**“Enumeration: Data Gathering”**

***Table of Contents Pages***

*Introduction………………………………………………..(1)*

*Extraction………………………………………………..(1-2)*

*Tools……………………………………………………..(2-3)*

1. *NetBIOS Enumeration………………………..(2)*
2. *DNS Enumeration……………………………..(2-3)*
3. *enum4linux………………………………………(3-4)*

*Quick Fix………………………………………………..(4)*

*Citations………………………………………………..(5)*

Daniel Rao

Feb 28th, 2021

Vince Skinner

**Enumeration: Information Gathering**

**Introduction**

Enumeration usually involves connecting to a remote system and does not involve simply identifying the system. Hackers aren't satisfied with knowing what computers are connected on a network. Their goal is to find live systems and gain access to them.

From security perspective if we look at enumeration is a massive part of security testing and it usually thought to gain permissions in writing from the network owner to keep things cool, else this could lead to a criminal case as it involves the finding of resources that are shared on the systems, discovering logon accounts and their passwords, and gaining access to the network resources. As mentioned by geeks for geeks on their website, “Enumeration is fundamentally checking. An attacker sets up a functioning associated with the objective host. The weaknesses are then tallied and evaluated. It is done mostly to look for assaults and dangers to the objective framework. “

**Extraction**

As mentioned, enumeration is simply the process of extracting the following information from a network:

1. Resources shared on the network
2. Network topology and architecture
3. Usernames or groups assigned on the network
4. Sensitive information about the user such as their recent logon times.

In order to determine what resources are shared on the network the security testers must use port scanning or footpriniting first to determine what OS are being utilized by the system. It is only after that when the tester can make a decision on what tools to use. For example Windows operating system testers use very specific tools to view shares and possibly access resources.

Enumeration is far more intensive than a passive network scan to find a resource but it is rather a practise of trying to access it. For example, sometimes this process might entail the use of guessing a password considering we already know the user name.

**Tools**

Enumerations depend on the services that the systems offer. They can be −

* DNS enumeration
* NTP enumeration
* SNMP enumeration
* Linux/Windows enumeration
* SMB enumeration

Let us now discuss some of the tools that are widely used for Enumeration.

# **NetBIOS Enumeration**

NetBIOS stands for Network Basic Input Output System. It Allows computer communication over a LAN and allows them to share files and printers.

NetBIOS names are used to identify network devices over TCP/IP (Windows). It must be unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.

Attackers use the NetBIOS enumeration to obtain:

* List of computers that belong to a domain
* List of shares on the individual hosts on the network
* Policies and passwords

## Commands and tools used:

Nbtstat: utility used to find protocol statistics, NetBIOS name table and name cache details

Superscan: GUI tool used to enumerate windows machine

Net view: command line tool to identify shared resources on a network

# **DNS Enumeration**

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems. The list of DNS records provides an overview of types of resource records (database records) stored in the zone files of the Domain Name System (DNS). The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses.

DNS Zone Transfer used to replicate DNS data across a number of DNS servers or to back up DNS files. A user or server will perform a specific zone transfer request from a ―name server. If the name server allows zone transfers by an anonymous user to occur, all the DNS names and IP addresses hosted by the name server will be returned in human-readable ASCII text.

## **Tools:**

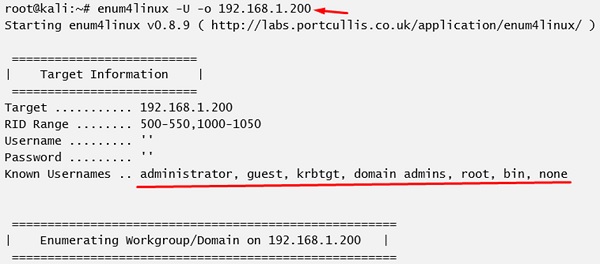
nslookup, maltego, dnenum,dnsrecon

## **Countermeasures:**

1. Disable Zone transfer by untrusted hosts
2. Ensure that private hostnames are not referenced to IP addresses within the DNS zone files of publicly accessible DNS servers.
3. Use premium registration services.

## **3) enum4linux**

enum4linux is used to enumerate Linux systems. Take a look at the following screenshot and observe how we have found the usernames present in a target host.



## **Quick Fix**

It is recommended to disable all services that you don’t use. It reduces the possibilities of OS enumeration of the services that your systems are running.

Citations:

<https://www.greycampus.com/opencampus/ethical-hacking/dns-enumeration>

<https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_enumeration.htm>

<https://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP>

<https://www.geeksforgeeks.org/cyber-security-types-of-enumeration/>