

Network Mapping and Reconnaissance

“The first step of any attack is to know your enemy” – Sun Tzu, “The Art of War”

- Before an attack, the hacker will gather as much information as possible about your network using a variety of tools and techniques.
- In general, a hacker will follow three basic steps in order to acquire a map and layout of an organization’s network:
 - o Web-based Reconnaissance
 - o Network Scanning and Reconnaissance
 - o Enumeration.

Web-based Reconnaissance

- This involves using company web-sites, ARIN, Whois, and DNS databases to gather as much public information about the company as possible.
- This information includes the technologies that are being used such as, Internet, Intranet, Remote Access and the Extranet.
- In addition, the hacker will try to determine business partners and administrative contacts. This information can be used later for spoofing attacks.
- And attacker will conduct network enumeration to identify the domain names and associated networks related to a particular organization.
- This technique will allow an attacker to discover all the domain names and networks attached to the organization.
- There are a lot of **whois** databases that can be queried to provide a large amount of information about a network.

Network Scanning and Reconnaissance

- Network Reconnaissance is used to create a network topology, as well as a potential access path into the network.
- There a wide variety of tools that can be used for this purpose:
 - o traceroute
 - o ping
 - o CartoReso
 - o nmapfe
 - o hping3
- The above tools will provide a network map showing all the hosts, routers, gateways and other switching equipment in the network.
- One of the most basic steps in mapping out a network is performing an automated ping sweep on a range of IP addresses and network blocks to determine if individual systems are alive.
- One of the techniques of performing a ping sweeps is to use applications such as **fping**.
- Unlike the traditional ping utility, which waits for a response from each system before moving on to the next host, **fping** is a utility that will send out mass ping requests in a parallel, round robin fashion.
- At this point the attacker has a good idea of the machines on the network, their operating systems, the topology, policies, management and administration of their systems.
- The next step is to identify open ports and services on individual systems. The tools that are available are:
 - o **nmap (nmapfe)**
 - o **nessus**
 - o **hping3**
- There are also commercial products and Internet Security scanners available for sale on the open market.
- Of the above, **nmap** is the most popular and advanced tool (and free) available for port scanning.
- It also comes with a GUI, an X-based front end (**nmapfe**) which makes it very easy to use.
- The freely distributable source code is available at <http://www.insecure.org/nmap/>.

Enumeration

- If the initial target attempt and non-intrusive probing haven't turned up any immediate results, an attacker will turn to identifying valid user accounts, or poorly protected resource shares.
- There are many ways to extract valid account or exported resource names from a system by using a process called enumeration.
- Enumeration involves active connections to a system and directed queries. As such, they must be logged on or otherwise noticed.
- Much of the information collected through enumeration may appear to be harmless. Once a valid username or share is enumerated, it's usually only a matter of time before the hacker guesses the corresponding password or identifies some weakness associated with the resource sharing protocol.
- The type of information enumerated by hackers can be loosely grouped into the following categories:
 - o Network resources and shares
 - o Users and Groups
 - o Applications and Banners
- Enumeration techniques are also mostly operating-system specific and thus targeted using information gathered in earlier reconnaissance activities to map out the network and systems.

Windows Enumeration

- Windows systems have a well-deserved reputation for giving away free information to attackers.
- This is primarily due to the Common Internet File System/Server Message Block (CIFS/SMB) and NetBIOS protocols upon which its network services heavily depend.
- Although current Windows systems have the capability to run TCP/IP natively and are quite functional without NetBIOS, they still come out of the box configured with all of the insecurities of their older sibling NT.

Null Sessions

- Null sessions allow an anonymous attacker to extract a great deal of information about a system--most importantly, user account names. They are dangerous because they allow attackers to enumerate user data remotely across the LAN or internet.
- Windows NT, 2000 and even Server 2003 domain controllers are susceptible to enumeration using null sessions. There is a lot more information available on null sessions and SMB enumeration.
- The important point to keep in mind is that null sessions and subsequent enumeration can give away important information such as account names, which can then be used with dictionary attacks and other information like last logon, privileges, and when and if the user's password expires.
- These techniques will even give you the logon hours so that the attack can be carried out safely when the user is not around.
- The CIFS/SMB and NetBIOS standards include APIs that return valuable information about a machine via TCP port 139 even to unauthenticated users.
- The first step in accessing these APIs remotely is creating just such an unauthenticated connection to an NT/2000 system by using the so-called "null session" command:

C:\>net use \\192.168.202.33\IPC\$ "" /user:""

- The preceding command will connect to the hidden interprocess communications "share" (IPC\$) at IP address 192.168.1.200 as the built-in anonymous user (/user:"") with a null ("") password.

- If successful, the attacker now has an open channel over which to attempt the various techniques to steal as much information as possible from the target: network information, shares, users, groups, Registry keys, and so on.
- Almost all the information-gathering techniques that we will discuss take advantage of this one out-of-the-box security failing of Windows systems.
- Also known as the "Red Button" vulnerability, null session connections, or anonymous logon, can be the single most important network foothold sought by intruders.

Null Session Countermeasure

- Null sessions require access to TCP 139 (and/or 445 on Win 2000), so the most effective way to stop them is to filter TCP and UDP ports 139 and 445 at all perimeter network access devices.
- Ideally, blocking UDP 137 and 138, TCP 139, and TCP 445 at the firewall will not allow null session from outside the network but the network is still vulnerable to internal attackers or if the attacker finds a way through the firewall (source port spoofing or application exploits).
- Unfortunately there are still many machines and networks that do not block 139 access to the internet.
- We can also disable SMB services entirely on individual hosts by unbinding WINS Client (TCP/IP) from the appropriate interface using the Network Control Panel's Bindings tab.
- This is accomplished by unbinding File and Print Sharing for Microsoft Networks from the appropriate adapter under the Network and Dial-up Connections applet | Advanced | Advanced Settings.
- The Security Policies MMC snap-in provides a graphical interface to the many arcane security-related Registry settings like **RestrictAnonymous** that needed to be configured manually under older NT systems.
- These settings can be applied at the Organizational Unit (OU), site, or domain level so they can be inherited by all child objects in Active Directory if applied from a Win 2000 domain controller.
- Setting RestrictAnonymous to 1 does not actually block anonymous connections. However, it does prevent most of the information leaks available over the null session, primarily enumeration of user accounts and shares.
- However, some enumeration tools and techniques will still extract sensitive data from remote systems even if RestrictAnonymous is set to 1.

User Account Enumeration

- User2sid and Sid2user are two useful utilities for Windows that can be used to query the SAM to find out a SID value for a given account name and vice versa.
- These utilities are provided for administrative purposes and use two functions: LookupAccountName and LookupAccountSid respectively.
- User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine and Sid2user.exe can then be used to retrieve the names of all the user accounts and more.
- These tools can be called against a remote machine without providing logon credentials except those needed for a null session connection. These tools rely on the ability to create a null session in order to work.
- **SID** is short for **security identifier**, a security feature of the Windows NT, 2000, XP, 2003 operating systems. The SID is a unique name (alphanumeric character string) that is used to identify an object, such as a user or a group of users in a network of NT/2000/XP/2003 systems.
- Windows grants or denies access and privileges to resources based on ACLs, which use SIDs to uniquely identify users and their group memberships. When a user requests access to a resource, the user's SID is checked by the ACL to determine if that user is allowed to perform that action or if that user is part of a group that is allowed to perform that action.
- All SIDs are unique within a given system and are issued by what is known as an "Authority" such as a domain. There are five authorities:
- **SECURITY_NULL_SID_AUTHORITY (null user)**
 - There is a universal Well-Known SID S-1-0-0 that represents a group with no members and is generally used when the SID of an object is not known. A universal well-known SID is a SID that is common to all machines. That is, the value of the Null_SID is the same on my machine as it is on yours.
- **SECURITY_WORLD_SID_AUTHORITY (everyone)**
 - This authority is responsible for the Everyone group. The well-known SID of this group is S-1-1-0
- **SECURITY_LOCAL_SID_AUTHORITY (local user)**
 - Responsible for Local issues. Users with the right to Log on locally will have membership of the group SID S-1-2-0.
- **SECURITY_CREATOR_SID_AUTHORITY (creator owner/group)**

- o There are two group well-known SIDs issued by this authority namely Creator Owner ID (S-1-3-0) and Creator Group (S-1-3-1)

The following are some of the default SIDs that would be of interest to hackers:

Default Global groups (SidTypeGroup)

Domain Admins S-1-5-21-<number>-<number>-<number>-512
 Domain Users S-1-5-21-<number>-<number>-<number>-513
 Domain Guest S-1-5-21-<number>-<number>-<number>-514

Non-Default Global Groups (SidTypeAlias)

Example S-1-5-21-<number>-<number>-<number>-n=> 1000

Non-Default Local Groups (SidTypeAlias)

Example S-1-5-21-<number>-<number>-<number>-n=> 1000

Default Accounts (SidTypeUser)

Administrator S-1-5-21-<number>-<number>-<number>-500
 Guest S-1-5-21-<number>-<number>-<number>-501

Non-Default User Accounts (SidTypeUser)

username S-1-5-21-<number>-<number>-<number>-n=> 1000

Any group or user that is not created by default will have a RID of 1000 or greater. A RID is a Registered ID. This is the last portion of the SID. Once a RID has been issued it will never be used again even if the user and user account are deleted.

- **Using The Tools** (from the readme text for user2sid and sid2user):

User2sid is a command line interface to a WIN32 function LookupAccountName.

Usage: user2sid [\\computer_name] account_name

Where computer_name is optional. By default, the search starts at a local Windows NT computer.

Sid2user is a command line interface to a WIN32 function LookupSidName.

Usage: sid2user [\\computer_name] authority subauthority1 ...

Where computer_name is optional. By default, the search starts at a local Windows NT computer. For example,

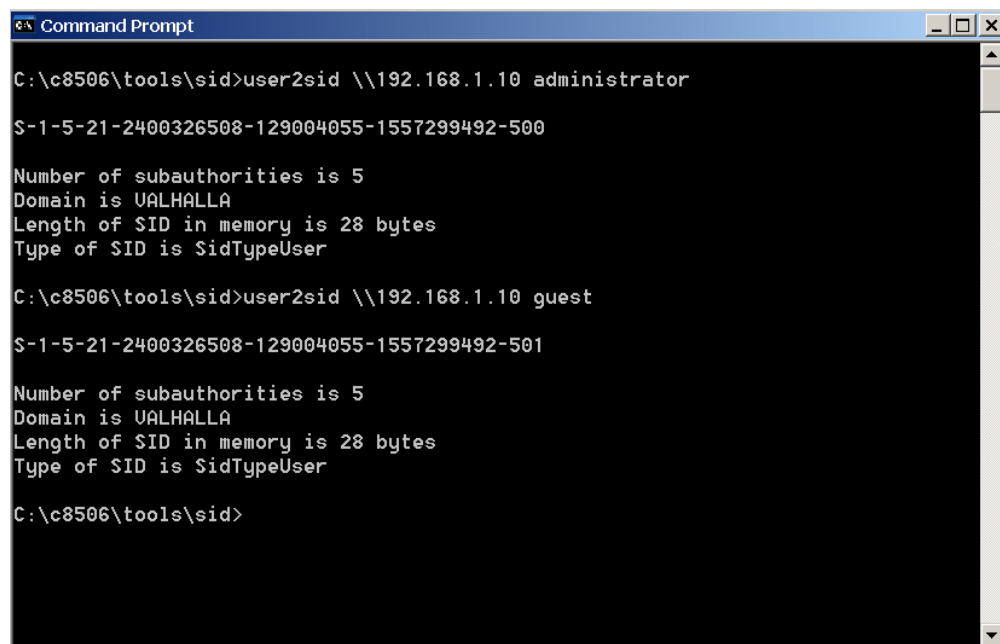
sid2user 5 32 544

- Basically all you need to know is the computer name/IP and an account name to get the SID. The following examples illustrate the use of the tools.

- The first thing you have to do is set up a null session. A null session connects to the IPC\$ share on the remote machine. You can do this by issuing:

`c:\>net use \\192.168.1.10\IPC$ "" /user:""`

- Now, to be able to acquire the user list from the remote machine we need to know the value of a SID issued by the SECURITY_NT_AUTHORITY.
- We can use user2sid.exe for getting this information since the SIDs of the Global groups are issued by the SECURITY_NT_AUTHORITY, renaming the default accounts (Administrator and Guest) to something else will not help (as far as this attack is concerned anyway.)
- Usually as first step the easiest accounts to try are "administrator" and "guest". The following screen shot illustrates this:



```

C:\c8506\tools\sid>user2sid \\192.168.1.10 administrator
S-1-5-21-2400326508-129004055-1557299492-500

Number of subauthorities is 5
Domain is VALHALLA
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\c8506\tools\sid>user2sid \\192.168.1.10 guest
S-1-5-21-2400326508-129004055-1557299492-501

Number of subauthorities is 5
Domain is VALHALLA
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\c8506\tools\sid>
```

- The next step is to use the information found to escalate (via the default guest account) to the administrators' group by changing the RID (relative identifier) using sid2user. The next screen shot illustrates this:


```
Command Prompt
C:\c8506\tools\sid>sid2user \\192.168.1.10 5 21 2400326508 129004055 1557299492
500
Name is Administrator
Domain is UALHALLA
Type of SID is SidTypeUser
C:\c8506\tools\sid>
```

Windows Network Enumeration

- The first thing a remote attacker will try on a well-mapped-out Windows network is to get a sense of what exists on the subnet.
- Since Windows still depends heavily on NetBIOS naming services (UDP 137), these activities are known as "enumerating the NetBIOS wire."
- The tools and techniques for sniffing on the NetBIOS wire are readily available-most are built into the OS itself. In addition there are also some third-party tools.
- The ***net view*** command is a good example of a built-in enumeration tool. It is a simple NT/2000 command-line utility that will list domains available on the network and then lay bare all machines in a domain.
- The syntax is as follows:

C:\>net view /domain

- The above will list all the domains available on the network.
- The command can then be used to interrogate individual domains as follows:

C:\>net view /domain:olympus
Server Name Remark

\\COLISEUM
\\ITHACA Samba Server
\\PROMETHEUS
The command completed successfully.

- Another very useful built-in tool is **nbtstat**, which calls up the NetBIOS Name Table from a remote system.
- The Name Table contains great information, as seen in the following example:

C:\>nbtstat -A 192.168.1.100

Local Area Connection:

Node IpAddress: [192.168.1.100] Scope Id: []

NetBIOS Remote Machine Name Table

| Name | Type | Status |
|----------------------|--------------------------|-------------------|
| ----- | | |
| PROMETHEUS | <00> UNIQUE | Registered |
| PROMETHEUS | <20> UNIQUE | Registered |
| OLYMPUS | <00> GROUP | Registered |
| OLYMPUS | <1E> GROUP | Registered |
| PROMETHEUS | <03> UNIQUE | Registered |
| ADMINISTRATOR | <03> UNIQUE | Registered |

MAC Address = 00-01-02-28-85-37

- As illustrated, **nbtstat** extracts the system name (PROMETHEUS), the domain it's in (OLYMPUS), any logged-on users (ADMINISTRATOR), any services running, and the network interface hardware media access control (MAC) address.
- These entities can be identified by their NetBIOS service codes (the two-digit number to the right of the name), which are partially listed in the table below:

| NetBIOS Code | Resource |
|---------------------|--|
| <computer name>[00] | Workstation Service |
| <domain name> [00] | Domain Name |
| <computer name>[03] | Messenger Service (for messages sent to this computer) |
| <user name>[03] | Messenger Service (for messages sent to this user) |
| <Computer name>[20] | Server Service |
| <domain name>[1D] | Master Browser |
| <domain name>[1E] | Browser Service Elections |
| <domain name>[1B] | Domain Master Browser |

- One of the best tools for enumerating Windows shares (and a much more) is **DumpSec** (formerly DumpACL), available free from Somarsoft.

- It audits everything from file system permissions to services available on remote systems. Basic user information can be obtained even over an innocuous null connection, and it can be run from the command line, making for easy automation and scripting.
- The following is a command line example of DumpSec to pull a list of users, groups, and the NT system's policies and user rights: (note that DumpSec requires a null session with the target computer to operate):

```
C:\>dumpsec /computer=\\192.168.1.6 /rpt=usersonly /saveas=tsv /outfile=c:\temp\users.txt
```

```
C:\>cat c:\temp\users.txt
```

**5/2/2010 8:47 PM - Somarsoft DumpSec (formerly DumpAcl)
- \\192.168.1.5**

| UserName | FullName | Comment |
|-------------------|----------------------|---|
| root | Administrator | Built-in account for administering |
| the domain | | |
| Guest | | Built-in account for guest access |
| athena | | |

- Using the DumpSec GUI, many more information fields can be included in the report.
- Check out the following tools that are available free:
 - superscan
 - Enum
 - getacct

Windows Host Enumeration Countermeasures

- Blocking host enumeration comes down to blocking access to TCP and UDP ports 135-159 and 445.
- Without this precaution, we have to either disable SMB services or set RestrictAnonymous to secure them.
- To disable SMB, unbind WINS Client (TCP/IP) from the appropriate network adapter under NT4. On Win 2000, disable File and Print Sharing for Microsoft Networks under the appropriate adapter.
- If you must allow access to SMB, block the ability to obtain sensitive host information by setting the appropriate value for the RestrictAnonymous Registry key, found under HKLM\SYSTEM\CurrentControlSet\Control\LSA. RestrictAnonymous = 1 is the highest setting for NT4, which still allows null sessions but blocks retrieval of sensitive information.

- RestrictAnonymous = 2 is the highest value on Win 2000, which blocks null sessions entirely.

Banner Grabbing Basics

- The two most widely available tools for enumerating applications are: **telnet** and **netcat**.
- The simplest technique is to open a telnet connection to a known port on the target server, press ENTER a few times if necessary, and see what comes back:

```
C:\>telnet 192.168.1.5 80
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
to /index.html not supported.<P>
Invalid method in request <P>
<HR>
<ADDRESS>Apache/1.3.20 Server at ithaca.olympus.net Port
80</ADDRESS>
</BODY></HTML>

Connection to host lost.
C:\>
```

- For a more surgical probing tool, hackers use the "TCP/IP Swiss army knife" called **netcat**, written by the original NT hacker, Hobbit (<http://www.avian.org>), and ported to NT by Weld Pond of the L0pht security research group.
- Netcat is available at <http://packetstorm.securify.com/UNIX/scanners/nc110.exe>.
- When employed by a competent enemy, it is extremely effective. The following is one of its more simplistic uses, connecting to a remote TCP/IP port:

```
C:\>nc -v www.olympus.net 80
www.olympus.net [192.168.1.10] 80 (?) open
```

- Pressing ENTER results in the following:

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Sat, 06 Apr 2002 13:02:40 GMT
Content-Type: text/html
Content-Length: 87
```

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

- For the more sophisticated hacker, the HTTP HEAD method is a clean way to elicit banner info:

C:\>nc -v www.olympus.net 80

www.corleone.com [192.168.1.10 80 (?) open

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Server: Microsoft-IIS/5.0

Date: Sat, 06 Apr 2002 13:31:34 GMT

Connection: Keep-Alive

Content-Length: 1270

Content-Type: text/html

Set-Cookie: ASPSESSIONIDGGQGQLAO=IPGFKBKGDGPOOHCOHIKOAKHI;

path=/
Cache-control: private

- This information will allow the attacker to focus her efforts to specific exploits in compromising a system now that the vendor and version of web server software are known.

Windows Banner Grabbing Countermeasures

- Inventory your mission-critical applications, and research the correct way to disable presentation of vendor and version in banners.
- Audit the network systems regularly with port scans and raw **netcat** connects to active ports to make sure applications are not giving away even the slightest information to attackers.

UNIX Enumeration

- Most current UNIX implementations rely on standard TCP IP networking features and therefore are not as prone to giving up information as freely as NT does via its legacy NetBIOS interfaces.
- However UNIX systems are vulnerable to enumeration techniques depending on how the system is configured.
- For example, Remote Procedure Call (RPC), Network Information System (NIS), and Network File System (NFS) are still widely used and have all been targeted by attackers over the years.

UNIX Network Resources and Share Enumeration

- The best sources of UNIX network information are the basic port scanning techniques discussed earlier such as nmap.
- A useful tool for digging a little deeper is the UNIX utility **showmount**, useful for enumerating NFS-exported file systems on a network.
- For example, say that a previous scan indicated that port 2049 (NFS) was listening on a potential target.
- **showmount** can then be used to see exactly what directories are being shared:

```
[root$]showmount -e 192.168.1.5
export list for 192.168.1.5:
/pub          (everyone)
/var          (everyone)
/home/data    192.168.1.200
```

- The **-e** switch shows the NFS server's export list. The best countermeasure is to ensure that the exported file systems have the proper permissions (read/write should be restricted to specific hosts) and that NFS is blocked at the firewall (port 2049).
- **showmount** requests can also be logged, another good way to catch interlopers.
- In addition to NFS there are other file-system sharing software that have grown in popularity; the open source **Samba software suite** provides seamless file and print services to SMB clients.
- SMB (Server Message Block) forms the underpinnings of Windows networking. Although the Samba server configuration file (**/etc/samba/smb.conf**) in

Linux) has some straightforward security parameters, misconfiguration can still result in unprotected network shares.

UNIX Users and Group Enumeration

- One of the oldest trick when it comes to enumerating users is the UNIX **finger** utility.
- This was a convenient way of giving out user information automatically back in the days of a much smaller and friendlier Internet.
- Most systems disable it by default but many scripted attack tools still try it, and many unwitting systems administrators leave finger running with minimal security configurations.
- Other such outdated and mostly disabled tools include:
- **rwho** - returns users currently logged on to the remote host.
- **rusers** - same as above but provides additional user information such as idle time, etc.

UNIX Applications and Banner Enumeration

- Like any network resource, applications need to have a way to talk to each other over a network. One of the most popular protocol for doing just that is Remote Procedure Call (RPC).
- RPC employs a program called the **portmapper** (now known as **rpcbind**) to arbitrate between client requests and ports that it dynamically assigns to listening applications.
- Despite its long history of exploits and security holes, RPC remains extremely popular.
- **rpcinfo** is the equivalent of **finger** for enumerating RPC applications listening on remote hosts and can be targeted at servers found listening on port 111 (**rpcbind**) or 32771 (Sun's alternate portmapper):

```
[root$] rpcinfo -p 192.1681.5
program vers proto  port
100000    2    tcp    111  portmapper
100000    2    udp    111  portmapper
100024    1    udp    32768 status
100024    1    tcp    32768 status
100011    1    udp    914  rquotad
100011    2    udp    914  rquotad
```

```

100005    1    udp    32769    mountd
100005    1    tcp    32769    mountd
100005    2    udp    32769    mountd
100005    2    tcp    32769    mountd
100005    3    udp    32769    mountd
100005    3    tcp    32769    mountd
100003    2    udp     2049    nfs
100003    3    udp     2049    nfs
100021    1    udp    32770    nlockmgr
100021    3    udp    32770    nlockmgr
100021    4    udp    32770    nlockmgr

```

- The above listing tells attackers that this host is running NFS, and samba. Thus, **showmount -e**, will produce further information.
- A variant of **rpcinfo** that can be used from Windows NT systems is called **rpcdump**, available from David Litchfield of Cerberus Information Security. (For more information see <http://www.atstake.com/research/tools/rpcdump.exe>.)
- rpcdump behaves like rpcinfo -p, as shown next:

```
C:\>rpcdump 192.168.1.5
```

| Program no. | Name | Version | Protocol | Port |
|-------------|------------|---------|----------|-------|
| (100000) | portmapper | 4 | TCP | 111 |
| (100000) | portmapper | 3 | TCP | 222 |
| (100001) | rstatd | 2 | UDP | 32774 |
| (100021) | nlockmgr | 1 | UDP | 4045 |

RPC Enumeration Countermeasures

- There is no simple way to limit this information leakage other than to use some form of authentication for RPC. (Check with your RPC vendor to learn which options are available.)
- You can use a package like Sun's Secure RPC that authenticates based on public-key cryptographic mechanisms.
- Make sure that port 111 and 32771 (rpcbind) as well as all other RPC ports are filtered at the firewall or disabled on your UNIX systems.

UNIX SNMP Enumeration

- SNMP can provide useful information to attackers for UNIX systems running SNMP agents as well Windows.
- The **snmpwalk** tool is part of the **net-snmp** package found on many flavors of UNIX. It can be used to great effect if default community strings are used on your network.
- An attacker will first determine via UDP port scanning that SNMP is running on UDP port 161 on the target server.

```
[root]# nmap -sU -p161 192.168.1.5  
Starting nmap V. 2.53 by fyodor@insecure.org www.insecure.org/nmap/  
Interesting ports on (192.168.1.5):  
Port      State      Service  
161/udp   open       snmp
```

Nmap run completed 1 IP address (1 host up) scanned in 3 seconds

- The next step is to query a specific MIB with **snmpget**:

```
[root]# snmpget 192.168.1.60 public system.sysName.0  
system.sysName.0   ithaca
```

- It is much faster to examine the contents of the entire MIB using **snmpwalk**.

SNMP Countermeasures

- The simplest way to prevent such activity is to disable SNMP.
- If shutting off SNMP is not an option, at least ensure that it is properly configured with properly chosen community names (not the default "public" or "private").
- If SNMP is being used to manage your network, make certain that access to TCP and UDP ports 161 (SNMP GET/ SET) is blocked at all perimeter network access devices.
- Finally, consider using SNMP V3 detailed in RFC 2571-2575. SNMP V3 is much more secure than V1 and provides enhanced encryption and authentication mechanisms.