesting is changing in 2022

Ransomware penetration testing: Verifying your ransomware readiness

Red Teaming: Main tools for wireless penetration tests

Fundamentals of IoT firmware reverse engineering

Red Teaming: Top tools and gadgets for physical assessments

Red teaming: Initial access and foothold

Top tools for red teaming

2. SNMP enumeration
3. LDAP enumeration
4. NTP enumeration
5. SMTP enumeration
6. DNS enumeration
7. Windows enumeration
8. UNIX/Linux enumeration

The rest of the document explains each one of the above enumeration types, as well as tools and controls for preventing the same.

What is NetBIOS?

NetBIOS stands for Network Basic Input Output System. It was developed by Sytek and IBM. The primary intention of NetBIOS was developed as an Application Programming Interface (API) to enable access to LAN resources by the client's software.

NetBIOS naming convention starts with a 16-character ASCII string used to identify the network devices over TCP/IP; 15 characters are used for the device name, and the 16th character is reserved for the service or name record type.

NetBIOS enumeration explained

NetBIOS software runs on port 139 on the Windows operating system. File and printer service needs to be enabled to enumerate NetBIOS over Windows. An attacker can perform the following on the remote machine:

1. Choosing to read or write to a remote machine, depending on the availability of shares.
2. Launching a Denial of Service (DoS) attack on the remote machine.
3. Enumerating password policies on the remote machine.

NetBIOS enumeration tools

The following table shows the list of tools to perform NetBIOS enumeration:

Number	Name of the tool	Web links
01	Nbtstat	www.technet.microsoft.com
02	SuperScan	http://www.mcafee.com/in/downloads/free-tools/superscan.aspx
03	Hyena	http://www.systemtools.com/hyena/
04	Winfingerprint	https://packetstormsecurity.com/files/38356/winfingerprint-0.6.2.zip.html
05	NetBIOS enumerator	http://nbtenum.sourceforge.net/

NetBIOS security controls

The following are the security controls to prevent NetBIOS enumeration attacks:

- Minimize the attack surface by minimizing the unnecessary service like Server Message Block (SMB).
- Remove file and printer sharing in Windows OS.

What is SNMP?

SNMP stands for Simple Network Management Protocol. SNMP is an application-layer protocol that runs on User Datagram Protocol (UDP) and is used for managing network devices, which run on the IP layer like routers.

SNMP is based on a client-server architecture where the SNMP client or agent is located on every network device and communicates with the SNMP managing station via requests and responses. Both SNMP requests and responses are configurable variables accessible by the agent software. SNMP contains two passwords for authenticating the agents before configuring the variables and for accessing the SNMP agent from the management station.

SNMP passwords are:

1. Read community strings are public, and configuration of the device can be viewed with this password.
2. Read/write community strings are private, and configuration of the device can be modified using this password.

SNMP uses a virtual hierarchical database internally for managing the network objects; this database is called Management Information Base (MIB). MIB contains a treelike structure, and object IDs uniquely represent each network object. The network objects can be viewed or modified based on the SNMP passwords.

SNMP enumeration

Default SNMP passwords allow attackers to view or modify the SNMP configuration settings. Attackers can enumerate SNMP on remote network devices for the following:

1. Information about network resources such as routers, shares, devices, etc.
2. ARP and routing tables
3. Device specific information
4. Traffic statistics
5. Etc.

SNMP enumeration tools

The following table shows the list of tools to perform SNMP enumeration:

Number	Name of the tool	Web links
01	OpUtils	https://www.manageengine.com/products/oputils/
02	SolarWinds	http://www.solarwinds.com/
03	SNScan	http://www.mcafee.com/us/downloads/free-tools/snscan.aspx
04	SNMP Scanner	http://www.secure-bytes.com/snmp-scanner.php
05	NS Auditor	http://www.nsauditor.com/

SMTP security controls

The following are the security controls to prevent SNMP enumeration attacks:

- Minimize the attack surface by removing the SNMP agents where not needed.
- Change default public community strings.

- Upgrade to SNMPv3, which encrypts the community strings and messages.
- Implement group policy for additional restriction on anonymous connections.
- Implement firewalls to restrict unnecessary connections.
- Implement IPSec filtering.
- Block access to TCP/UDP ports 161.
- Encrypt and authenticate using IPSEC.

What is LDAP?

LDAP Stands for Light-Weight Directory Access Protocol. It is an Internet protocol for accessing distributed directory services like Active Directory or OpenLDAP. A directory service is a hierarchical and logical structure for storing records of users.

LDAP is based on client and server architecture. LDAP transmits over TCP and information is transmitted between client and server using Basic Encoding Rules (BER).

LDAP enumeration

LDAP supports anonymous remote queries on the server. The query will disclose sensitive information such as usernames, address, contact details, department details and so on.

LDAP enumeration tools

The following table shows the list of tools to perform LDAP enumeration:

Number	Name of the tool	Web links
01	Softerra LDAP Administrator	http://www.ldapadministrator.com/
02	Jxplorer	http://jxplorer.org/
03	active directory domain services management pack for system center	https://www.microsoft.com/en-in/download/details.aspx?id=21357
04	LDAP Admin Tool	http://www.ldapadmin.org/
05	LDAP Administrator tool	https://sourceforge.net/projects/ldapadmin/

LDAP security controls

The following are the security controls to prevent LDAP enumeration attacks:

- Use SSL to encrypt LDAP communication.
- Use Kerberos to restrict the access to known users.
- Enable account lockout to restrict brute-forcing.

What is NTP?

NTP stands for Network Time Protocol, and it was designed to synchronize clocks of networked computers. NTP can achieve accuracies of 200 milliseconds or better in local area networks under ideal conditions. NTP can maintain time to within ten milliseconds (1/100 second) over the internet.

NTP is based on agent-server architecture, where an agent queries the NTP server. It works on User Datagram Protocol (UDP) and the well-known port 123.

NTP enumeration

An attacker can enumerate the following information by querying an NTP server.

1. List of hosts connected to the NTP server
2. Internal client IP addresses, hostnames and operating system used

NTP enumeration tools

The following table shows the list of tools to perform NTP enumeration:

Number	Name of the tool	Description
01	ntptrace	Query to determine from where the NTP server updates its time and traces the chain of NTP servers from a source.
02	ntpdc	Query the NTP daemon about its current state and to request changes in the state.
03	Ntpq	Monitors NTP daemon NTPD operations and determines performance.

NTP security controls

The following are the security controls to prevent NTP enumeration attacks:

- Restrict the usage of NTP and enable the use of NTPSec, where possible.
- Filter the traffic with IPTables.
- Enable logging for the messages and events.

What is SMTP?

SMTP stands for Simple Mail Transfer Protocol and it is designed for electronic mail (email) transmissions. SMTP is based on client-server architecture and works on Transmission Control Protocol (TCP) on port 25.

SMTP uses Mail Exchange (MX) servers to send the mail via the Domain Name Service; however, should an MX server not detected, SMTP will revert and try an A or alternatively SRV records.

SMTP enumeration

SMTP provides three built-in commands:

- VRFY: Validate users on the SMTP servers
- EXPN: Delivery addresses of aliases and mailing lists
- RCPT TO: Defines the recipients of the message

SMTP servers respond differently to the commands mentioned above, and SMTP enumeration is possible due to varied responses. Attackers can determine the valid users on the SMTP servers with the same technique.

SMTP enumeration tools

The following table shows the list of tools to perform SMTP enumeration:

Number	Name of the tool	Web links
01	NetScan Tools Pro	http://www.netscantools.com/nstpromain.html
02	SMTP User Enum	http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum

SMTP security controls

The following are the security controls to prevent SMTP enumeration attacks:

- Ignore email responses from unknown recipients.
- Disable open relay functionality.
- Prune any sensitive information like mail server and localhost in the mail responses.

What is DNS?

DNS stands for Domain Name Service, and it is primarily designed as hierarchical decentralized distributed naming systems for computers, services or any resource connected to the network. DNS resolves hostnames to its respective IP addresses and vice versa.

DNS internally maintains a database for storing the records. The following are the most commonly used record types in DNS.

- Start of Authority (SOA)
- IP addresses (A and AAAA)
- SMTP mail exchangers (MX)
- Nameservers (NS)
- Pointers for reverse DNS lookups (PTR)
- Domain name aliases (CNAME)

DNS works on both UDP and TCP on port 53. It uses UDP for resolving queries and TCP for zone transfers. DNS zone transfer allows DNS databases to replicate the portion of the database from primary server to the secondary server. DNS zone transfer must only be allowed by other validated secondary DNS servers acting as clients.

DNS enumeration

DNS enumeration is possible by sending zone transfer requests to the DNS primary server pretending to be a client. DNS enumerating reveals sensitive domain records in response to the request.

DNS enumeration tools

The following table shows the list of tools to perform DNS enumeration:

Number	Name of the tool	Web links
01	nslookup	https://centralops.net/co/
02	DNS Dumpster	https://dnsdumpster.com/
03	DNS Recon	http://tools.kali.org/information-gathering/dnsrecon

DNS security controls

The following are the security controls to prevent DNS enumeration attacks:

- Configure DNS servers not to send DNS zone transfers to unauthenticated hosts.
- Ensure DNS zone transfers do not contain HINFO information.
- Ensure to trim DNS zone files to prevent revealing unnecessary information.

Windows enumeration

Windows operating systems can be enumerated with multiple tools from Sysinternals. Many more sysinternal tools can be downloaded here. The following list is the list of some important utilities.

Numbers	Name of the tool	Description
01	PsExec	Execute processes on remote machines.
02	PsFile	Displays list of files opened remotely.
03	PsGetSid	Translate SID to display name and vice versa.
04	PsKill	Kill processes on local or remote machines.
05	PsInfo	Displays installation, install date, kernel build, physical memory, processors type and number and so on.
06	PsList	Displays process, CPU, memory, thread statistics and more.
07	PsLoggedOn	Displays local and remote logged users.
08	PsLogList	View event logs.

Windows security controls

The following are the security controls to prevent Windows enumeration attacks.

- Minimize the attack surface by removing any unnecessary or unused service.
- Ensure Windows Firewall is configured to restrict the access.

UNIX or Linux enumeration

UNIX or the Linux operating system can be enumerated with multiple command-line utilities provided by the OS. Below is the list of utilities.

Number	Name of the tool	Description or links
01	Finger	Enumerate users on remote machines.
02	rpcInfo	Enumerate remote procedure calls.
03	rpcclient	Enumerate usernames on Linux.
04	showmount	Enumerate list of shared directories.
05	Enum4Linux	https://labs.portcullis.co.uk/tools/enum4linux/

LINUX security controls

The following are the security controls to prevent Linux enumeration attacks

- Minimize the attack surface by removing any unnecessary or unused service.
- Ensure IPTables is configured to restrict the access.

Posted: January 22, 2021

Share:

Raghu Chakravartula

VIEW PROFILE

Raghu Nallani Chakravartula is a Subject matter expert in Incident handling and response, Penetration testing, Vulnerability assessment, forensics, malware analysis, Intrusion analysis and response, Secure Software Development, Code reviews, Secure documentation. He possesses 13+ years of professional Information Security experience with companies like C-DAC R&D, Citrix R&D, Samsung R&D, WTM-WAP, HP R&D and GE R&D.

Related Articles