



Hands-On Ethical Hacking and Network Defense

Chapter 6 Enumeration

Modified 2-22-14

Objectives

- Describe the enumeration step of security testing
- Enumerate Microsoft OS targets
- Enumerate NetWare OS targets
- Enumerate *NIX OS targets

Introduction to Enumeration

- Enumeration extracts information about:
 - Resources or shares on the network
 - User names or groups assigned on the network
 - Last time user logged on
 - User's password
- Before enumeration, you use Port scanning and footprinting
 - To Determine OS being used
- Intrusive process

NBTscan

- NBT (NetBIOS over TCP/IP)
 - is the Windows networking protocol
 - used for shared folders and printers
- NBTscan
 - Tool for enumerating Microsoft OSs

```
yourname@S214-01u:~$ nbtscan 192.168.2.1-254
Doing NBT name scan for addresses from 192.168.2.1-254
```

IP address	NetBIOS Name	Server	User	MAC address

192.168.2.30	RICKHP	<server>	<unknown>	00:40:2b:66:78:80
192.168.2.14	SAMP4	<server>	<unknown>	00:10:b5:0e:5c:8a
192.168.2.22	SAM_LAPTOP		SAM_LAPTOP	00:10:60:03:b6:bf
192.168.2.222	SAM2G	<server>	<unknown>	00:30:48:82:11:bd

Enumerating Microsoft Operating Systems

- Study OS history
 - Knowing your target makes your job easier
 - Many attacks that work for older Windows OSs still work with newer versions

Windows 95

- The first Windows version that did not start with DOS
- Still used the DOS kernel to some extent
- Introduced the Registry database to replace Win.ini, Autoexec.bat, and other text files
- Introduced Plug and Play and ActiveX
- Used FAT16 file system

Windows 98 and ME

- More Stable than Win 95
- Used FAT32 file system
- Win ME introduced System Restore
- Win 95, 98, and ME are collectively called "Win 9x"

TSA Carry-On Baggage Scanners Easy To Hack

- They run Windows 98
- Use plaintext passwords
 - Research from Billy K Rios, published 2-11-14

Windows NT 3.51 Server/Workstation

- No dependence on DOS kernel
- Domains and Domain Controllers
- NTFS File System to replace FAT16 and FAT32
- Much more secure and stable than Win9x
- Many companies still use Win NT Server Domain Controllers
- Win NT 4.0 was an upgrade

Windows 2000 Server/Professional

- Upgrade of Win NT
- Active Directory
 - Powerful database storing information about all objects in a network
 - Users, printers, servers, etc.
 - Based on Novell's Novell Directory Services
- Enumerating this system would include enumerating Active Directory

Windows XP Professional

- Much more secure, especially after Service Pack 2
 - Windows File Protection
 - Data Execution Prevention
 - Windows Firewall

Bill Gates: Trustworthy Computing

Bill Gates  01.17.02

This is the e-mail Bill Gates sent to every full-time employee at Microsoft, in which he describes the company's new strategy emphasizing security in its products.

From: Bill Gates

Sent: Tuesday, January 15, 2002 5:22 PM

To: Microsoft and Subsidiaries: All FTE

Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing -- or able -- to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

- Link Ch 6n

Windows Server 2003

- Much more secure, especially after Service Pack 1
 - Network services are closed by default
 - Internet Explorer security set higher

Windows Vista

- User Account Control
 - Users log in with low privileges for most tasks
- BitLocker Drive Encryption
- Address Space Layout Randomization (ASLR)

ASLR Demo

- Download Process Explorer (link Ch 3e)
- View, Show Lower Pane
- View, Lower Pane View, DLLS
- View, Select Columns, DLL tab, Base Address
- Select explorer.exe and find ntdll.dll
- Reboot to see base address change

ASLR on Windows 7

Process Explorer - Sysinternals: www.sysinternals.com [WIN-CVTTKBE78BP\student]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
explorer.exe	0.03	57,876 K	83,924 K	1496	Windows Explorer	Microsoft Corporation
vmware-toolsd.exe	0.18	14,768 K	25,844 K	1720	VMware Tools Core Service	VMware, Inc.
jusched.exe		3,652 K	11,796 K	1752	Java(TM) Update Scheduler	Sun Microsystems, Inc.
procexp.exe	4.21	11,108 K	21,308 K	3068	Sysinternals Process Explorer	Sysinternals - www.sysinter...

Name	Description	Company Name	Path	Base
NppShell_05.dll	ShellHandler for Notepad++		C:\Program Files\Notepad++\NppShel...	0x6BB0000
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation	C:\Windows\System32\nsi.dll	0x76990000
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll	0x76DB0000
ntdsapi.dll	Active Directory Domain Services ...	Microsoft Corporation	C:\Windows\System32\ntdsapi.dll	0x734E0000

Process Explorer - Sysinternals: www.sysinternals.com [WIN-CVTTKBE78BP\student]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
winlogon.exe		1,832 K	5,508 K	436		
explorer.exe	0.04	29,512 K	45,456 K	1492	Windows Explorer	Microsoft Corporation
vmware-toolsd.exe	0.29	11,716 K	21,748 K	1660	VMware Tools Core Service	VMware, Inc.
AdobeARM.exe	0.49	1,804 K	7,848 K	1668	Adobe Reader and Acrobat	Adobe Systems Incorporated

Name	Description	Company Name	Path	Base
npmproxy.dll	Network List Manager Proxy	Microsoft Corporation	C:\Windows\System32\npmproxy.dll	0x74560000
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation	C:\Windows\System32\nsi.dll	0x761D0000
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll	0x77D40000
ntlanman.dll	Microsoft® Lan Manager	Microsoft Corporation	C:\Windows\System32\ntlanman.dll	0x72930000

Windows Server 2008

- User Account Control
- BitLocker Drive Encryption
- ASLR
- Network Access Protection
 - Granular levels of network access based on a clients level of compliance with policy
- Server Core
 - Small, stripped-down server, like Linux
- Hyper-V
 - Virtual Machines

Windows 7

- XP Mode
 - A virtual machine running Win XP
- User Account Control was refined and made easier to use

Windows 8

- Built-in antivirus
- SmartScreen protects against phishing and social engineering by using a URL and application reputation system
- Windows 8 secure boot using EFI on ARM prevents rootkits

Windows 8.1

- Pass the Hash finally fixed, after 15 years!

Wed 2-26, 6:30, Chinatown Campus, 808 Kearny St., Fourth floor

Guest Speaker: Nathan Ide from Microsoft

Pass the Hash is a powerful attack hackers have been using to compromise Windows systems for 15 years. Microsoft finally patched it in Windows 8.1. (This is worth extra credit)

Presenting will be one of Microsoft's top security researchers, Nathan Ide who developed the "fix" at Microsoft.

NetBIOS Basics

- Network Basic Input Output System (NetBIOS)
 - Programming interface
 - Allows computer communication over a LAN
 - Used to share files and printers

NetBIOS names

- Computer names on Windows systems
- Limit of 16 characters
- Last character identifies type of service running
- Must be unique on a network

NetBIOS Suffixes

Table 6-2 NetBIOS names and suffixes

NetBIOS Name	Suffix	Description
<computer name>	00	The Workstation service registered the computer name (also referred to as the NetBIOS name).
<_MSBROWSE_>	01	Signifies that the computer is the master browser on the network. The master browser is responsible for notifying all computers on the network of any NetBIOS name changes or additions.
<computer name>	03	The computer is registered by the Messenger service, which the client uses when sending and receiving messages.
<computer name>	06	Registered by Routing and Remote Access Service (RRAS).
<computer name>	1F	Network Dynamic Data Exchange (NetDDE) services have been started on the computer. NetDDE is a system process that runs on Microsoft OSs to facilitate the exchange of network data.
<computer name>	20	Registered by the Server service. A computer must have this service running to share printers or files.

- For complete list, see link Ch 6h

NetBIOS Null Sessions

- Null session
 - Unauthenticated connection to a Windows computer
 - Does not use logon and passwords values
- Around for over a decade
 - Still present on Windows XP
 - Disabled on Server 2003
 - Absent entirely in Vista and later versions
- A large vulnerability
 - See links Ch 6a-f

Null Session Information

- 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 SIDs (Security Identifiers)
 - From brown.edu (link Ch 6b)

Demonstration of Null Sessions

- Start Win 2000 Pro
- Share a folder
- From a Win XP command prompt
 - **NET VIEW \\ip-address** Fails
 - **NET USE \\ip-address\IPC\$ "" /u:""**
 - Creates the null session
 - Username="" Password=""
 - **NET VIEW \\ip-address** Works now

Demonstration of Enumeration

- Download Winfo from link Ch 6g
- Run it – see all the information!

```
C:\Documents and Settings\SamLimited\Desktop>winfo 2.0 -c  
Winfo 2.0 - copyright (c) 1999-2003, Arne Vidstrom  
- http://www.ntsecurity.nu/toolbox/winfo  
  
Trying to establish null session...  
Null session established.  
  
SYSTEM INFORMATION:  
- OS version: 5.0  
DOMAIN INFORMATION:  
- Primary domain (legacy): WORKGROUP  
- Account domain: S214-i7-SAM2  
- Primary domain: WORKGROUP  
- DNS name for primary domain:  
- Forest DNS name for primary domain:  
  
PASSWORD POLICY:  
- Time between end of logon time and forced logon:  
- Maximum password age: 42 days  
- Minimum password age: 0 days  
- Password history length: 0 passwords  
- Minimum password length: 0 characters  
  
LOCKOUT POLICY:  
- Lockout duration: 30 minutes  
- Reset lockout counter after 30 minutes  
- Lockout threshold: 0  
  
SESSIONS:  
- Computer: 192.168.2.222  
- User:  
  
LOGGED IN USERS:  
* Administrator
```

NULL Session Information

- 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
 - From brown.edu (link Ch 6b)

NULL Sessions in Win XP and 2003 Server

- Windows XP and 2003 don't allow Null Sessions, according to link Ch 6c.
 - I tried the NET USE command on Win XP SP2 and it did not work
 - Link Ch 6f says you can still do it in Win XP SP2, but you need to use a different procedure

NetBIOS Enumeration Tools

- Nbtstat command
 - Powerful enumeration tool included with the Microsoft OS
 - Displays NetBIOS table

```
F:\Install\hacking>nbtstat -a 192.168.2.15
```

```
SAMCO:
```

```
NodeIpAddress: [192.168.2.14] Scope Id: []
```

NetBIOS Remote Machine Name Table

Name	Type	Status
S214-17-SAM2	<00>	UNIQUE
WORKGROUP	<00>	GROUP
S214-17-SAM2	<20>	UNIQUE
S214-17-SAM2	<03>	UNIQUE
WORKGROUP	<1E>	GROUP

```
MAC Address = 00-0C-29-3B-D9-BE
```

NetBIOS Enumeration Tools

- Net view command
 - Shows whether there are any shared resources on a network host

```
F:\Install\hacking>net view
Server Name          Remark
-----
\\RICKHP
\\S214-00
\\S214-17-SAM2
\\SAM2G
\\SAMP4
The command completed successfully.
```

```
F:\Install\hacking>net view 192.168.2.15
Shared resources at 192.168.2.15
```

Share name	Type	Used as	Comment
My Documents	Disk		The command completed successfully.

NetBIOS Enumeration Tools (continued)

- Net use command
 - Used to connect to a computer with shared folders or files

Additional Enumeration Tools

- Windows tools included with BackTrack
 - Smb4K tool
- DumpSec
- Hyena
- Nessus and OpenVAS

Using Windows Enumeration Tools

- Backtrack Smb4K tool
 - Used to enumerate Windows computers in a network

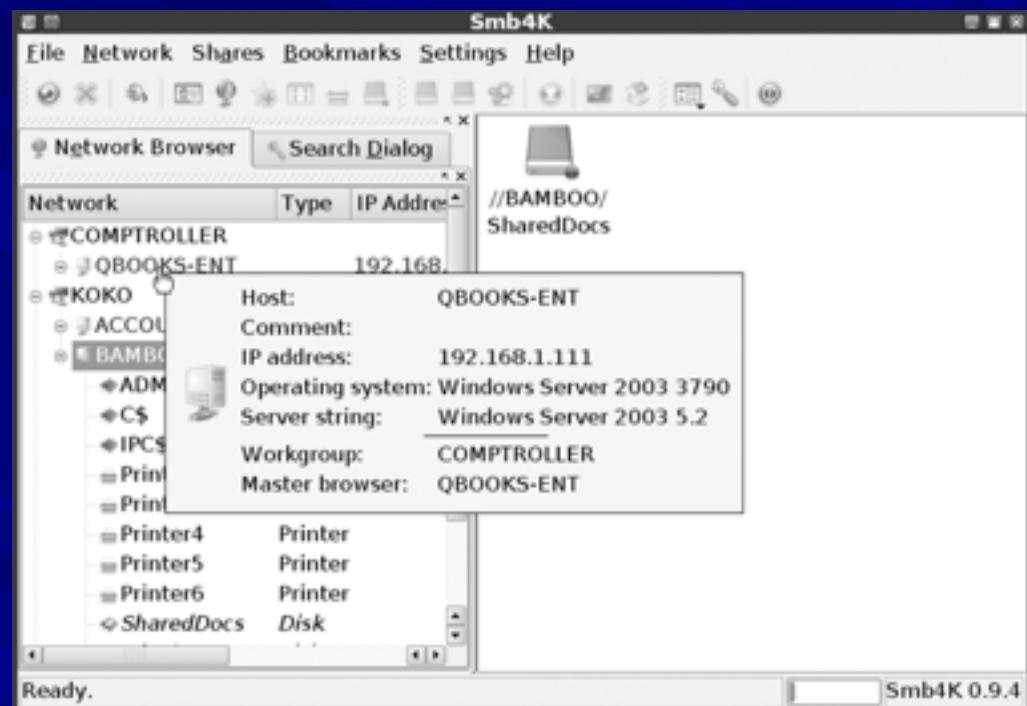


Figure 6-6 Using Smb4K on a Windows network

DumpSec

- Enumeration tool for Windows systems
 - Produced by Foundstone, Inc.
- Allows user to connect to a server and “dump”:
 - Permissions for shares
 - Permissions for printers
 - Permissions for the Registry
 - Users in column or table format
 - Policies
 - Rights
 - Services

Hyena

- Excellent GUI product for managing and securing Windows OSs
 - Shows shares and user logon names for Windows servers and domain controllers
 - Displays graphical representation of:
 - Microsoft Terminal Services
 - Microsoft Windows Network
 - Web Client Network
 - Find User/Group

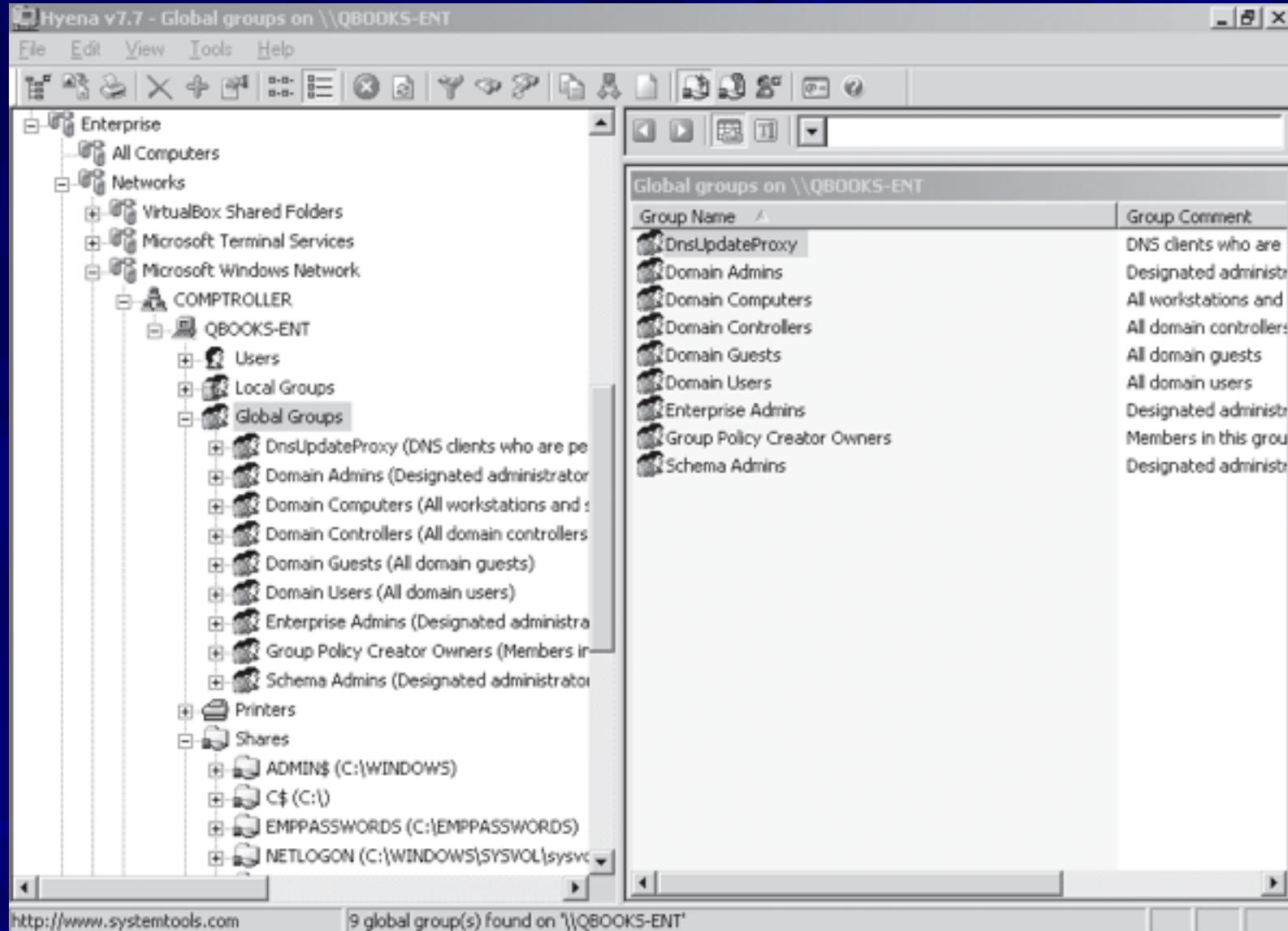


Figure 6-8 The Hyena interface

Nessus and OpenVAS

- OpenVAS
 - Operates in client/server mode
 - Open-source descendent of Nessus
 - Popular tool for identifying vulnerabilities
- Nessus Server and Client
 - Latest version can run on Windows, Mac OS X, FreeBSD, and most Linux distributions
 - Handy when enumerating different OSs on a large network
 - Many servers in different locations

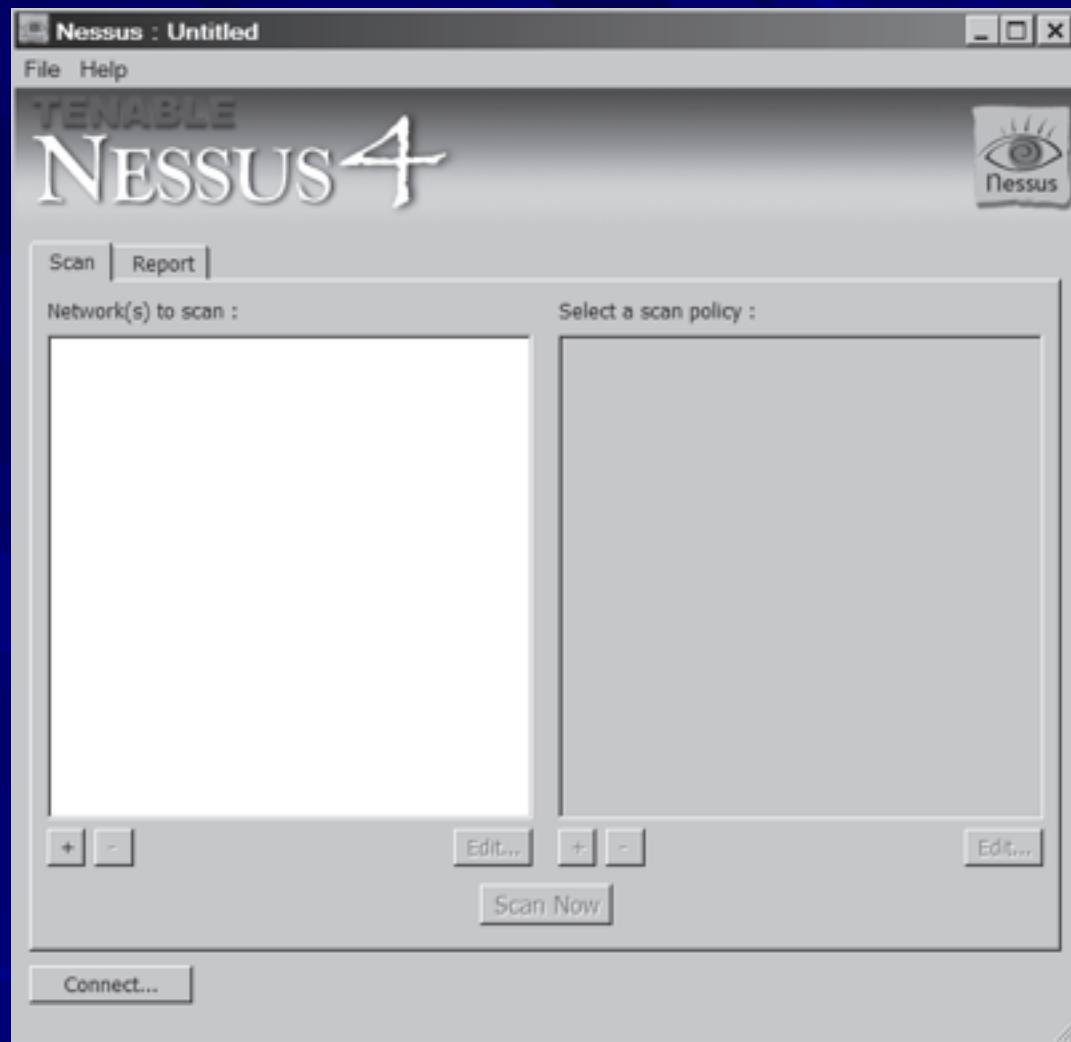


Figure 6-10 The Nessus session window

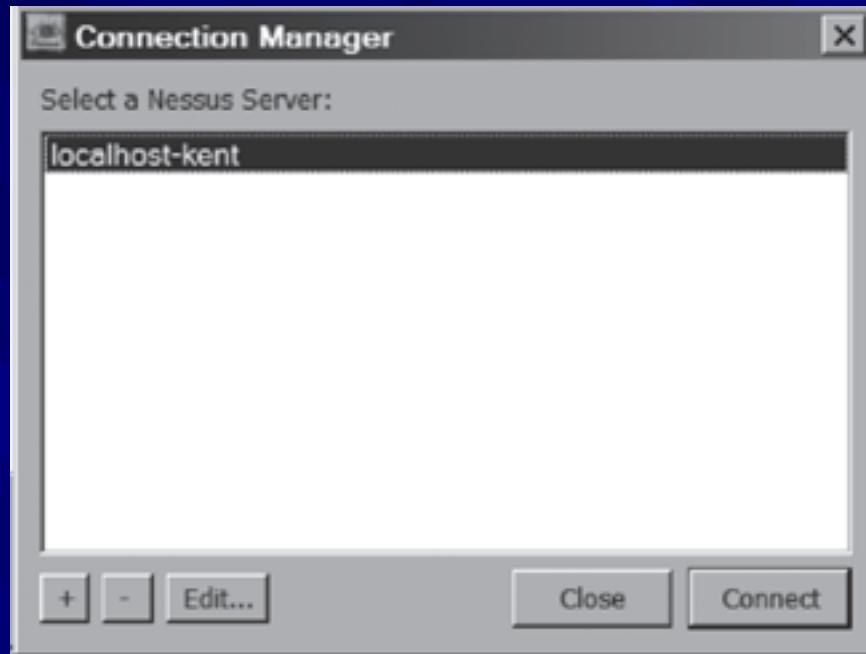


Figure 6-12 The Connection Manager dialog box

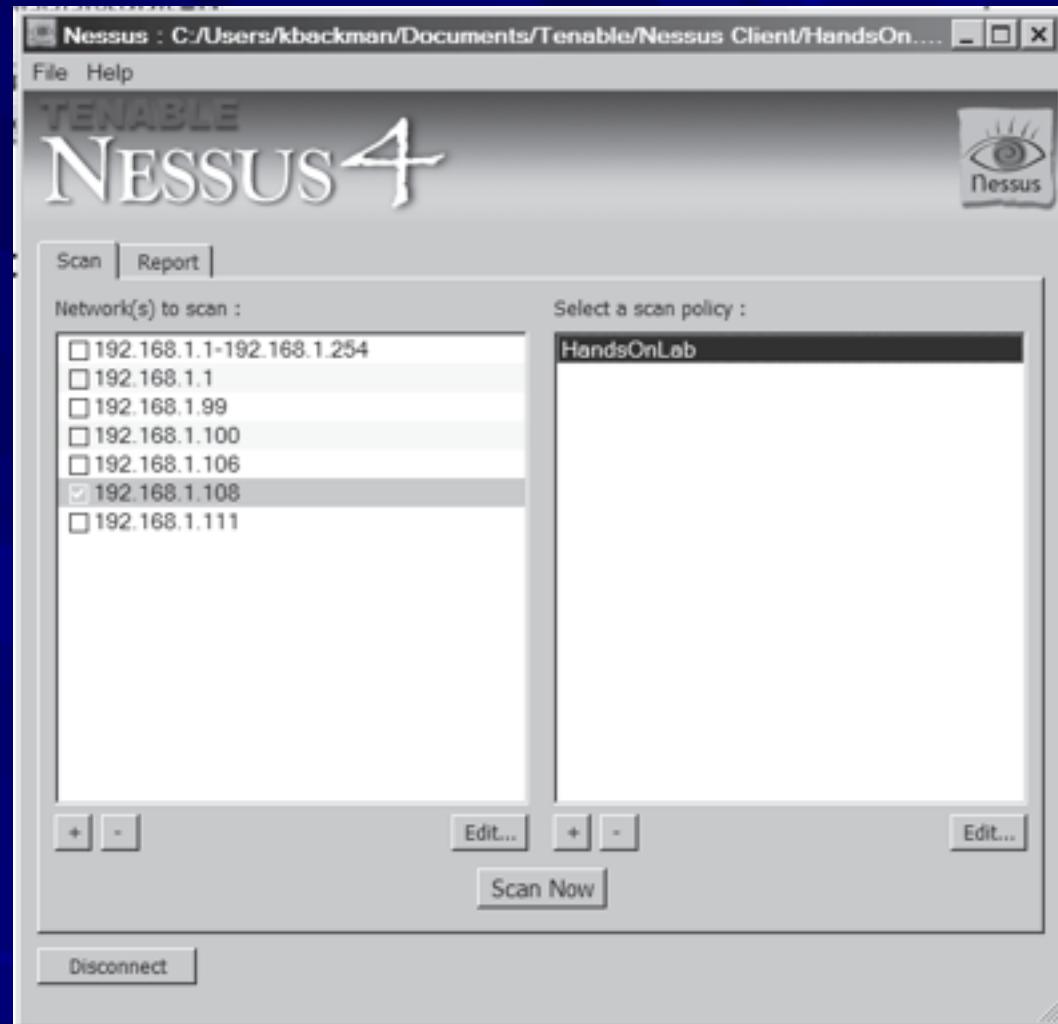


Figure 6-13 Nessus ready to scan

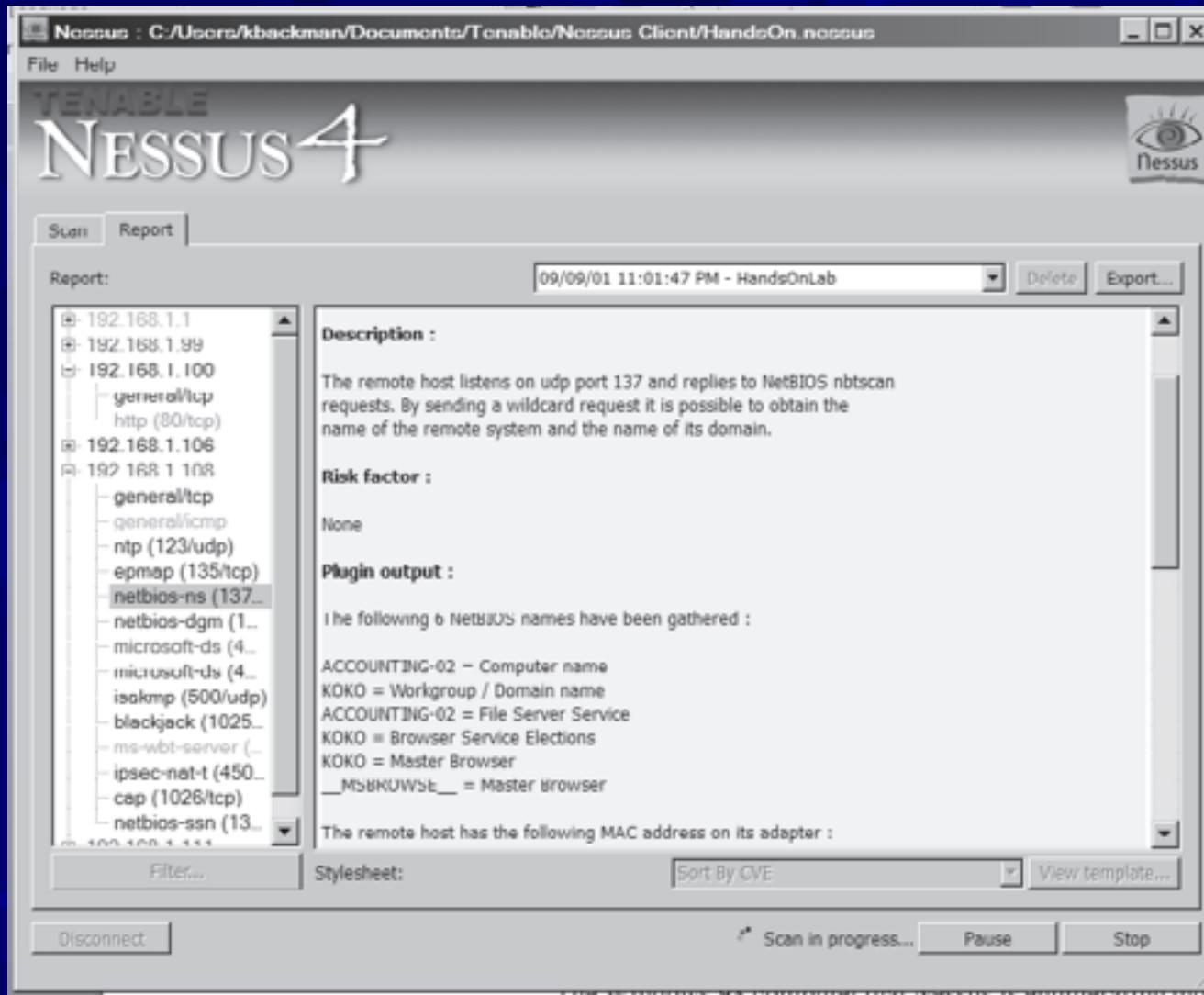


Figure 6-14 Nessus enumerates a NetBIOS system

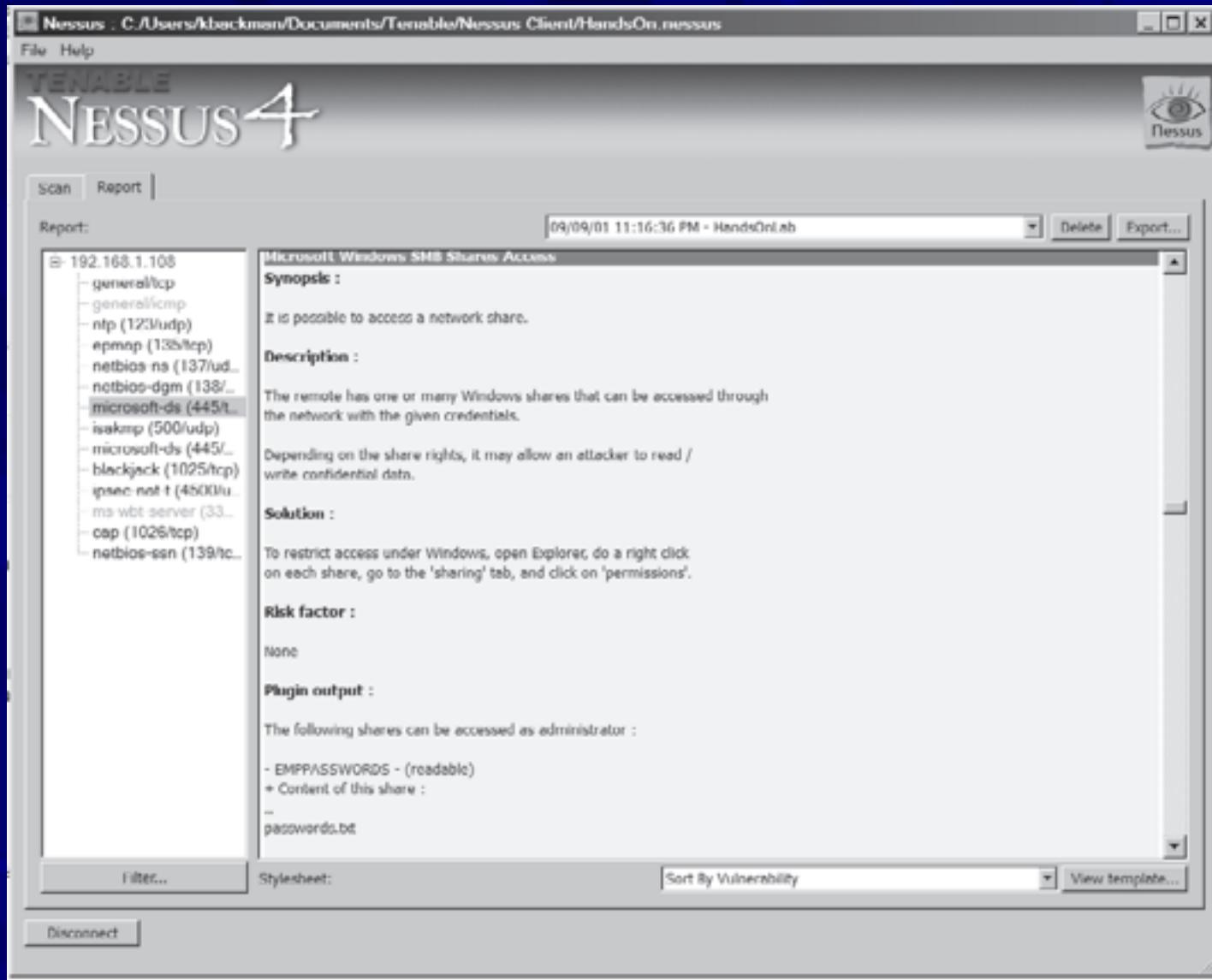


Figure 6-15 Enumerating shares in Nessus

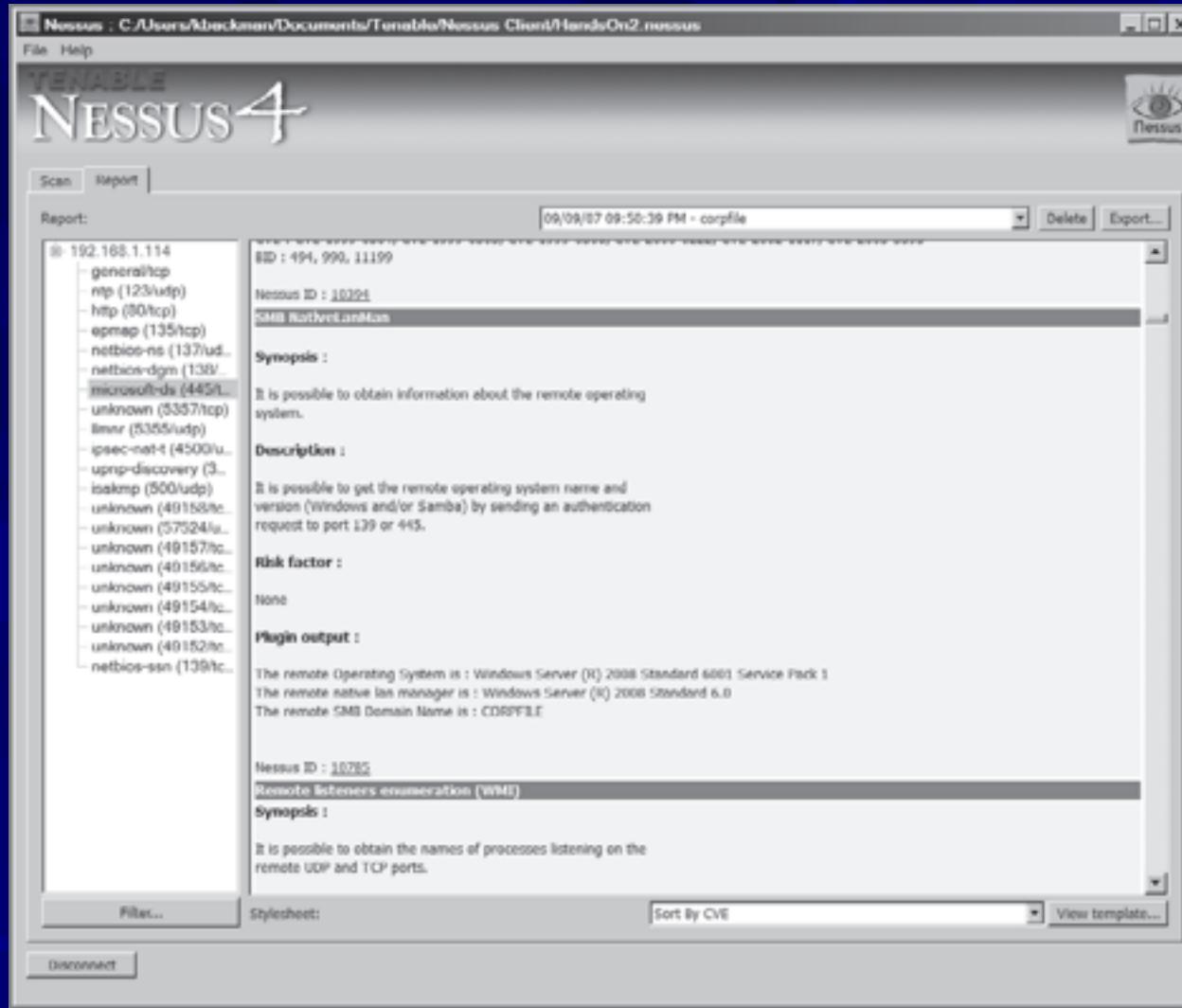


Figure 6-16 Nessus indicates the OS and service pack

Enumerating the NetWare Operating System

- Novell NetWare
 - Some security professionals see as a “dead” OS
 - Ignoring an OS can limit your career as a security professional
- NetWare
 - Novell does not offer any technical support for versions before 6.5

NetWare OS version	Description
NetWare 5.0	This version emphasized the use of a windowed environment instead of command-line utilities. In addition, TCP/IP replaced IPX/SPX as the default protocol.
NetWare 5.1	This version emphasized the Internet as an integral part of businesses. New features included IBM WebSphere Application Server; eDirectory (an enhancement of NDS); ConsoleOne, a graphical Java utility for centralized network administration; and the Novell Certificate Authority service, which enabled a server to issue digital certificates.
NetWare 6.0	This version offered more tools for accessing files and folders from remote Web browser clients, improved the eDirectory structure, and added Apache Web Server, Tomcat Servlet Engine, and NetWare Enterprise Web Server as part of the OS.
NetWare 6.5	This version, released on both NetWare and Linux kernels, improved Web access and included Web development and software development tools, such as MySQL and the PHP scripting language, to create dynamic Web pages. The latest NetWare version is 6.5 SP8, which is the same as Novell Open Enterprise Server 2 SP1, NetWare kernel.
Novell Open Enterprise Server	The most recent Novell OS reflects a trend away from the NetWare name and uses SUSE Linux as the OS.

Table 6-3 NetWare OS descriptions

NetWare Enumeration Tools

- NetWare 5.1
 - Still used on many networks
- New vulnerabilities are discovered daily
 - Vigilantly check vendor and security sites
- Example
 - Older version of Nessus to scan a NetWare 5.1 server

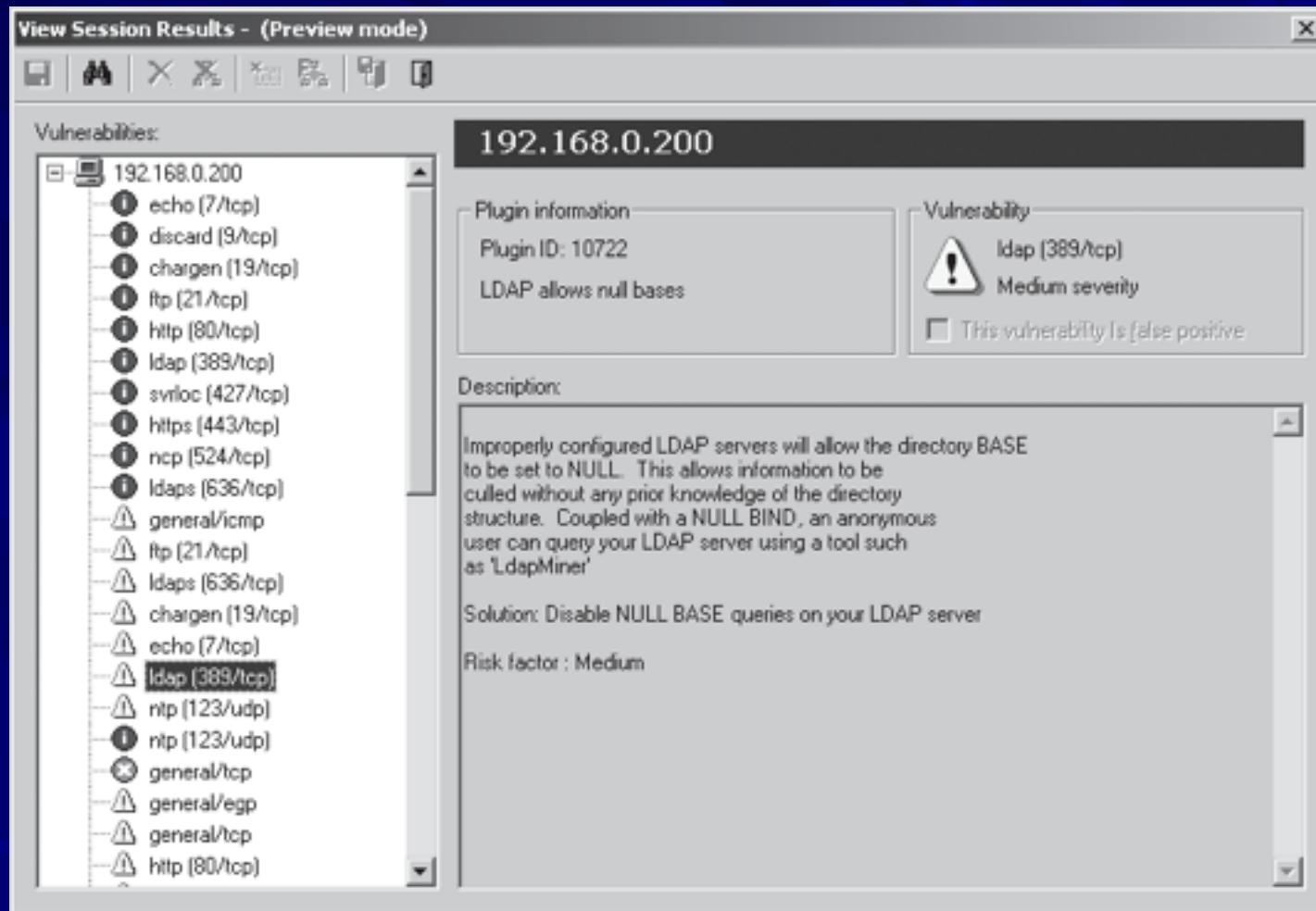


Figure 6-17 Nessus enumerates a NetWare server

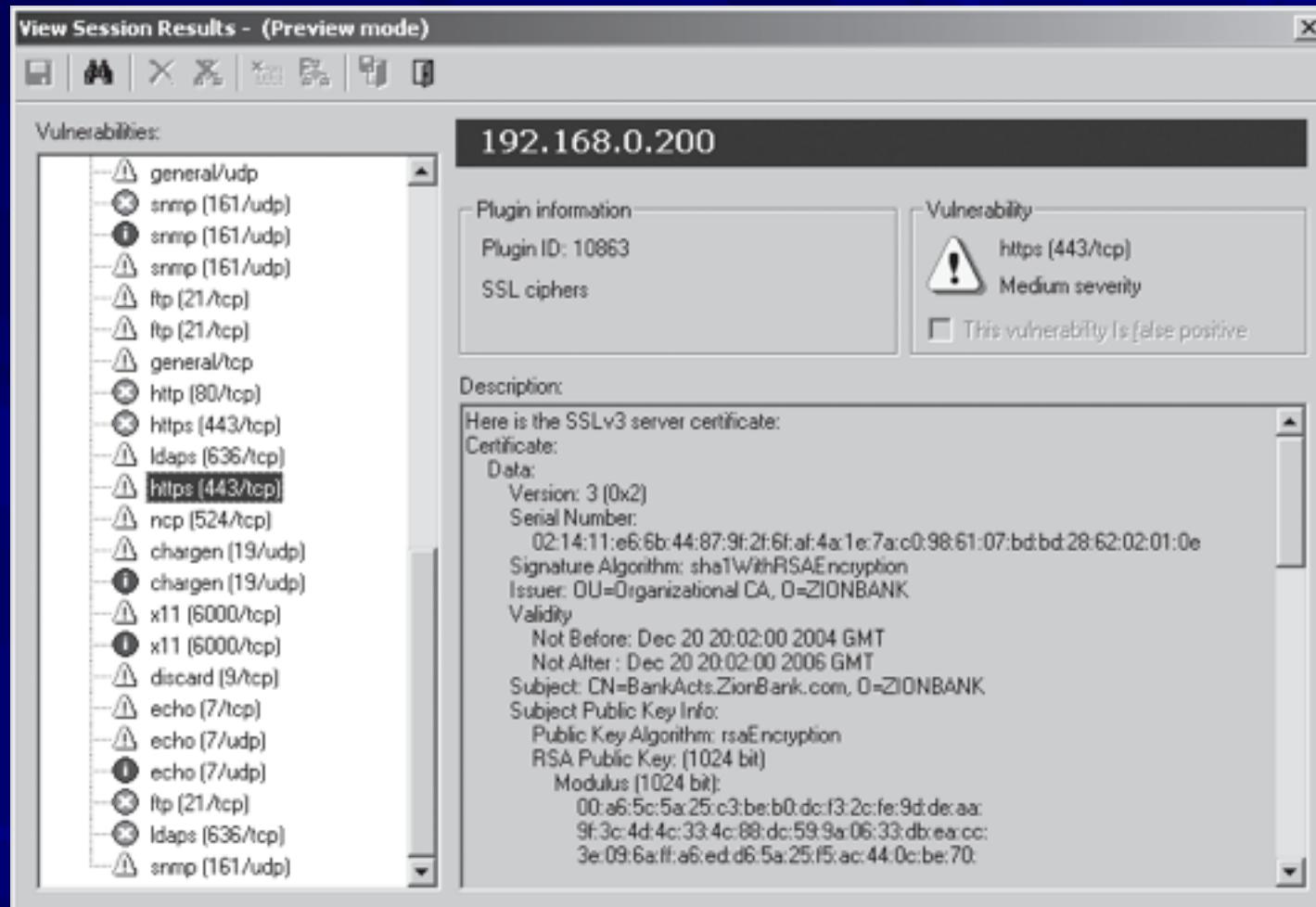


Figure 6-18 Enumerating eDirectory in Nessus

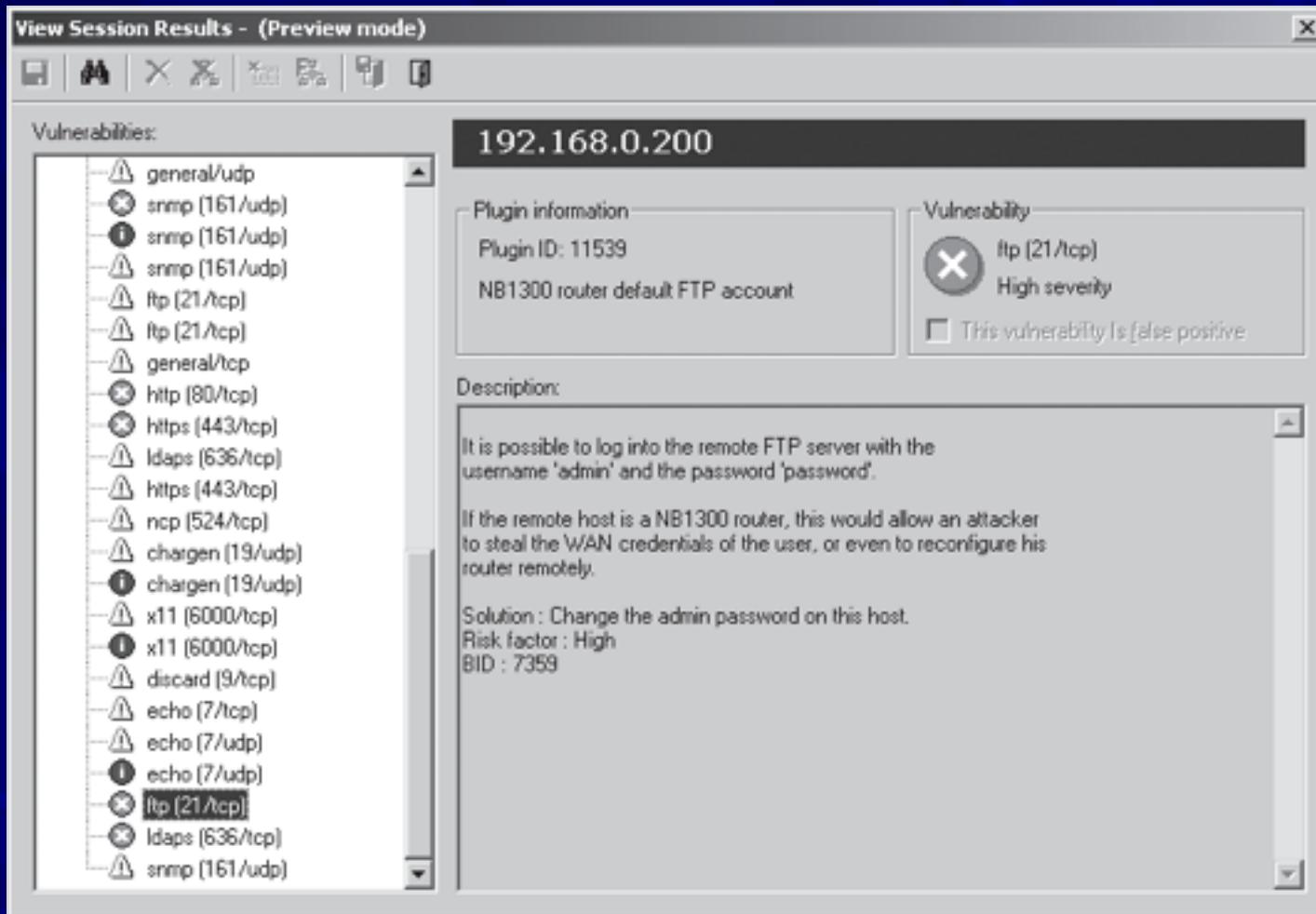


Figure 6-19 Nessus discovers the FTP account's username and password

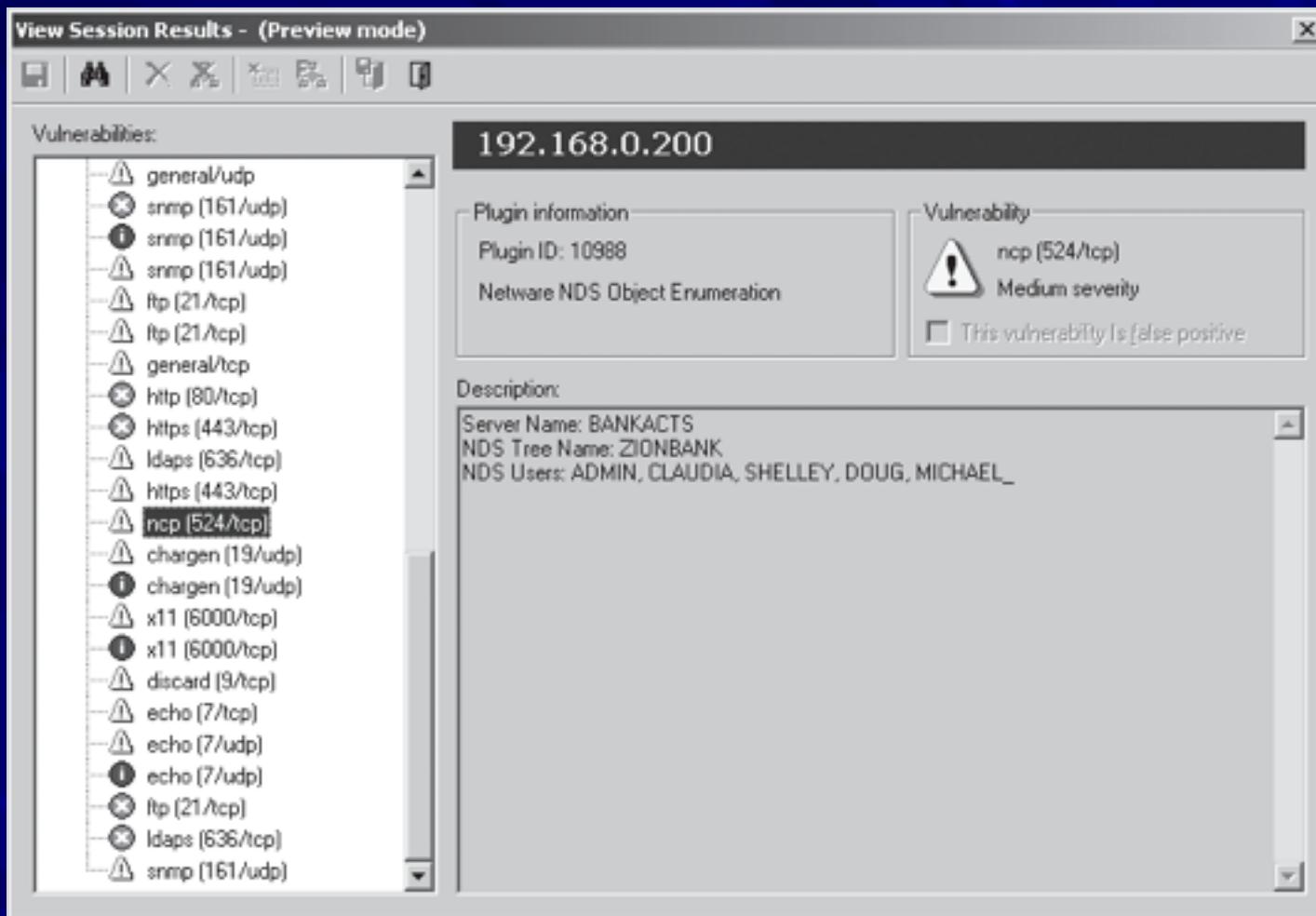


Figure 6-20 Nessus enumerates several user accounts

NetWare Enumeration Tools (cont'd.)

- Novell Client for Windows
 - Gathers information on shares and resources
- Vulnerability in NetWare OS
 - You can click Trees, Contexts, and Servers buttons without a login name or password
 - Open dialog boxes showing network information

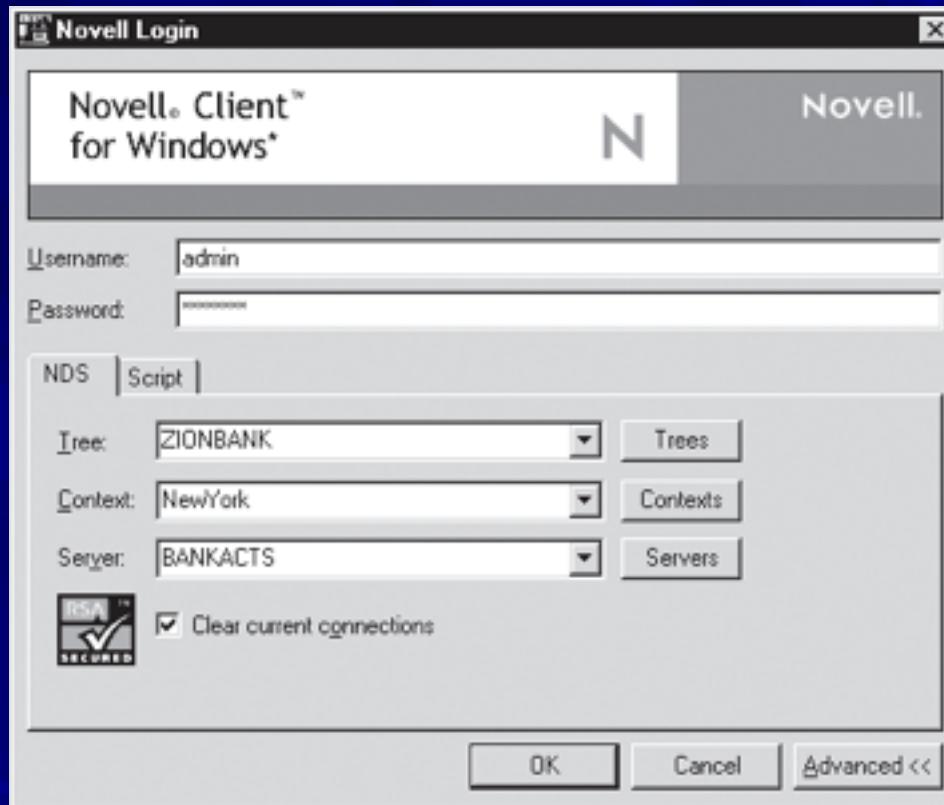


Figure 6-22 Logging in with credentials supplied by Nessus

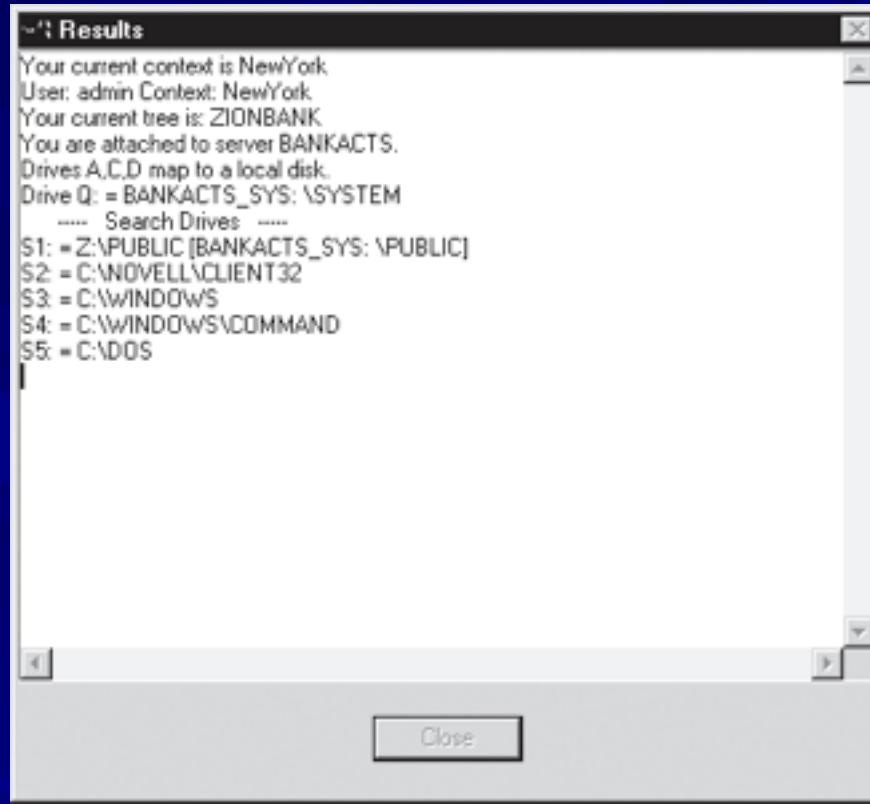


Figure 6-23 Information displayed after the NetWare login is accepted

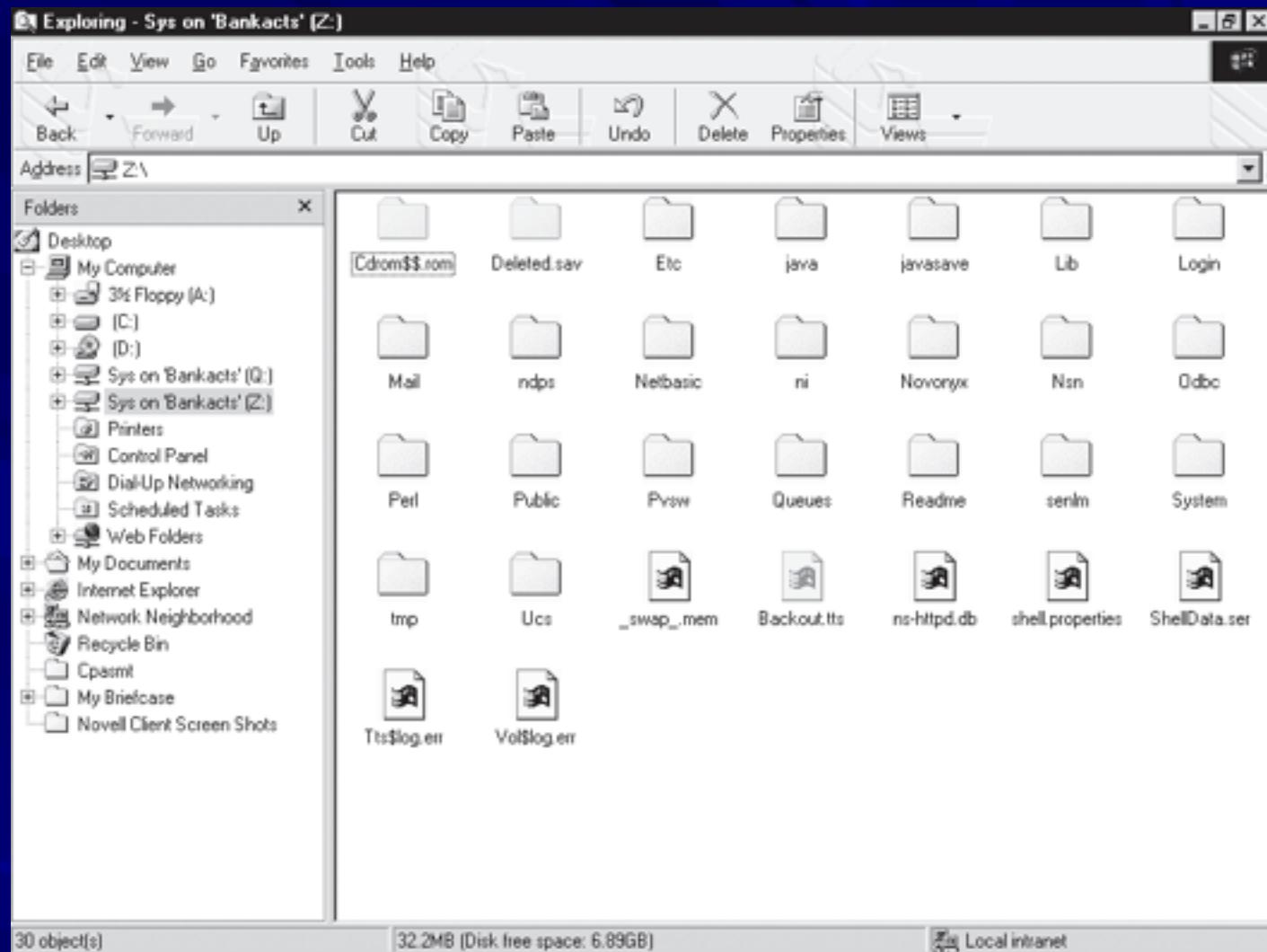


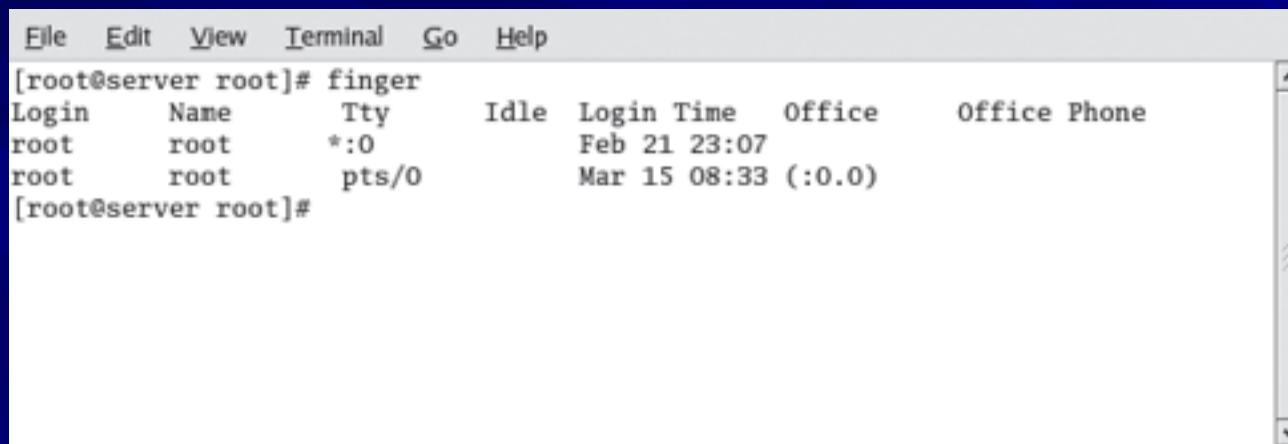
Figure 6-24 Accessing NetWare through mapped drives

Enumerating the *nix Operating System

- Several variations
 - Solaris and OpenSolaris
 - HP-UX
 - Mac OS X and OpenDarwin
 - AIX
 - BSD UNIX
 - FreeBSD
 - OpenBSD
 - NetBSD
 - Linux, including several distributions

UNIX Enumeration

- Finger utility
 - Most popular enumeration tool for security testers
 - Finds out who is logged in to a *nix system
 - Determines who was running a process
- Nessus
 - Another important *nix enumeration tool



A screenshot of a terminal window titled "File Edit View Terminal Go Help". The window displays the output of the "finger" command. The output shows two entries for the user "root": one entry for root at the console (TTY *:0) last seen on Feb 21 at 23:07, and another entry for root at a pts/0 terminal last seen on Mar 15 at 08:33. The command "finger" was run by the user "root" at the server.

```
[root@server root]# finger
Login      Name      Tty      Idle  Login Time   Office      Office Phone
root        root      *:0          Feb 21 23:07
root        root      pts/0        Mar 15 08:33 (:0.0)
[root@server root]#
```

Figure 6-25 Using the Finger command

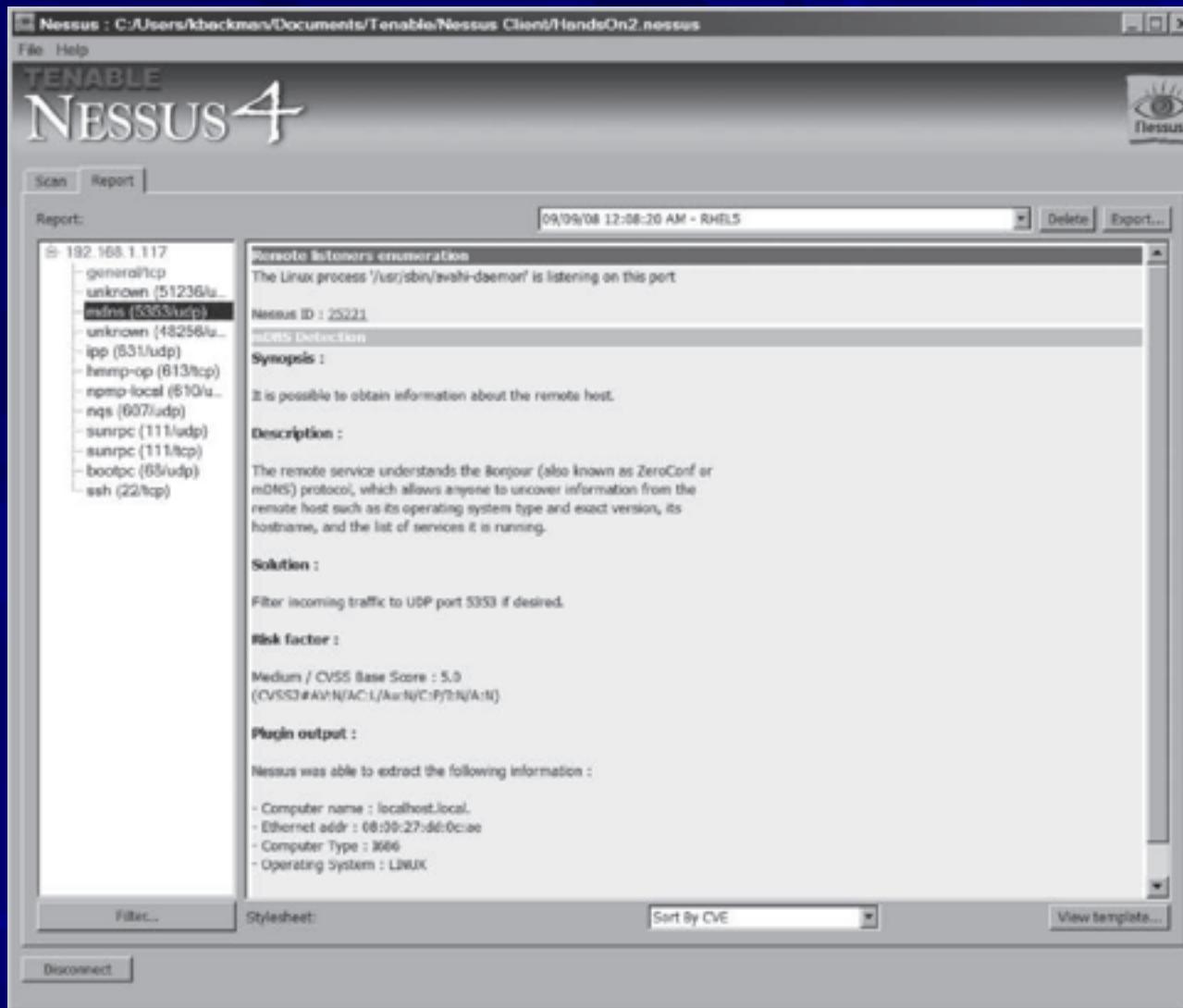


Figure 6-26 Nessus enumerates a Linux system