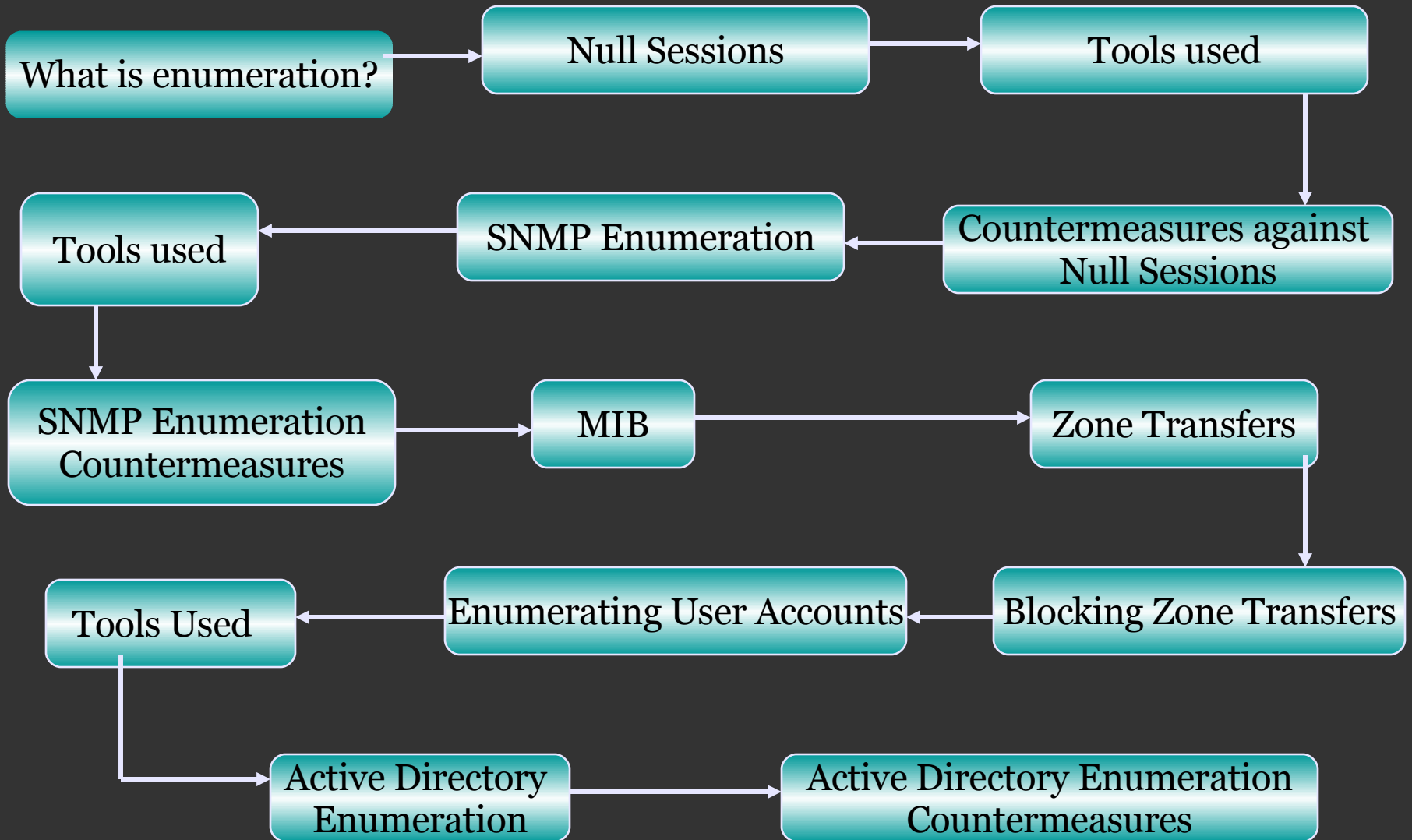


Enumeration

Presented by
Sheetal Joseph

Enumeration



Enumeration

- Enumeration involves active connections to systems and directed queries.
- The type of information enumerated by intruders:
 - Network resources and shares
 - Users and groups
 - Applications and banners

NetBIOS NULL Sessions

The Good, The Bad, and The Ugly

The NULL Session Concept: The Good?

NULL sessions take advantage of features in the SMB (Server Message Block) protocol that exist primarily for trust relationships.

Using these NULL connections allows you to gather the following information from the host:

- List of users and groups
- List of machines
- List of shares
- Users and host SID' (Security Identifiers)

The NULL Session Concept: The Good?

NULL sessions exist in windows networking to allow:

- Trusted domains to enumerate resources
- Computers outside the domain to authenticate and enumerate users
- The SYSTEM account to authenticate and enumerate resources
- NetBIOS NULL sessions are enabled by default in Windows NT and 2000. Windows XP and 2003 will allow anonymous enumeration of shares, but not SAM accounts.

The Bad and the Ugly

Port	Protocol	Description
135	TCP/UDP	Location Service (RPC endpoint mapping)
137	TCP/UDP	NETBIOS Name Service
138	TCP/UDP	NETBIOS Datagram Service
139	TCP/UDP	NETBIOS Session Service
6	TCP	SMB/CIFS

Command: C: \>net use \\192.34.34.2 \IPC\$ "" /u: ""

Enum-Symantec

```
C:\tools>enum -SU <IP Address>
server: <IP Address>
setting up session... success.
getting user list (pass 1, index
0)... success, got 5.
Administrator Guest IUSR_CHANNEL
IWAM_CHANNEL victim_user
enumerating shares (pass 1)... got 4
shares, 0 left:
IPC$ c ADMIN$ C$
cleaning up... success.
```

Hunt -Foundstone

```
C:\tools>hunt \\<IP Address>
share = IPC$ - Remote IPC
share = c -
share = ADMIN$ - Remote Admin
share = C$ - Default share
User = Administrator, , , Built-in account for
administering the computer/domain
Admin is <NetBIOS Name>\Administrator
User = Guest, , , Built-in account for guest access to
the computer/domain
User = IUSR <NetBIOS Name>, Internet Guest Account,
Built-in account for anonymous access to Internet
Information Services, Built-in account for anonymous
access to Internet Information Services
User = IWAM <NetBIOS Name>, Internet Guest Account,
Built-in account for anonymous access to Internet
Information Services out of process applications, Built-
in account for anonymous access to Internet Information
Services out of process applications
User = victim_user Victim Name, ,
```

Winfo-NTSecurity

```
C:\>wininfo 128.148.151.7 ?n
```

```
wininfo 1.5 - copyright (c) 1999-2001, Arne Vidstrom  
- http://www.ntsecurity.nu/toolbox/wininfo/
```

```
Trying to establish null session...  
Null session established.
```

```
USER ACCOUNTS:
```

```
* Administrator
```

```
(This account is the built-in administrator account)
```

```
* Guest
```

```
(This account is the built-in guest account)
```

```
* victim_user
```

```
WORKSTATION TRUST ACCOUNTS:
```

```
INTERDOMAIN TRUST ACCOUNTS:
```

```
SERVER TRUST ACCOUNTS:
```

```
SHARES:
```

```
* IPC$
```

```
* drivec$
```

Using the Information

- Try to logon to the system, using various tools that will try different username and password combinations.
- Install FTP servers, IRC bots, and DDOS tools, then copy the illegal (copyrighted and pirated) software up for distribution.
- A worm called Zotob relies on NULL sessions to propagate.

How to Disable NetBIOS NULL Sessions

Below are instructions on how to manually disable NetBIOS NULL sessions:

Windows XP Home Edition

Note: This also works in Windows 2000 and XP Professional.

- 1. Set the Following Registry Key:
HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=2
- 2. Reboot to make the changes take effect.

Windows XP Professional Edition and Windows Server 2003

- 1. Go to Administrative Tools --> Local Security Policy --> Local Policies --> Security Options. Make sure the following two policies are enabled:
Network Access: Do not allow anonymous enumeration of SAM accounts: Enabled (*Default*)
Network Access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
- This can also be accomplished using the following registry keys:
HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=1 (*This disallows enumeration of shares*)
HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=1 (*Default, not allowing enumeration of user accounts*)
- 2. Reboot to make the changes take effect.

Disabling NetBIOS NULL Sessions

Windows 2000

1. Go to --> Administrative Tools --> Local Security Settings --> Local Policies --> Security Options
2. Select "Additional restrictions of anonymous connections" in the Policy pane on the right
3. From the pull down menu labeled "Local policy setting", select: "No access without explicit anonymous permissions"
4. Click OK
5. The registry setting equivalent is:
HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=2
6. Reboot to make the changes take effect.

Windows NT 4.0 (Service Pack 3 or later)

Set the Following Registry Key:

HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=1

Further Defenses

While the above describes how to disable this vulnerability on the host, there are some things you can do on the network to help defend against NULL sessions:

- Blocking NetBIOS ports on your firewall or border router
- Blocking the Windows networking ports in Figure 1 will prevent against NULL sessions (And other attacks that use NetBIOS)
- Remove the IPC\$ share (net share IPC\$ /delete)
- Intrusion Detection

.

SNMP - Enumeration

BASIC TERMS

SNMP - (Simple Network Management Protocol) - an application-layer protocol for managing TCP/IP based networks. SNMP runs over UDP (which runs over IP).

SNMP Agent - a device running some software that understands the language of SNMP.

SNMP Manager - As an SNMP manager, the router can send SNMP requests to agents and receive SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps

MIB - (Management Information Base) - provides a standard representation of the SNMP agent's available information and where it is stored.

SNMP-Enumeration (contd)

- **Traps** let the manager know that something significant has happened at the agent's end of things:
 - a reboot
 - an interface failure
 - or that something else that is potentially bad has happened
- SNMP requests are typically sent to UDP port 161.
- SNMP responses are typically sent from UDP port 161.
- SNMP notifications are typically sent to UDP port 162.

IP Network Browser

- IP Address or Hostname
- A Subnet Address and Mask
- A Range of IP Addresses
- System MIB Information
- IOS levels and information
- Interface and Memory Information
- Operational Status
- Route and ARP Tables
- MAC Address
- TCP/IP and IPX Network Information
- UDP Services
- TCP Connections
....plus much more.

SNMP Enumeration Defenses

- The simplest way to prevent such activity is to remove the SNMP agent or turn off the SNMP service.
- If shutting off SNMP is not an option, then change the default 'public' community name.
- Implement the Group Policy security option called Additional restrictions for anonymous connections.
- Access to null session pipes, null session shares, and IPsec filtering should also be restricted.

DNS Zone transfer

- The zone transfer is the method a secondary DNS server uses to update its information from the primary DNS server.
- ```
> nslookup
```

```
> set type=any
```

```
> ls -d techM.net > dns.techM.net
```

```
> exit
```

# DNS zone transfer defenses

- Configure the server to only respond to requests for zone transfers from authorized IP addresses.
- Click Start | Programs | Administrative Tools | DNS Manager
- Open the DNS server on which the zone is hosted.
- Right-click on the zone and select Properties | Notify
- Add the IP addresses for any systems that will be allowed to do zone transfers
- Enable the Only Allow Access From Secondaries Included On Notify List check box.
- Click OK.

# Active Directory Enumeration

- All the existing users and groups could be enumerated with a simple LDAP query.
- The only thing required to perform this enumeration is to create an authenticated session via LDAP.
- Connect to any AD server using ldp.exe port 389.
- Authentication can be done using Guest/or any domain account.
- Now all the users and built-in groups could be enumerated.

# AD Enumeration Defenses

- How is this possible with a simple guest account?
- The Win 2k dcpromo installation screen queries the user if he wants to relax access permissions on the directory to allow legacy servers to perform lookup:
  1. Permission compatible with pre-Win2k
  2. Permission compatible with only with Win2k
- Choose option 2 during AD installation.

# Summary

Please do it for me :-)