

Enumeration



Reconnaissance



Enumeration is the process of obtaining network resources, usernames and passwords, services, and machine names.

Information that can be gained by enumeration:

- **Banners from FTP servers, web servers, email servers**
- **FQDNs and IP addresses**
- **IP configuration of routers and servers**
- **Information from Active Directory**
- **Usernames**
- **Share names**

In this chapter, we will show the methods and tools used to perform enumeration, as well as the countermeasures to protect against it.

Web Server Banners

Command to use:

`telnet <webserver> 80`



Type: `GET / HTTP/1.0`

Then hit enter a few times and you will get an error showing what software the web server is running.

```
C:\ Telnet 10.1.1.201
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Wed, 29 Dec 2004 04:00:11 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.
</html>

Connection to host lost.
Press any key to continue...
```

Practice: Banner Grabbing with Telnet

IIS6.0 and other new Web Server's will NOT allow for a standard:
telnet <IP> 80



Solution / Practice:

From a
command
prompt type:
telnet <IP> 80

Then type:

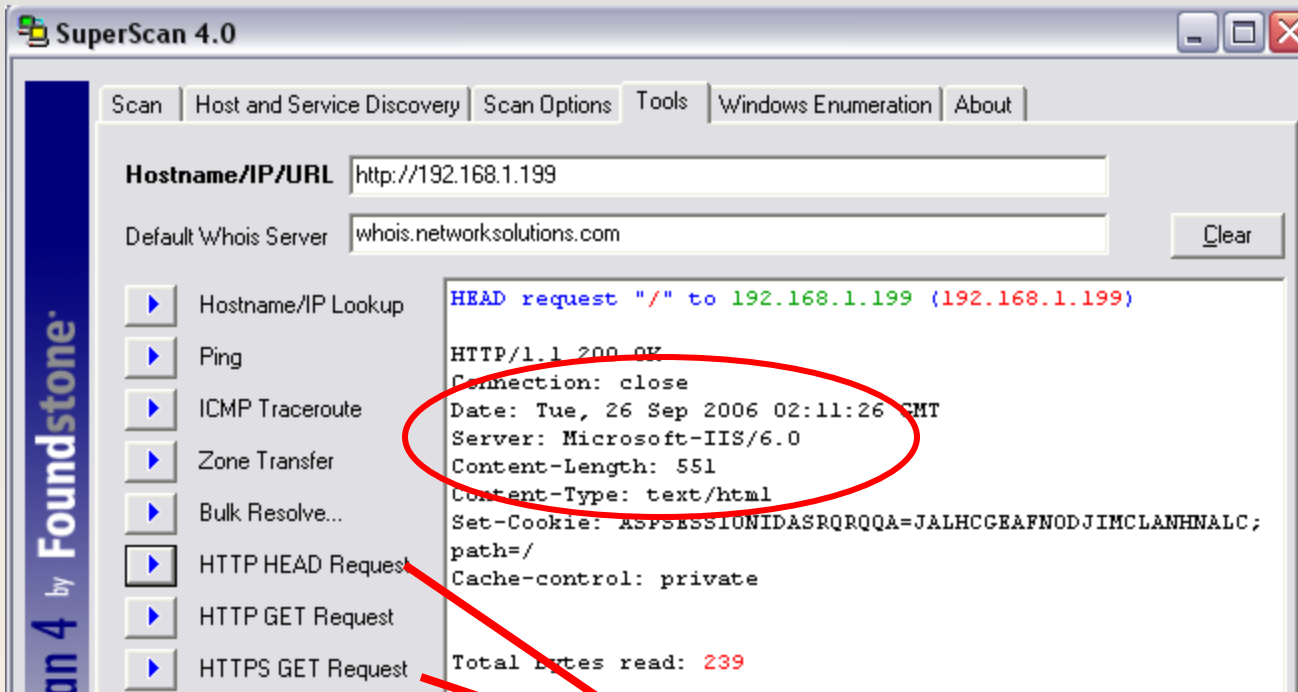
HEAD / HTTP/1.0

enter/return
twice

C:\WINDOWS\system32\cmd.exe

```
HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://192.168.1.10/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 18:48:30 GMT
Accept-Ranges: bytes
ETag: "8938ad3d9d9c21:33a"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 22 Oct 2005 23:15:43 GMT
Connection: close
```

SuperScan 4 Tool: Banner Grabbing



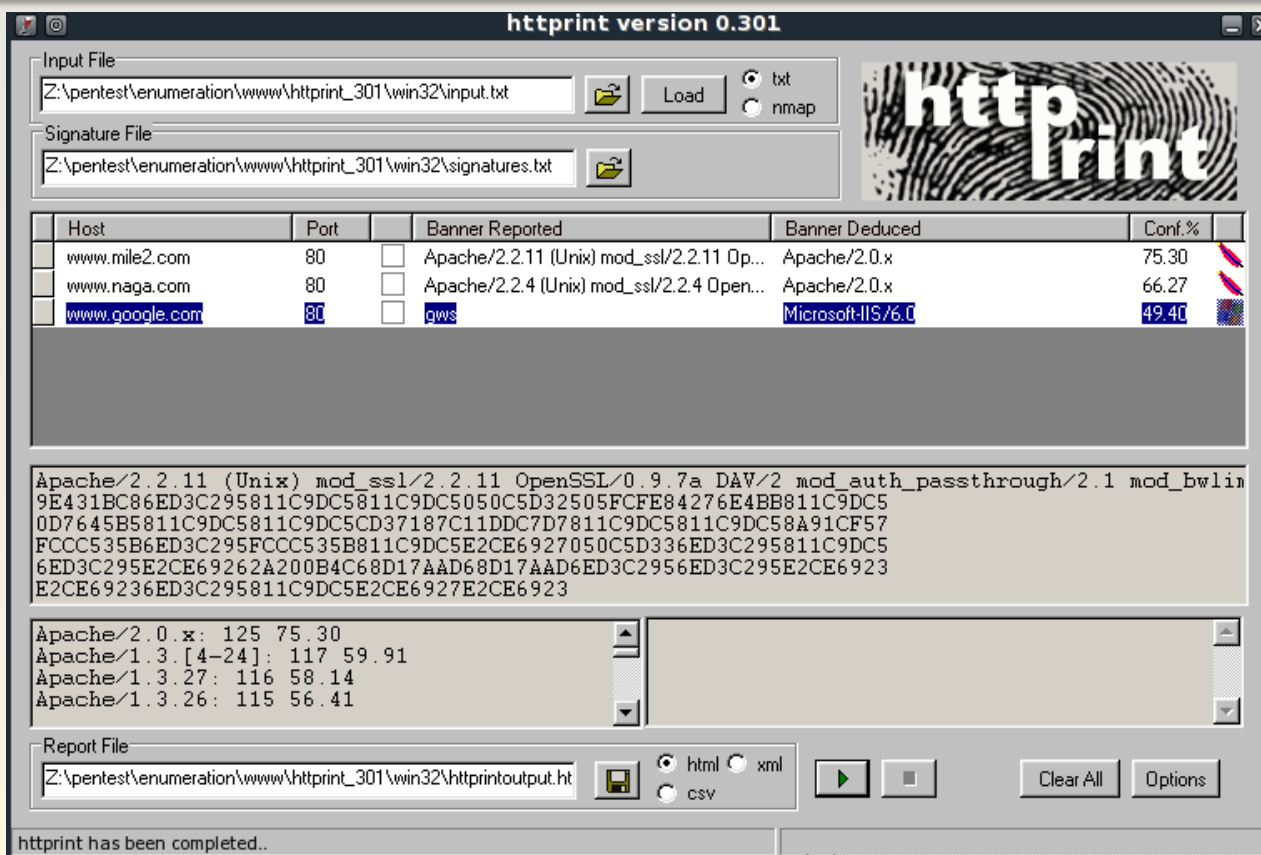
**Using the HTTP HEAD Request
against a Windows 2003 IIS 6 Server**

HTTPrint

Windows and Linux

Command Line and GUI

httpprint is a web server fingerprinting tool.



SMTP Server Banner

SMTP banners can be retrieved using the command:

```
telnet <email_server> 25
```



The expected response is a banner from the SMTP server stating what software version it is running.

```
C:\ Telnet 192.168.1.100
220 win2k.ceh.com Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at Fri, 20 Aug 2004 06:13:51 +0100
```

```
220 et-dfw-10.site.stayonline.net ESMTP Sendmail 8.12.6/8.12.6; Fri, 20 Aug 2004 05:10:52 GMT
500 5.5.1 Command unrecognized: ""
```

DNS Enumeration

Any DNS server that is accessible from the Internet can be queried and tell a hacker about server names and IP addresses.



If the DNS server contains records for not only the DMZ servers, but also internal servers, this is a security hole. If the hacker is able to determine internal machine names, the hacker can then find out the machine's IP addresses.



Countermeasure: Have separate internal and external DNS servers.

```
C:\WINDOWS>nslookup physics.ucsd.edu
Server:  ns1.sd.cox.net
Address:  68.6.16.30

Non-authoritative answer:
Name:     physics.ucsd.edu
Address:  132.239.69.26

C:\WINDOWS>_
```



Zone Transfers from Windows 2000 DNS

The default setting on Windows 2000 DNS Servers allow for zone transfers to ANY other machine. Thus, a hacker/pen tester can use nslookup to do a zone transfer of all of the records in a domain.

```
C:\WINNT\System32\cmd.exe - nslookup

C:\>nslookup
Default Server:  w2kinstructor0.acme.com
Address:  192.168.1.202

> ls -d acme.com
[w2kinstructor0.acme.com]
acme.com.                SOA      w2kinstructor0.acme.com administrator. (4
3 900 600 86400 3600)
acme.com.                A        192.168.1.202
acme.com.                NS       w2kinstructor0.acme.com
4805edcc-ba26-42c1-b638-723e0ea8d6f4._msdcs CNAME   w2kinstructor0.acme.com
_kerberos._tcp.default-first-site-name._sites.dc._msdcs SRV      priority=0, weig
ht=100, port=88, w2kinstructor0.acme.com
_ldap._tcp.default-first-site-name._sites.dc._msdcs SRV      priority=0, weight=1
00, port=389, w2kinstructor0.acme.com
_kerberos._tcp.dc._msdcs SRV      priority=0, weight=100, port=88, w2kinstr
uctor0.acme.com
_ldap._tcp.dc._msdcs     SRV      priority=0, weight=100, port=389, w2kinst
ructor0.acme.com
_ldap._tcp.3be79dc6-6083-43e4-9ad7-6038ce322512.domains._msdcs SRV      priority=
```

Backtrack

- **dns-bruteforce**
- **dnswalk**
- **dnsenum**
- **fierce**
- **list-urls**

```
bt fierce # fierce.pl --help
```

```
fierce.pl (C) Copyright 2006,2007 - By RSnake at http://ha.ckers.org/fierce/
```

```
Usage: perl fierce.pl [-dns example.com] [OPTIONS]
```



Countermeasure: DNS Zone Transfers

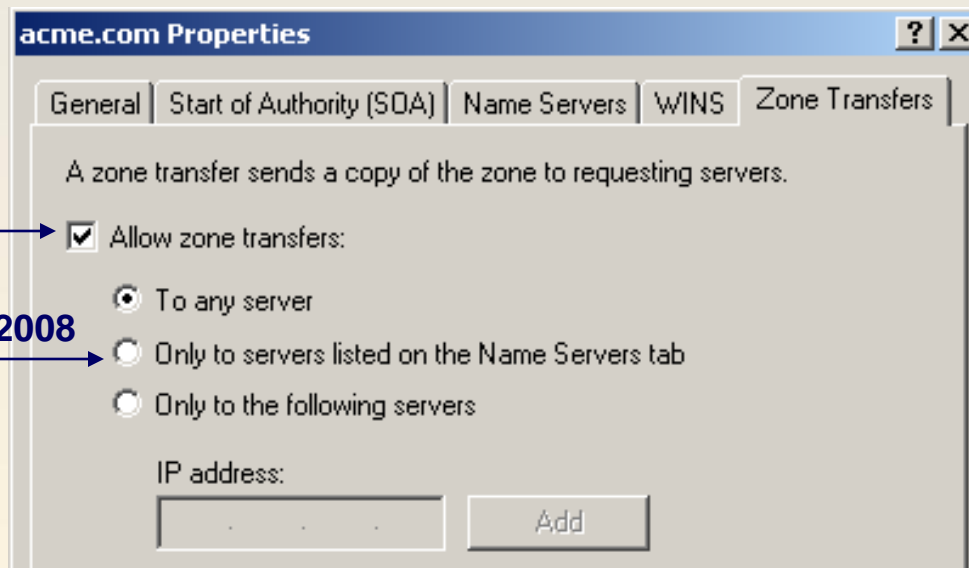
To prevent zone transfers from going to any machine, do the following on the Windows 2000 DNS Server:

Obtain the properties of the zone (using the DNS snap-in)

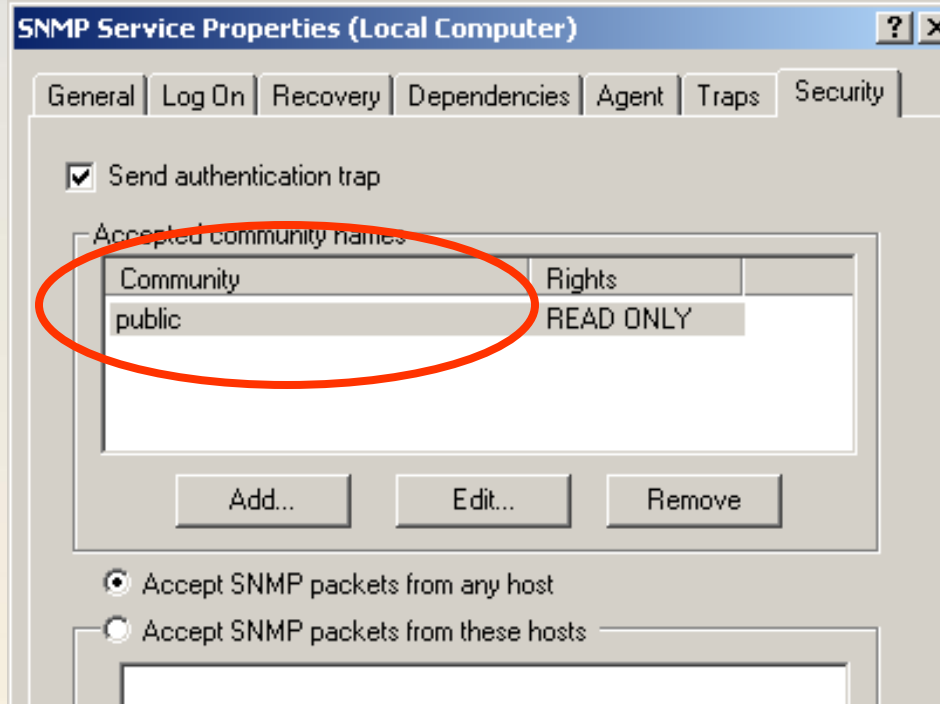
On the Zone Transfers tab, select a more restrictive setting.

W2K

Win2003 and 2008



SNMP Insecurity



SNMP is used to remotely manage TCP/IP devices.

There are two security issues with SNMP version 1 & 2:

The community string is sent in clear text.

The community string is often set to a default of "public".

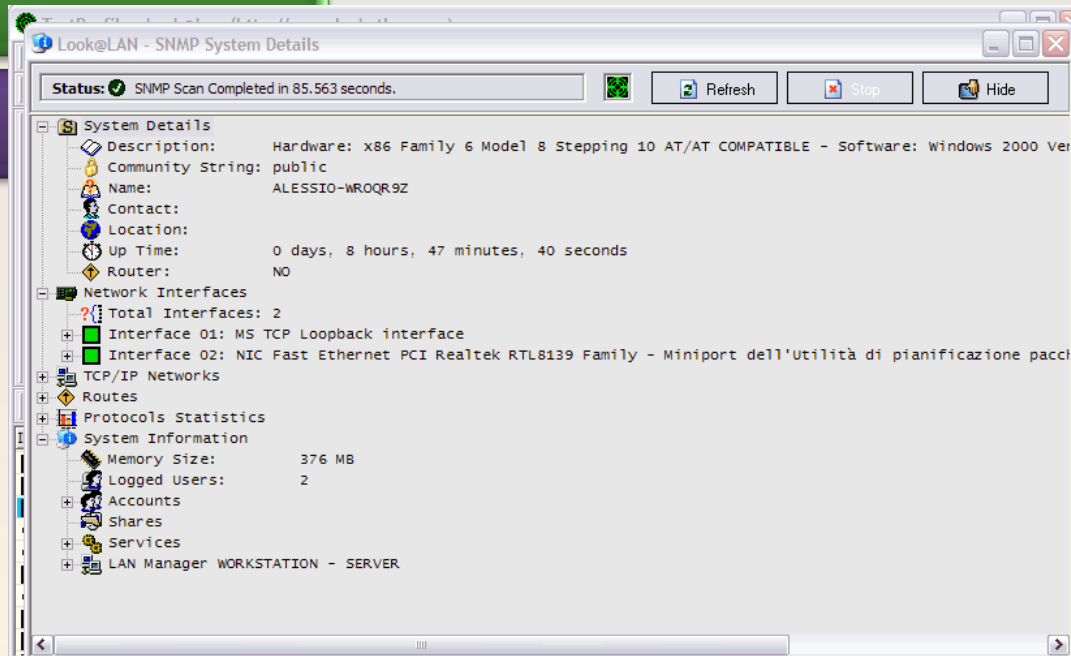
SNMP Enumeration Tools

Look@LAN

snmpenum.pl

Mibble :: MIB Parser

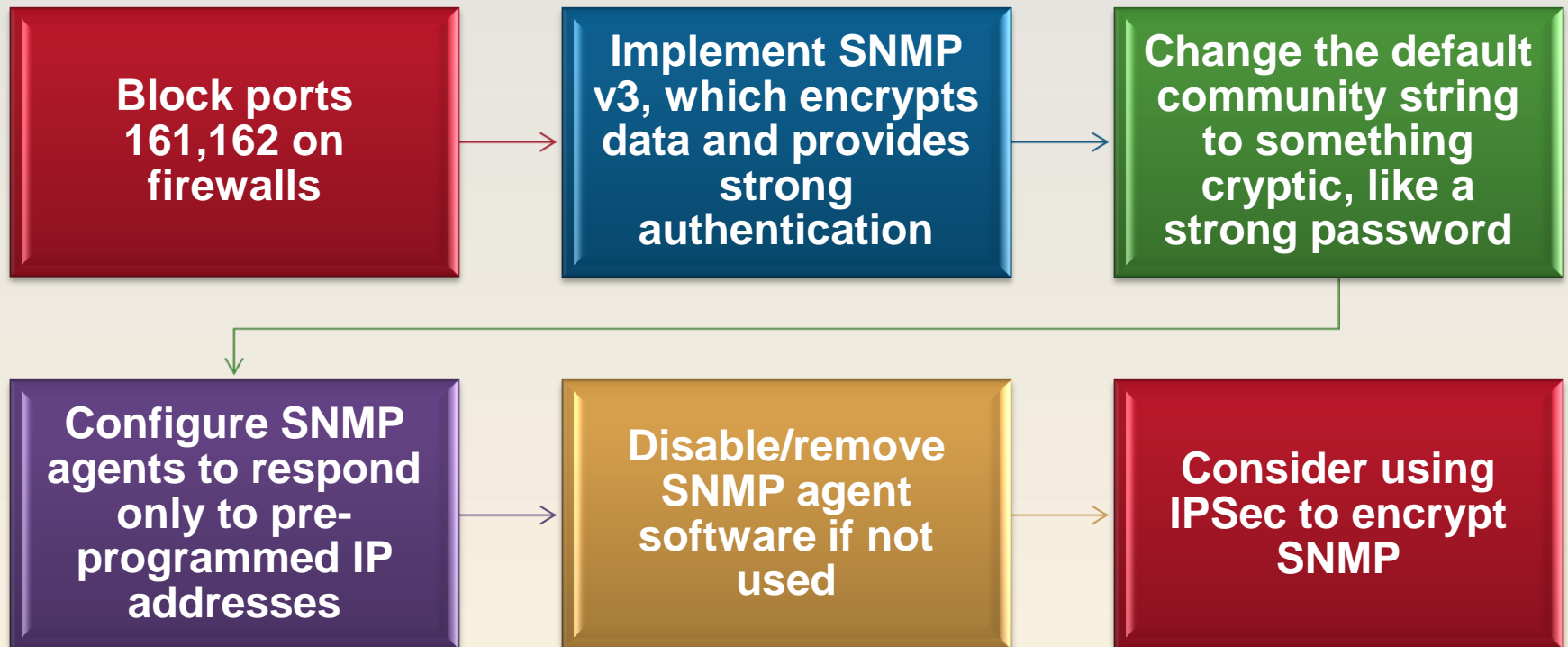
SolarWinds MIB Browser



```
bt snmpenum # snmpenum.pl --help
```

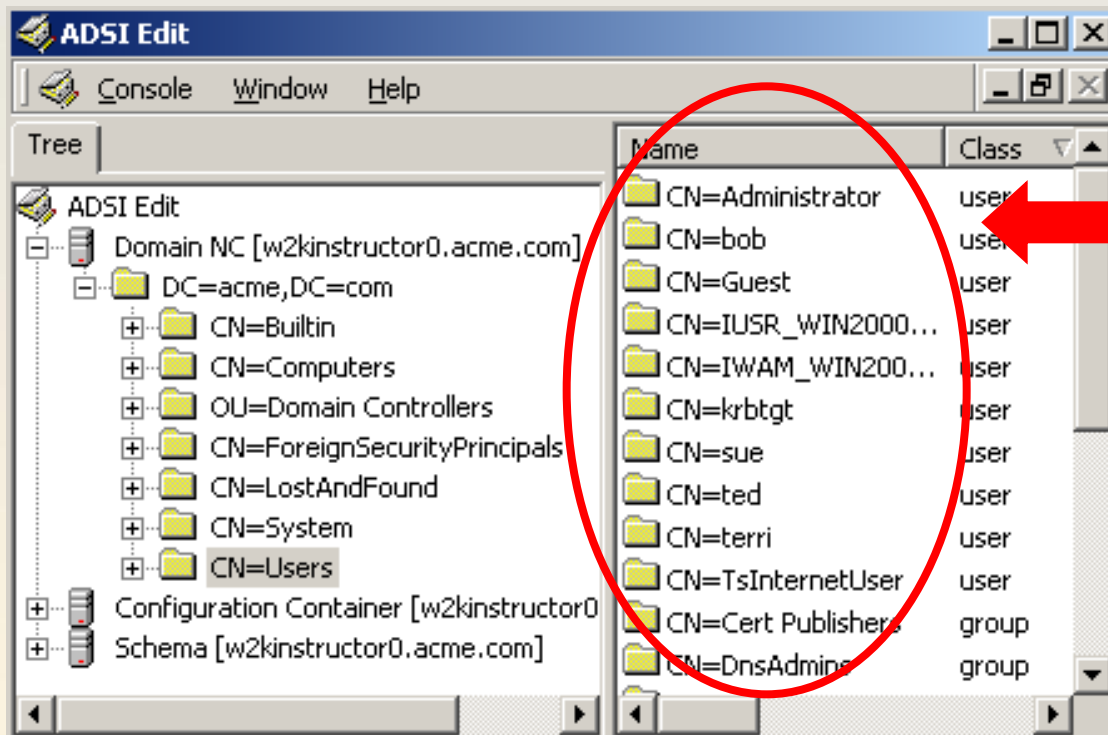
```
Usage: perl enum.pl <IP-address> <community> <configfile>
```

SNMP Enumeration Countermeasures



Active Directory Enumeration

Windows 2000/2003 Active Directory is accessed using Lightweight Directory Access Protocol (LDAP). LDAP uses the X.500 naming scheme for objects in the directory. This naming scheme uses Distinguished Names (DN) to identify objects in the directory.



List of domain users, located using DN of: CN=users, DC=acme, DC=com

LdapMiner is a tool that collects information from different LDAP Server implementations.

Note: Anonymous queries will fail if LDAP NULL BASE queries are disabled.

Usage:

- **ldapminer.exe -h host option**
- **-p [port] : default to 389**
- **-B [bind dn] : user. default null**
- **-w [password] : user password. default null**
- **-b [base search] : base for searching for user, group, ...**
- **-F [output format] : 0 for ldif, 1 for clean**
- **-d : dump all data you can grab**

AD Enumeration countermeasures

Block ports 389 (ldap), 3268 (global catalog) on firewalls



Remove the Everyone group from “Pre-Windows 2000 Compatible Access Group”. This “pre-Windows 2000” group by default has read permission on all objects in the AD database.



If you need to protect against internal employees, set OU permissions such that users in other OUs cannot read, i.e., remove Authenticated Users: Read permission. This will limit the information they can retrieve.



Null sessions

Windows NT and higher support “Null Sessions”, which are an anonymous connection allowed to retrieve certain information such as usernames, groups, shares, and services.



NULL sessions take advantage of “features” in the SMB (Server Message Block) protocol that exist for:

- Trusted domains to enumerate resources
- External computers to authenticate and enumerate users
- The SYSTEM account to authenticate and enumerate resources



Port 139 or 445 TCP is required to be open in order for a NULL session to be successful (it needs to connect to IPC\$ first).

Syntax for a Null Session

```
cmd.exe

C:\>net use \\10.1.1.201\ipc$ "" /u:""
The command completed successfully.

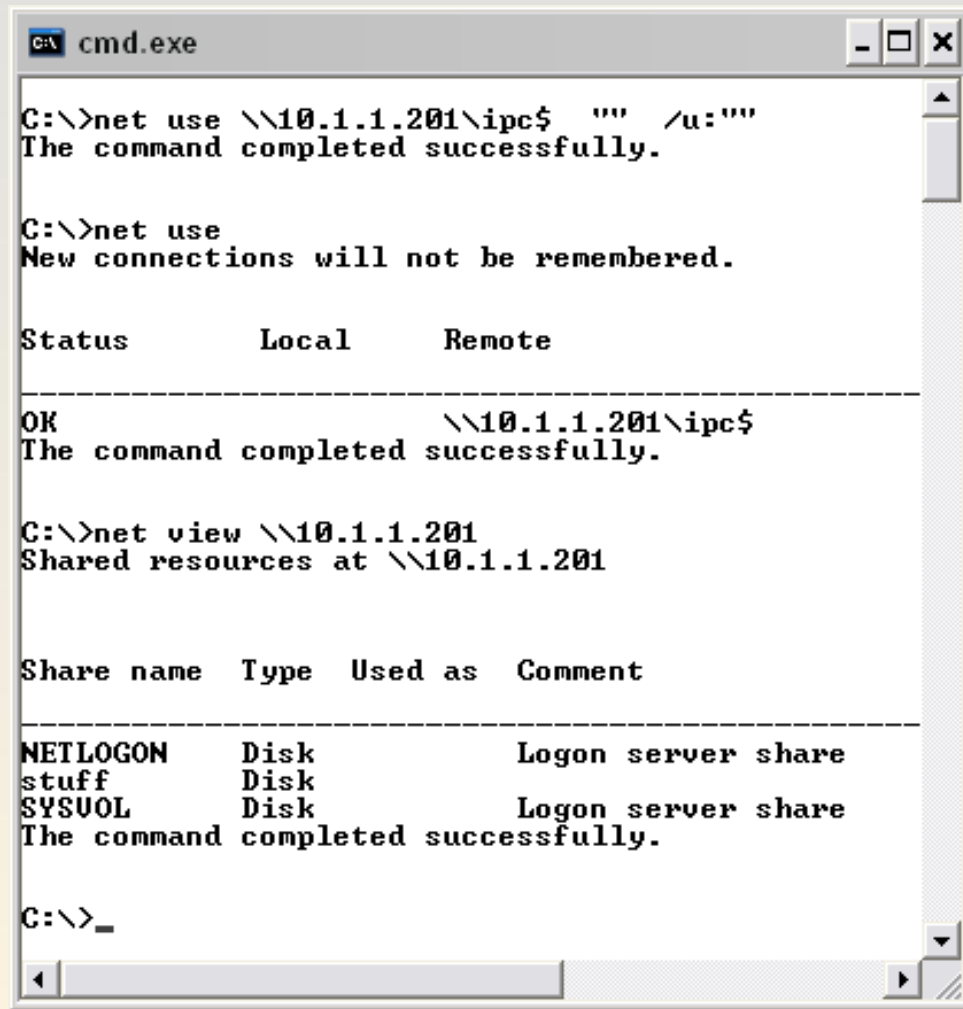
C:\>net use
New connections will not be remembered.

Status          Local          Remote          Network
-----
OK              \\10.1.1.201\ipc$  Microsoft Windows Network
The command completed successfully.

C:\>
```

The above syntax connects to the hidden Inter-Process Communication share (IPC\$) at IP address 10.1.1.201 with the built-in anonymous user (/u:"") and a null password ("").

Viewing Shares



```
C:\>net use \\10.1.1.201\ipc$ "" /u:""
The command completed successfully.

C:\>net use
New connections will not be remembered.

Status          Local          Remote
-----
OK               \\10.1.1.201\ipc$
The command completed successfully.

C:\>net view \\10.1.1.201
Shared resources at \\10.1.1.201

Share name      Type    Used as    Comment
-----
NETLOGON        Disk    Logon server share
stuff           Disk
SYSVOL          Disk    Logon server share
The command completed successfully.

C:\>_
```

Once a null session is established, a list of shares, users, and groups can be obtained – all without authentication!



Shown here is a null session to 10.1.1.201, and a list of the shares on that machine.




There are many tools that use the null session to retrieve information from the target machine.

Tool: DumpSec

DumpSec is a tool that can retrieve information from a target machine to which there is a null session.



Shown here is a list of usernames and SIDs pulled from the remote Windows 2000 server at 10.1.1.201

 **Somarsoft DumpSec (formerly DumpAcl) - \10.1.1.201**

File Edit Search Report View Help

UserName	Sid
Administrator	S-1-5-21-2025429265-1659004503-725345543-500
bob	S-1-5-21-2025429265-1659004503-725345543-1003
Guest	S-1-5-21-2025429265-1659004503-725345543-501
IUSR_WIN2000SERVER	S-1-5-21-2025429265-1659004503-725345543-1001
IWM WIN2000SERVER	S-1-5-21-2025429265-1659004503-725345543-1002
krbtgt	S-1-5-21-2025429265-1659004503-725345543-502
sue	S-1-5-21-2025429265-1659004503-725345543-1005
ted	S-1-5-21-2025429265-1659004503-725345543-1004
terri	S-1-5-21-2025429265-1659004503-725345543-1006
TsInternetUser	S-1-5-21-2025429265-1659004503-725345543-1000

00010

Tool: Enumeration with Cain and Abel

Create a NULL session to the class 2000 and 2003 Server, then use C&A to enumerate

The screenshot shows the Cain v2.5 beta58 interface. The left pane displays the network tree with '10.1.1.201' selected under 'Quick List'. The right pane shows a table of enumeration results for this IP address.

User	SID	Pass Required
Administrator	S-1-5-21-2025429265-1659004503-...	No
Guest	S-1-5-21-2025429265-1659004503-...	Yes
krbtgt	S-1-5-21-2025429265-1659004503-...	No
TsInternetUser	S-1-5-21-2025429265-1659004503-...	No
IUSR_WIN20...	S-1-5-21-2025429265-1659004503-...	No
IWAM_WIN2...	S-1-5-21-2025429265-1659004503-...	No
bob	S-1-5-21-2025429265-1659004503-...	No
ted	S-1-5-21-2025429265-1659004503-...	No
sue	S-1-5-21-2025429265-1659004503-...	No
terri	S-1-5-21-2025429265-1659004503-...	No

The interface also shows a 'Protected Storage' tab selected in the top bar. The bottom status bar indicates 'Cain v2.5 beta58 by mao'.

Cain connects anonymously to retrieve groups, services, shares and users. Even basic enumeration on a 2003 Server

NAT Dictionary Attack Tool

Purpose is to dictionary attack SMB shares:

Once you have an Admin account password, you own the box.

Usage: nat [-o filename] [-u userlist] [-p passlist] <address>

```
C:\nat>nat -o demo.txt -u USERLIST.TXT -p PASSLIST.TXT 192.168.1.190
[*]--- Reading usernames from USERLIST.TXT
[*]--- Reading passwords from PASSLIST.TXT

[*]--- Checking host: 192.168.1.190
[*]--- Obtaining list of remote NetBIOS names

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Mon Jul 02 04:42:54 2007
[*]--- Timezone is UTC+1.0
[*]--- Remote server wants us to encrypt, telling it not to

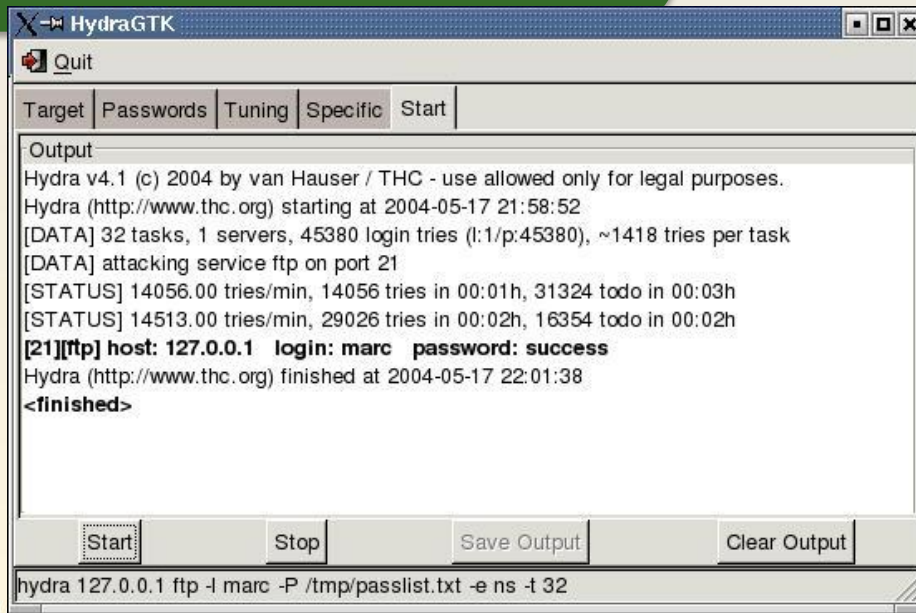
[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'ADMINISTRATOR'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'GUEST'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'ROOT'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'ADMIN'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'PASSWORD'
[*]--- CONNECTED: Username: 'ADMINISTRATOR' Password: 'PASSWORD'
```



THC-Hydra

A very fast network logon cracker which supports many different services

Currently this tool supports: TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC, RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, LDAP2, Cisco AAA (incorporated in telnet module).



The screenshot shows the HydraGTK application window. The title bar reads 'HydraGTK'. Below the title bar is a menu bar with 'Quit'. Below the menu bar is a tabbed interface with tabs for 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Output' tab is selected, displaying the following text:

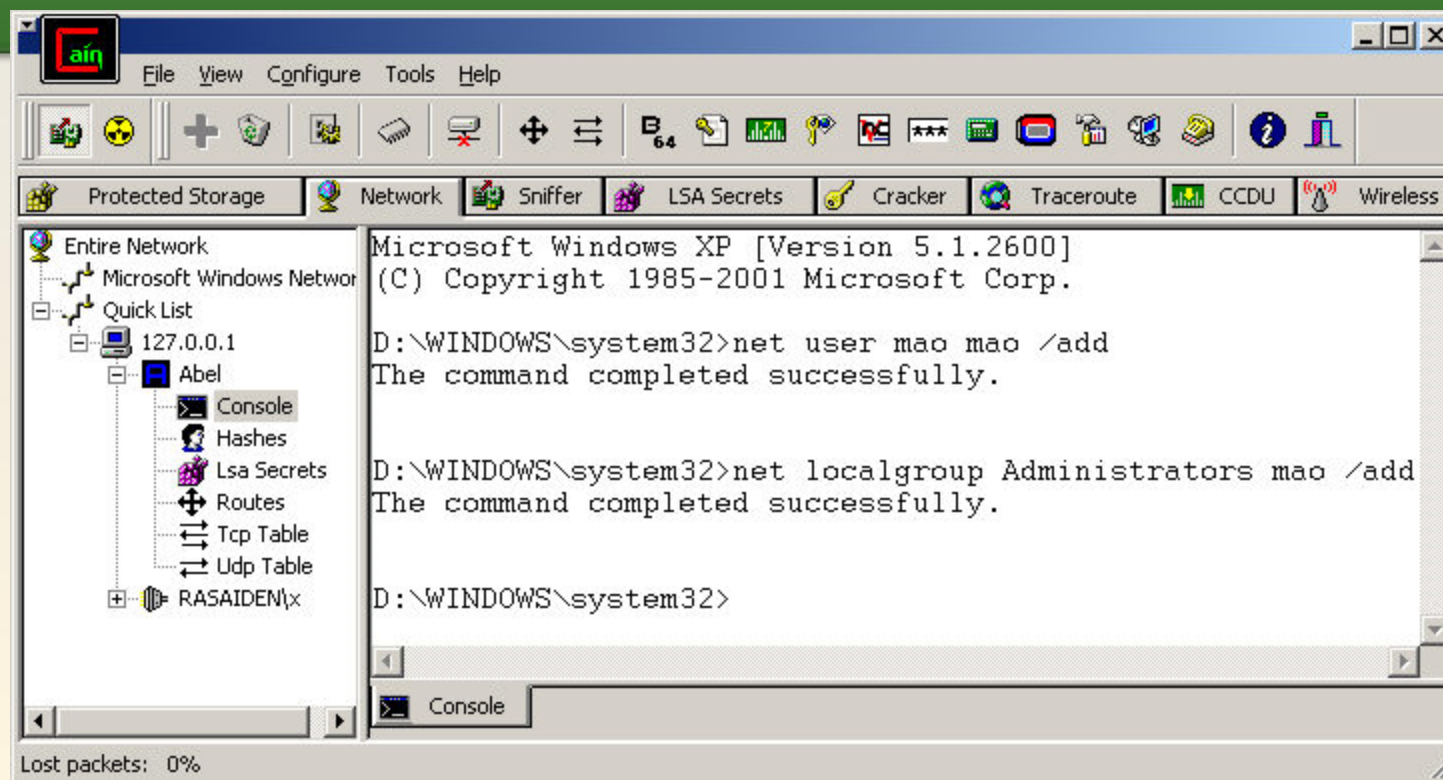
```
Output
Hydra v4.1 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2004-05-17 21:58:52
[DATA] 32 tasks, 1 servers, 45380 login tries (l:1/p:45380), ~1418 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 14056.00 tries/min, 14056 tries in 00:01h, 31324 todo in 00:03h
[STATUS] 14513.00 tries/min, 29026 tries in 00:02h, 16354 todo in 00:02h
[21][ftp] host: 127.0.0.1 login: marc password: success
Hydra (http://www.thc.org) finished at 2004-05-17 22:01:38
<finished>
```

At the bottom of the window are four buttons: 'Start', 'Stop', 'Save Output', and 'Clear Output'. Below the buttons is a command line showing the command used to run the tool:

```
hydra 127.0.0.1 ftp -l marc -P /tmp/passlist.txt -e ns -t 32
```


Injecting Abel Service

By injecting the Abel Service you can: add users, enumerate networks, ping remote hosts, map network drives, dump LSA secrets, grab password hashes, view/modify TCP/UDP connection parameters, view/edit route table, and so on
.... every command is executed on the Abel-side.



Null Session Countermeasures

Block the following ports at the firewall:

135
RPC locator

137
WINS

138
NetBIOS
datagram
service

139
mapped
drives

445
CIFS/SMB

Disable the Server service (called “File & Printer Sharing” in TCP/IP properties)

Never have ANY blank passwords for any accounts; always use strong passwords

Configure the registry settings (if in a workgroup) or associated group policies (if in a domain) as shown on the next slide.

In Windows 2000:

- registry value:
HKLM\System\CCS\Control\LSA\RestrictAnonymous
or
- group policy: Local Policies->Security Options->Additional restrictions for anonymous connections
- set to:
- “Do not allow enumeration of SAM accounts” (registry value=1)
- “No access without explicit permission” (registry value=2)

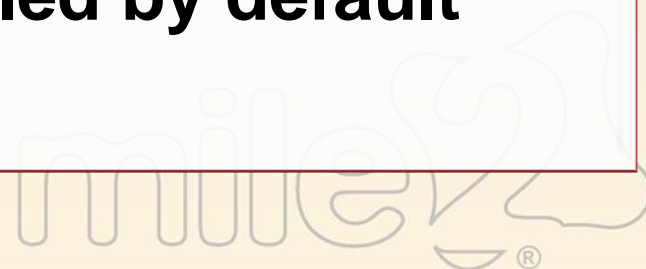


Setting RestrictAnonymous key = 1 is not recommended, as several tools (Enum, GetAcct) can still obtain lists of users and SIDs through other means!



In Windows XP/2003

- **group policy:**
Local Policies->Security Options->
Network Access:
“do not allow enumeration of SAM
accounts and shares”
 - **set to: enabled**
- **This will restrict enumerating shares, all**
other restrictions are enabled by default



Enumeration is the process of obtaining information from computer systems without having to login to those systems.

Information that can be gained by enumeration:

- **Banners from FTP servers, web servers, email servers**
- **FQDNs and IP addresses**
- **IP configuration of routers and servers**
- **Information from Active Directory**
- **Usernames**
- **Share names**

Remember Cain and Abel can bypass Windows 2003 enumeration

Module 5 Lab Enumeration

