Nessus scanning on Windows Domain

A little inside information and Nessus can go a long way...

By Sunil Vakharia
sunilv@phreaker.net

Version 1.0 *4 November 2003*

About this paper

This paper is not a tutorial for Nessus. For that, please refer to the man pages or Nessus' website (http://www.nessus.org).

This paper is about using Nessus to scan Windows networks and considers various sceanrios which one might encounter.

It is a guide to using Nesssus in such cases.

Note: This paper does not talk about running Nessus *from* a Windows machine. Instead it talks about running Nessus *on* a Windows machine or network. In other words, *Windows computers are the targets.*

Warning

Running a tool such as Nessus (which is a Vulnerability Assessment tool) or any other tool on any network/ computer without permission, is illegal.

This tool should only be used to test the security of systems that you own or systems that you are authorized to audit.

Neither the Nessus authors, nor myself, are responsible for use/ misuse of the tool or of any information contained within this document.

Remember: You are at your own!

Topics covered

Part I: Scan Types

Scan comparison

1) Default Scan
2) Nessus scan with admin rights
3) Nessus scan with access to registry
4) So how do we give Nessus that inside information

Part II: Configuration issues

1) Configuration on Nessus' end
2) Configuration on target's end
3) Why not use Administrator accounts?
4) Special account: *nessus*
5) Enhancements in a domain environment

References

To do list

Comments, Suggestions, Feedback

Part 1 Scan Types

In most cases, an IP address (or a set of them) is pretty much all that Nessus gets. There is no information about the target that Nessus is given.

In this case, Nessus is just able to scan for open ports, find out what services are listening and probe them for vulnerabilities. There is no information about the service packs installed, hot-fixes missing or vulnerabilities in applications (such as Winamp) installed.

All this information can only be obtained if the registry is accessible to Nessus. Note that this is true for any vulnerability scanner, including commercial ones such as Retina.

With registry access, Nessus is able to audit the system in a much more accurate and complete manner. This is specially useful to Administrators, who want to find out, for instance, which patches are missing on which systems.

In order to highlight the difference in accuracy of the scan and the wealth of information that Nessus can gather if given a little inside information, three different scans are illustrated below.

1) A default scan – *no inside information*.

2) Scan with Administrator rights.

3) Scan without Administrator rights, but only access to the registry.

Note that all the scans were done on the same target which was a Windows 2000 Professional out-of-the-box machine. No changes were made in the security settings on the target machine for any of the scans.

Nessus 2.0.8 was used to scan the target.

Scan comparison

	Holes found	Warnings found
Default Scan	04	10
Scan with registry access plus administrative rights	46	20
Scan with only registry access	43	19

As is evident from the table above, Nessus can glean much more information if it is given access to the registry.

1. Default Scan

Results snippet:

Type	Port	Issue and Fix
Vulnerability	loc-srv (135/tcp)	The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. Solution: see http://www.microsoft.com/technet/security/bulletin/MS03-039.asp
Vulnerability	loc-srv (135/tcp)	The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. Solution: see http://www.microsoft.com/technet/security/bulletin/MS03-026.asp
Vulnerability	microsoft-ds (445/tcp)	It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access All the smb tests will be done as "/" in domain ADAM
Warning	netbios-ns (137/udp)	The following 8 NetBIOS names have been gathered : JOY = This is the computer name registered for workstation services by a WINS client. ADAM = Workgroup / Domain name JOY = This is the current logged in user registered for this workstation. JOY ADAM = Workgroup / Domain name (part of the Browser elections) ADAM __MSBROWSE__ ADMINISTRATOR = This is the current logged in user registered for this workstation. The remote host has the following MAC address on its adapter :...

2. Nessus scan with admin rights

Additional information gained

Type	Port	Issue and Fix
Vulnerability	microsoft-ds (445/tcp)	The remote Windows 2000 does not have the Service Pack 4 applied. (it uses instead) You should apply it to be up-to-date Solution : go to http://www.microsoft.com/windows2000/downloads/
Vulnerability	microsoft-ds (445/tcp)	The Windows shell of the remote host has an unchecked buffer which can be exploited by a local attacker to run arbitrary code on this host. See http://www.microsoft.com/technet/security/bulletin/ms02-014.asp
Vulnerability	microsoft-ds (445/tcp)	A flaw in the Windows 2000 Network Connection Manager could enable privilege elevation. See http://www.microsoft.com/technet/security/bulletin/ms02-042.asp
Vulnerability	microsoft-ds (445/tcp)	A security issue has been identified in WM_TIMER that could allow an attacker to compromise a computer running Microsoft Windows and gain complete control over it. http://www.microsoft.com/technet/security/bulletin/ms02-071.asp
Vulnerability	microsoft-ds (445/tcp)	The remote host is vulnerable to a flaw in ntdll.dll which may allow an attacker to gain system privileges, by exploiting it thru, for instance, WebDAV in IIS5.0 (other services could be exploited, locally and/or remotely) Note : On Win2000, this advisory is superceded by MS03-013 Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-007.asp
Vulnerability	microsoft-ds (445/tcp)	Hotfix to fix Certificate Validation Flaw (Q329115) is not installed. See http://www.microsoft.com/technet/security/bulletin/ms02-050.asp
Vulnerability	microsoft-ds (445/tcp)	XMLHTTP Control Can Allow Access to Local Files. See http://www.microsoft.com/technet/security/bulletin/ms02-008.asp
Vulnerability	microsoft-ds (445/tcp)	A flaw exists in the RPC endpoint mapper, which can be used by an attacker to disable it remotely. Solution for Win2k and XP: see http://www.microsoft.com/technet/security/bulletin/ms03-010.asp
Vulnerability	microsoft-ds (445/tcp)	The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-026.asp
Vulnerability	microsoft-ds (445/tcp)	The remote host is vulnerable to a flaw in the Windows Script Engine, which provides Windows with the ability to execute script code. Solution : See http://www.microsoft.com/technet/security/bulletin/ms03-008.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'ResetBrowser Frame' and the 'HostAnnouncement flood' has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-036.asp

Vulnerability	microsoft-ds (445/tcp)	The remote host is running a version of Windows with a version of DirectX which is vulnerable to a buffer overflow in the module which handles MIDI files. Solution : see http://www.microsoft.com/technet/security/bulletin/MS03-030.asp
Vulnerability	microsoft-ds (445/tcp)	The following shares can be accessed as administrator : - C$ - (readable, writeable) + Content of this share : - SUHDLOG.DAT - BOOTLOG.PRV .... - ADMIN$ - (readable, writeable) + Content of this share : - FeatherTexture.bmp .... - Event Logs - (readable, writeable) + Content of this share : - Application Log.evt - F$ - (readable, writeable) + Content of this share : - Apps ... - DATA - (readable, writeable) + Content of this share : - RECYCLED ... - D$ - (readable, writeable) + Content of this share : - Documents and Settings - RECYCLER - System Volume Information .. Solution : To restrict their access under WindowsNT, open the explorer, do a right click on each, go to the 'sharing' tab, and click on 'permissions'
Vulnerability	microsoft-ds (445/tcp)	The remote version of Windows has a flaw in the way the kernel passes error messages to a debugger. Solution : see http://www.microsoft.com/technet/security/bulletin/MS03-013.asp
Vulnerability	microsoft-ds (445/tcp)	The Microsoft VM is a virtual machine for the Win32 operating environment. Solution : See http://www.microsoft.com/technet/security/bulletin/ms02-013.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Still Image Service Privilege Escalation' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-065.asp
Vulnerability	microsoft-ds (445/tcp)	The remote host is running a Microsoft VM machine which has a bug in its bytecode verifier which may allow a remote attacker to execute arbitrary code on this host, with the privileges of the user running the VM. Solution : See http://www.microsoft.com/technet/security/bulletin/ms03-011.asp
Vulnerability	microsoft-ds (445/tcp)	Authentication Flaw in Windows Debugger can Lead to Elevated Privileges (Q320206) See http://www.microsoft.com/technet/security/bulletin/ms02-024.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'IP Fragment Reassembly' vulnerability has not been applied on the remote Windows host. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-029.asp

Vulnerability	microsoft-ds (445/tcp)	The remote host runs a version of windows which has a flaw in the way the utility manager handles Windows messages. As a result, it is possible for a local user to gain additional privileges on this host. Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-025.asp
Vulnerability	microsoft-ds (445/tcp)	An unchecked buffer in Windows help could allow an attacker to could gain control over user's system. See http://www.microsoft.com/technet/security/bulletin/ms02-055.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Webserver file request parsing' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-086.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'NetBIOS Name Server Protocol Spoofing' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-047.asp or Security Rollup: http://support.microsoft.com/support/kb/articles/q299/4/44.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Local Security Policy Corruption' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-062.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Telnet Client NTLM Authentication' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-067.asp
Vulnerability	microsoft-ds (445/tcp)	A vulnerability in the Certificate Enrollment ActiveX Control in Microsoft Windows 98, Windows 98 Second Edition, Windows Millennium, Windows NT 4.0, Windows 2000, and Windows XP allows remote attackers to delete digital certificates on a user's system via HTML. See http://www.microsoft.com/technet/security/bulletin/ms02-048.asp
Vulnerability	microsoft-ds (445/tcp)	The remote host is vulnerable to a denial of service attack, which could allow an attacker to crash it by sending a specially crafted SMB (Server Message Block) request to it. Solution : http://www.microsoft.com/technet/security/bulletin/ms02-045.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Service Control Manager Named Pipe Impersonation' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-053.asp
Vulnerability	microsoft-ds (445/tcp)	Incorrect VBScript Handling in IE can Allow Web Pages to Read Local Files. See http://www.microsoft.com/technet/security/bulletin/ms02-009.asp and: Microsoft Article Q319847 MS02-009 May Cause Incompatibility Problems Between VBScript and Third-Party Applications
Vulnerability	microsoft-ds (445/tcp)	The remote host is vulnerable to a flaw in its SMB stack which may allow an unauthenticated attacker to corrupt the memory of this host. This may result in execution of arbitrary code on this host, or an attacker may disable this host remotely. Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-024.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Malformed request to index server' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms01-025.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the Unchecked Buffer in SNMP Service has not been applied.

		See http://www.microsoft.com/technet/security/bulletin/ms02-006.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Malformed RPC Packet' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-066.asp
Vulnerability	microsoft-ds (445/tcp)	We were able to determine that you are running IE Version 5.0100 But is missing security update(s) Q822925 (MS03-032) See http://www.microsoft.com/technet/security/bulletin/ms03-032.asp Supersedes MS01-055, MS02-066, MS02-068, MS03-004, MS03-014, MS03-015 and others
Vulnerability	microsoft-ds (445/tcp)	Hotfix to fix Flaw in Microsoft VM could Allow Code Execution (810030) Supersedes : http://www.microsoft.com/technet/security/bulletin/ms02-052.asp See : http://www.microsoft.com/technet/security/bulletin/ms02-069.asp Also Note: Requires full registry access (Administrator) to run the test.
Vulnerability	microsoft-ds (445/tcp)	An overflow in the RAS phonebook service allows a local user to execute code on the system with the privileges of LocalSystem. See http://www.microsoft.com/technet/security/bulletin/ms02-029.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'Relative Shell Path' vulnerability has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-052.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the multiple LPC and LPC Ports vulnerabilities has not been applied on the remote Windows host. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-070.asp
Vulnerability	microsoft-ds (445/tcp)	Trust relationships are created between Windows NT or Windows 2000 domains to allow users in one domain to access resources in other domains without requiring them to authenticate separately to each domain. When a user in a trusted domain requests access to a resource in a trusting domain, the trusted domain supplies authorization data in the form of a list of Security Identifiers (SIDs) that indicate the user's identity and group memberships. The trusting domain uses this data to determine whether to grant the user's request. Solution : see http://www.microsoft.com/technet/security/ms02-001.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'domain account lockout' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-089.asp
Vulnerability	microsoft-ds (445/tcp)	Hotfix to fix Unchecked Buffer in PPTP Implementation (Q329834) is not installed. See http://www.microsoft.com/technet/security/bulletin/ms02-063.asp
Vulnerability	microsoft-ds (445/tcp)	The hotfix for the 'IrDA access violation patch' problem has not been applied. Solution : See http://www.microsoft.com/technet/security/bulletin/ms01-046.asp Or POST SP2 Security Rollup: http://www.microsoft.com/windows2000/downloads/critical/q311401/default.asp
Warning	microsoft-ds (445/tcp)	The remote registry can be accessed remotely using the login / password combination used for the SMB tests.

		Having the registry accessible to the world is not a good thing as it gives extra knowledge to a hacker. Solution : Apply service pack 3 if not done already, and set the key HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg to restrict what can be browsed by non administrators.
Warning	microsoft-ds (445/tcp)	The remote Microsoft Data Access Component (MDAC) server is vulnerable to a flaw which could allow an attacker to execute arbitrary code on this host, provided he can load and execute a database query on this server. See http://www.microsoft.com/technet/security/bulletin/ms http://www.microsoft.com/security/security_bulletins/ms03-033.asp http://www.microsoft.com/technet/security/bulletin/ms02-040.asp
Warning	microsoft-ds (445/tcp)	The SMB signing capability in the Server Message Block protocol in Microsoft Windows 2000 and Windows XP allows attackers to disable the digital signing settings in an SMB session to force the data to be sent unsigned, then inject data into the session without detection, e.g. by modifying group policy information sent from a domain controller. See http://www.microsoft.com/technet/security/bulletin/ms02-070.asp
Warning	microsoft-ds (445/tcp)	There are 28 services running on this host : Computer Browser [Browser] DHCP Client [Dhcp] Protected Storage [ProtectedStorage] Remote Registry Service [RemoteRegistry] Distributed Link Tracking Client [TrkWks] ……. You should turn off the services you do not use. This list is useful to an attacker, who can make his attack more silent by not portscanning this host. Solution : To prevent the listing of the services for being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.
Warning	microsoft-ds (445/tcp)	Buffer overflow in Multiple UNC Provider (MUP) in Microsoft Windows operating systems allows local users to cause a denial of service or possibly gain SYSTEM privileges via a long UNC request. See http://www.microsoft.com/technet/security/bulletin/ms02-017.asp
Warning	microsoft-ds (445/tcp)	The registry key HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount is non-null. It means that the remote host locally caches the passwords of the users when they log in, in order to continue to allow the users to log in in the case of the failure of the PDC. Solution : use regedt32 and set the value of this key to 0
Warning	microsoft-ds (445/tcp)	The messenger service is running. This service allows NT users to send pop-ups messages to each others. This service can be abused by who can trick valid users into doing some actions that may harm their accounts or your network (social engineering attack) Solution : Disable this service.
Warning	microsoft-ds (445/tcp)	The remote host is running a version of the shlwapi.dll which crashes when processing a malformed HTML form. An attacker may use this flaw to prevent the users of this host from working properly.

Oh.. that was a pretty long list. As you can see with Administrative rights, a lot more information is gathered.

3. Nessus scan with access to registry

The scan report is the same as above except for the following:

The following vulnerabilities could not be reported:

1. MS03-008
2. MS02-013
3. MS03-011

These require administrative rights.

Unlike in the earlier case, where Nessus reported that all the folders were accessible, only certain shares/ files were accessible using this limited account. This actually gives the true picture.

4. So how do we give Nessus that *inside information*

Well, it is evident from the results above, that a scan with access to the registry is much better for the administrators, since now he doesn't have to manually check for missing patches.

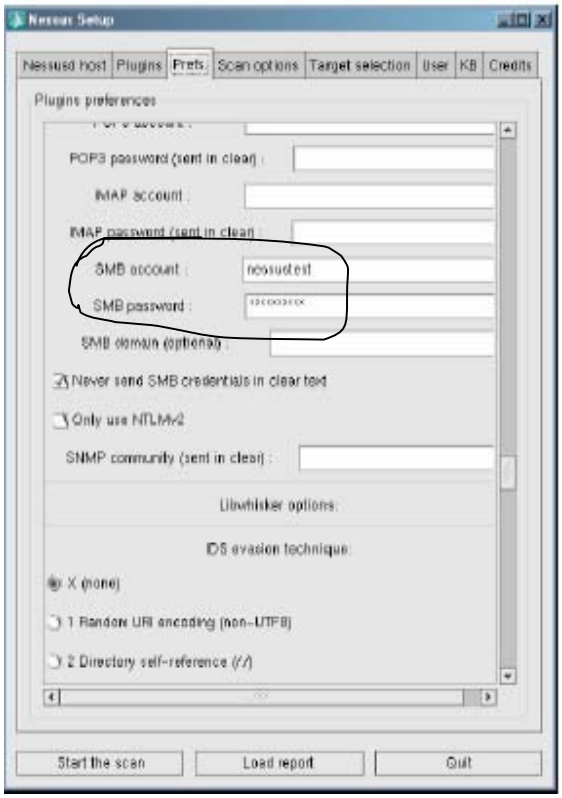
1. So how do we configure Nessus?
2. How do we scan multiple machines for missing patches?
3. How would the results be if I am using an account with domain admin rights?
4. What if I don't have a domain?

All this is dealt with in Part II.

Part 2 Configuration Issues

1. Configuration on Nessus' end

A vastly neglected option in Nessus is under the *Preferences* tab.
Scroll down to the *SMB Login* and *Password* boxes.
Just enter a valid username and password of an account on your target machine (Windows 2000 Professional in my case) that can access the registry from the network.



Make sure that the required plugins are selected. They are in the *Windows* family of plugins. That is about it.

2. Configuration on target's end

There are two basic requirements that a target has to meet.

1. **Remote Registry Service** has to be running.
   This is required for the registry to be accessible from the network.

2. The account trying to access the registry from the network should at the least have **read access** rights to the registry.

   If you have supplied Nessus with Administrative rights by feeding in the administrator username and password, then by default this is taken care.
   The same is true with Domain Administrator accounts.
   However, if you want to give the required access to the registry to another account, then you have to explicitly give access to that user or group.
   This is fairly simple.

   1. Just type *regedt32* in the *Run* box from *Start Menu*.

   2. Next navigate to the key:
      HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

   3. This key determines who can access the registry from the network.

      If you do not have this key, you can create it.
      a) Use the registry editor and go to the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control"
      b) On the "Edit" menu click "Add Key" and enter: "SecurePipeServers" for the key name and "REG_SZ" for the class
      c) Go into the new key "SecurePipeServers"
      d) On the "Edit" menu click "Add Key" and enter: "winreg" for the key name and "REG_SZ" for the class
      e) Go into the new key "winreg"
      f) On the "Edit" menu click "Add Value" and enter: "Description" for the value name and "REG_SZ" for the data type
      g) Modify the new "Description" string value to be "Registry Server"

      Warning: Modifying the registry may make your system unusable. Use caution!

   4. Now click on the winreg key and select Permissions from the context-menu or the menu on top. In Windows XP, it come in the Edit menu and in Windows 2000 it comes in the Security menu.

   5. Give any user you wish to choose Read rights to this key.

   6. That is about it!

3. Why not use Administrator accounts?

If you see the results, you will find that Nessus with administrative access is able to find three more vulnerabilities compared to an ordinary user with registry access.
However, also note that Nessus reports that all the drives are accessible, which is case just because of administrative rights.
Also, it is dangerous to run a plugin with administrative rights, unless you know exactly what it does.
So to be on the safer side, it is recommended that a separate account be created for auditing of the machines.

4. Special account: nessus

1. You can do this by creating a new group, say *NessusGroup*.

2. Make sure it is a global group.

3. Next you can create a new user called *nessus* which belongs only to this group and no other group.
   This way you can ensure that the user *nessus* has very limited rights.

4. Now, you can give this group *NessusGroup* read access to the key winreg.
   This way you can ensure that if you use a new plugin which is not tested enough, the damage done if any is restricted.

5. Enhancements in a domain environment

There are a couple of advantage if you have a Windows NT or 2000 domain environment and you want to make the audit many machines.

1. You can ensure that the Remote Registry service is always running automatically via group policy. So there is no need to manually visit each computer and start the service.

2. You can create a global account: *nessus* under the *NessusGroup*. The same account can then be used to access the registry of all machines.
   Thus there would be no need to create a local account *nessus* on each machine.

3. In order to modify the registry key *winreg* of each machine, group policy can be used. Thus there would be no manual change required for any machine on the domain.

4. If you have domain administrator rights to the account *nessus* (and if you trust the plugins), then there is no need to modify the registry key for any

machine (in most cases). By default, since domain admin will have at least read rights on the key, the registry is accessible.

Future versions of this guide will cover group policy methods in detail

References

Utilizing domain credentials to enhance Nessus scans by Ty Gast

http://www.nessus.org/doc/nessus_domain_whitepaper.pdf

To do list

Future version of this paper will cover details of how group policy features of Windows 2000 can be used to make the configuration tasks mentioned above simpler.

Comments, Suggestions, Feedback

Feel free to drop in a line here: sunilv@phreaker.net