GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

GIAC Incident Handling Analyst Certification (GCIH)
Level Two Practical Assignment for Network Security 2000
(October - December)

NBName.exe – NetBIOS Exploit

Toby S. Houser, M.S.I.S
boost@boosted.com

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Index:

1. Exploit Details
2. Introduction and Description
3. Protocol Description
4. How the exploit works
    a. Denial of Service
    b. Mapping of NetBIOS Namespace
    c. Enumeration of NetBIOSNodes
5. Diagram of exploits on network
6. How to use NBNames.exe
7. Signature of the NBName.exe attack
8. How to protect against NBName.exe
9. Source Code
10. Conclusion
11. Additional Information & References

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

1. Exploit Details:

Name: NBName.exe
Operating Systems Vulnerable: Windows 9x, NT and Windows 2000
Exploit Type: Denial of Service, Enumeration and Information Gathering
Protocol Exploited: NetBIOS

2. Introduction and Description:

The NBName.exe tool was released in August of 2000 by Sir Dystic of the Cult of the Dead Cow. NBName.exe decodes and displays all NetBIOS name packets, denies name registration, causes re-negotiation of existing names by spoofing conflict flags, broadcasts name negotiation requests, and enumerates adapter status. It can listen on any port, proxy through firewalls, sweep networks, query adapters, and generally exploit NetBIOS by manipulating the service value flag in NetBIOS packets. Although these functions are all part of the specified NetBIOS service, NBName.exe allows manipulation of NetBIOS packets that was not intended to be available at an application level.

3. Protocol Description:

The NetBIOS protocol is used for name resolution and management on TCP/IP networks using UDP packets and port 137 by default. Both local network and Internet operation are supported, in connection (session) and connectionless (datagram) services, broadcast and multicast modes. NetBIOS Name service is flat and uses 16 alphanumeric characters, consisting of 15 uppercase characters followed by a one-byte value (the service value).

Registration of NetBIOS names is handled on a bid basis, and contention for a name is handled in real time. When no objections are received during the Name Registration stage, implicit permission is assumed. Any application can register and use any name and value assuming the name is unique, and not already in use on the network. The NetBIOS service broadcasts a Name Registration Request to determine if a name is already in use. If a name is already in use, the machine owning the name will reject the Name Registration Request and deny the registration attempt. Each machine on the network maintains a list of names that it owns and is responsible for defending, and will deny requests for registration of names within it's list. If a machines detects a name conflict, it will mark the node in it's local table as being in conflict. The only valid user function against a marked name is Delete Name.

© SANS Institute 2000 - 2005, Author retains full rights.

4. How The Exploit Works:

NBName.exe has many functions, for denial of service, mapping of NetBIOS namespace, and enumeration of other NetBIOS nodes.

4a.*Denial of Service:*

Options: /QUERY, /CONFLICT, /RESPOND, /DENY

Machines which abuse the NetBios protocol can disable NetBIOS networks by causing name conflicts. By denying all name registration requests, NetBIOS nodes will repeatedly attempt to register their NetBIOS name. On Windows machines, a name conflict results in a reboot, thus if an attacker can prevent successful name requests from occurring, he/she can can effectively isolate a NetBIOS node from the network, disabling communication with other NetBIOS nodes.

Due to the connectionless nature of the NetBIOS protocol, any machine can respond to Name Registration broadcasts. This can lead to spoofing of machine names, since a rogue machine could impersonate another legitimate node by first causing denial of service to the legitimate node. Once that node has been disabled, an attacker could then spoof the name and impersonate the legitimate machine. In networks where DNS is also used, one must first disrupt DNS. Once that is accomplished, Windows machines will attempt to use NetBIOS to resolve names, and spoofing as described above can occur.

Using the QUERY option, a name query can be broadcast, flooding machines who listen for NetBIOS requests.

The CONFLICT option sends a release packet to a machine for a name that is registered, and the attacked machine marks the sent name in its table as being in conflict, and stops using it. When an adapter status response is received by NBName on the attackers machine, it will send a release packet for the name that is in conflict, which disables NetBIOS networking on the victim machine, requiring a reboot.

RESPOND allows an attacker to answer name queries. Using a wildcard, one can respond to all names, or a specific list of names can be used. This option is useful for spoofing, where the /RESPONDIP flag is used, which can substitute the attackers IP for a name previously registered to a legitimate machine.

© SANS Institute 2000 - 2005 Author retains full rights.

The DENY switch is self explanatory. It is used to deny all name registration requests on the network. Again, using wildcards one can deny all name registrations, or provide a list of specific names to deny.

4b. *NetBIOS Mapping:*

Options: /QUERY, /SWEEP, /SVCDESC,

Using the SWEEP option, an attacker will send adapter status requests to all IPs from *StartIP* to *EndIP* (even within a range that extends past a Class C network address block).

4c. *NetBIOS Node Enumeration:*

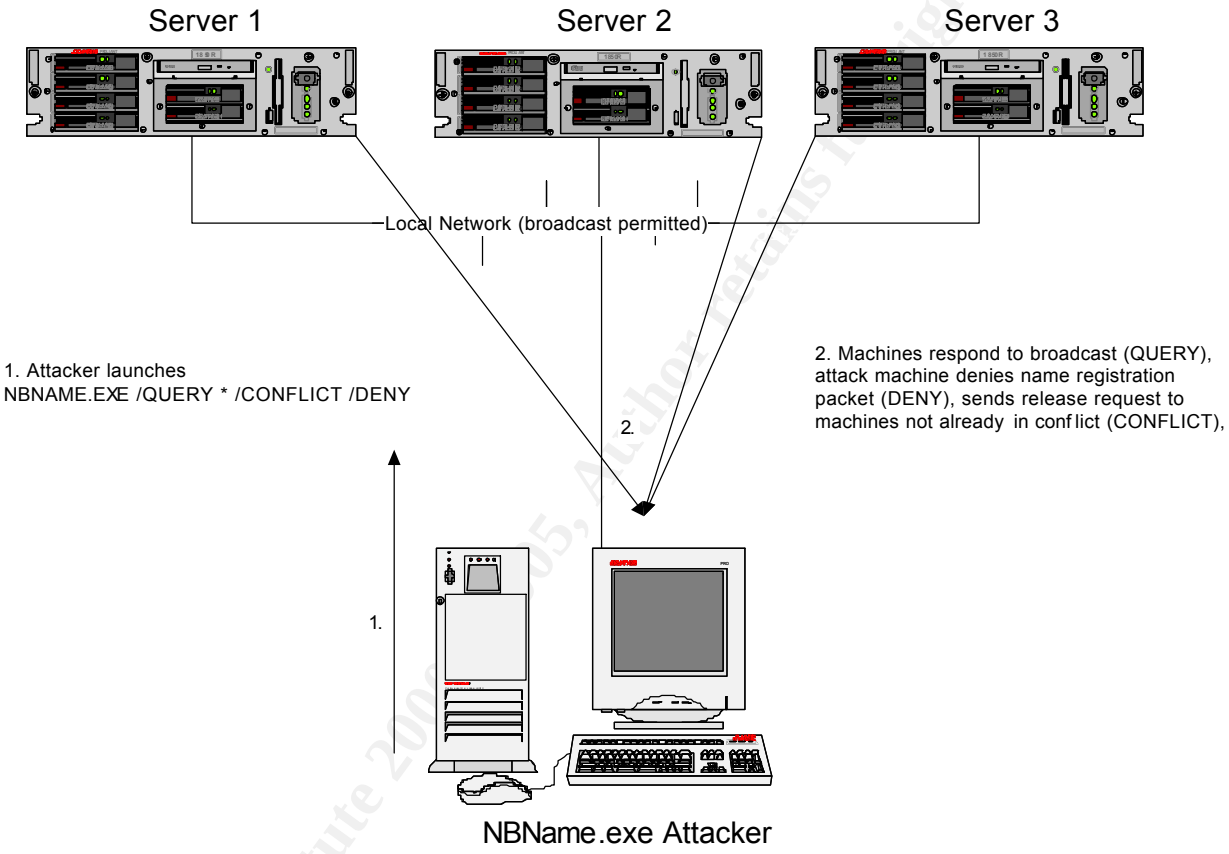
Options: /QUERY, /SCAN, /SVCDESC, /RESPOND, /ASTAT, /ASTATBACK

Using the SCAN option, an attacker can flood packets to a range of IP Addresses, and those machines with NetBIOS name services running will respond. The SCAN option will send adapter status requests to all IPs listed in the referenced IPLIST file. This IPLIST file is generated using the SWEEP option. This list can be used later by other tools that further assist in NetBIOS enumeration (see donete.bat).

© SANS Institute 2000 - 2005 Author retains full rights.

5. Diagram of exploits on network:

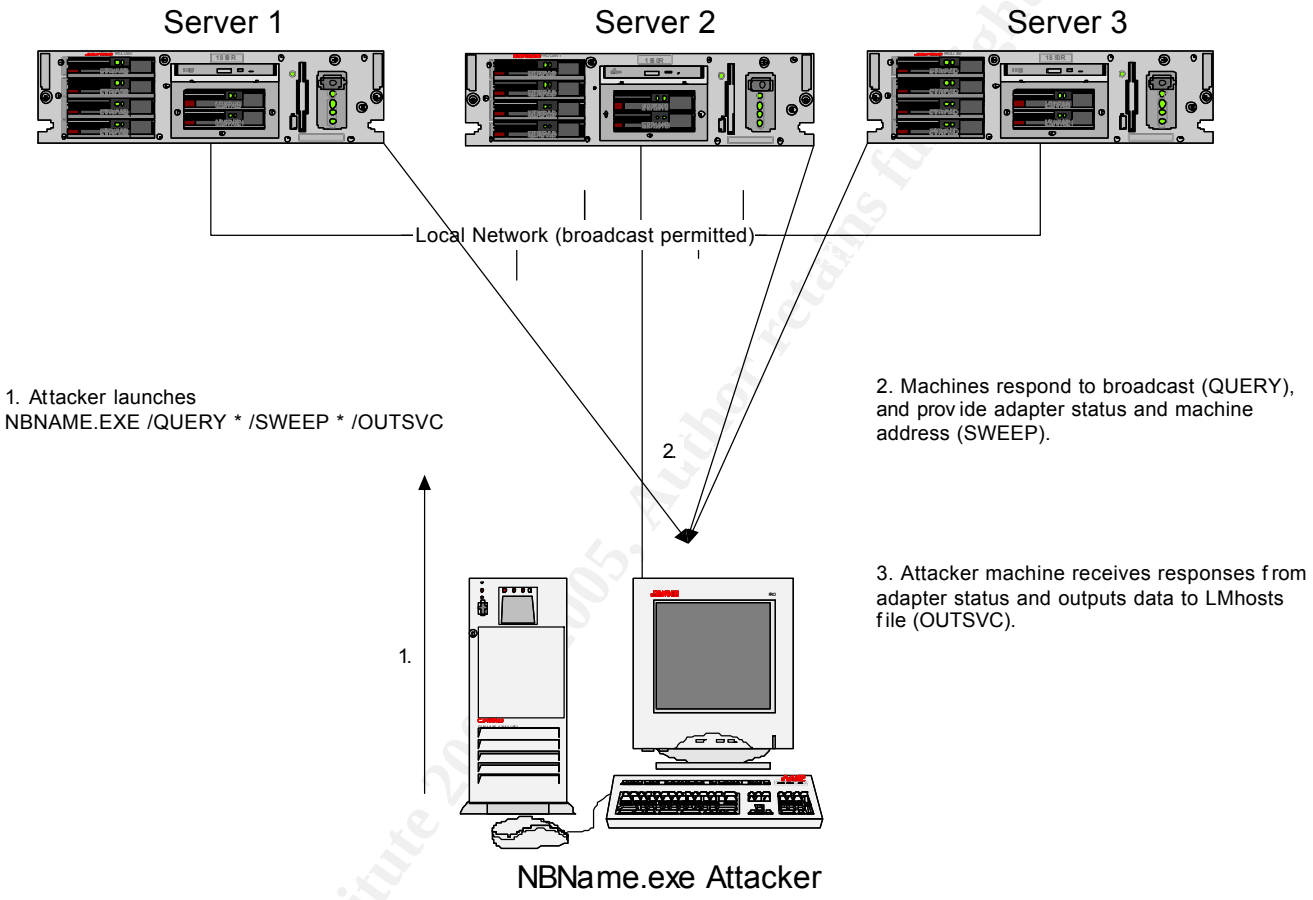
5a. Denial of Service



© SANS Institute 2000 - 2005, Author retains full rights.

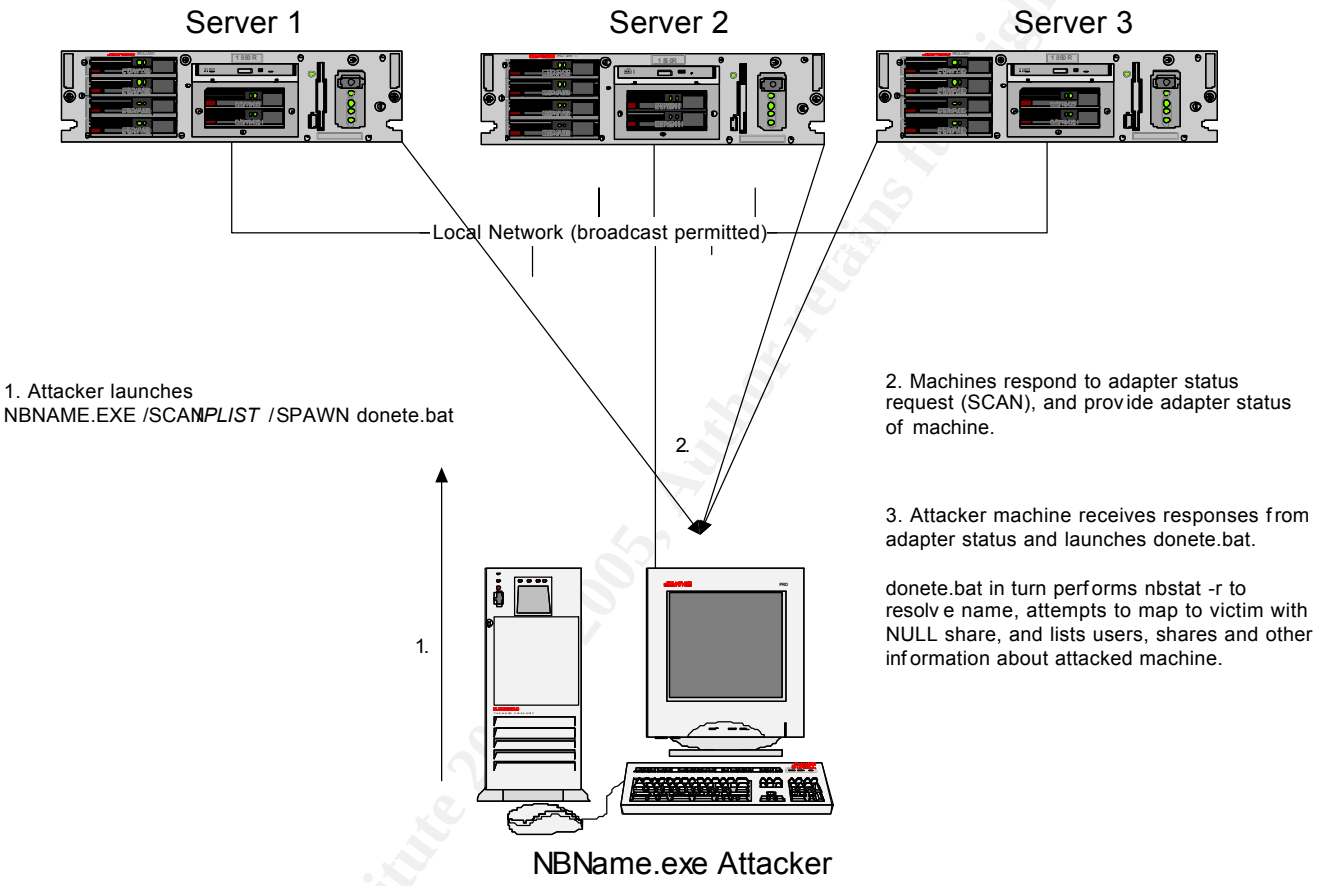
© SANS Institute 2000 - 2005 Author retains full rights.

5b. Mapping NetBIOS Namespace



© SANS Institute 2000 - 2005 Author retains full rights.

5c. Node Enumeration



© SANS Institute 2000 - 2005 Author retains full rights.

6. How to use NBNames.exe

There are many ways to use the NBName.exe tool. The typical use would be on a local segment, to manipulate a local NetBIOS network. The broadcast nature of NetBIOS, and the fact that is uses UDP 137 by default leads to the standard practice of using NetBIOS strictly for local area networks. Most firewalls are configured to deny UDP traffic, and many companies prevent broadcast traffic from crossing subnets. However, NBName also has some clever options that enable it to work through proxies and firewalls! There are switches to enable NBName.exe to listen on ports other than UDP 137, and options to route UDP through a SOCKS 5 proxy server. Details of the more useful switches are as follows:

/PORT – Assign the port that NBName.exe will list on for connections.

/DESTPORT – Send packets to a destination port other than 137. This would be useful in bounce attacks, where a compromised machine using netcat or some other re-director is listening on a non standard port. Especially effective for traversing firewalls through other default ports. For example, re-directing NetBIOS through UDP 53, which is usually open for DNS.

/PROXYIP, /PROXYPORT, /PROXYUSER, /PROXYPASS – Route UDP traffic through SOCKS 5 proxy, specify the proxy server address, user account and password.

/QUERY – Broadcast a name query and resolve name to address. Wildcards can be used.

/ASTAT, /ASTATBACK – Report adapter status and send status request to any machine that responds to a name query. Used in combination with /QUERY and /CONFLICT.

/REVERSE – When the attacker machine receives a name query, this option enables custom responses, where the attacker can manipulate the usual response with something contrived. Use in combination with other options to mask the attacking machine, disable NetBIOS networking of anyone who requests a status of the attacker, use with /SPAWN to execute a script or program in response to the query. Use /NOLOCALNET and /NOLOCAL with this command to prevent packets from be process on the attack machine, so the attacker doesn't fall victim to it's own abuse.

© SANS Institute 2000 - 2005 Author retains full rights.

/OUTSVC – append information to a file including machine name and service value in the format of LMhost file.

/RESPOND – allows one to answer name queries received on the attack machine. Can respond to all queries, or only specified machines included in a file. Can be used with /RESPONDIP to spoof the response to appear to come from a different IP address.

/ALLOW, /DENY – These options allow the attacker to manipulate name registration requests. Use /DENY to block all requests, except those specified with the /ALLOW switch.

7. Signature of the NBName.exe Attack:

For the most part, NBName.exe makes acceptable use of the NetBIOS protocol, thus there is not a true "exploit" of the protocol to detect in any single packet. However, analysis of multiple packets should reveal abuse of the protocol, such as multiple name requests within a short time, or extended periods of conflict negotiation between a single node and the rest of the network. A search of the websites for ISS Real Secure, Cisco Netranger, and Max Vision's WhiteHats did not reveal any documented attach signatures for the respective Intrusion Detection products. Whitehat did have signatures for netbios-name-query at http://www.whitehats.com/IDS/177, and ISS lists some information about NetBIOS spoofing at http://xforce.iss.net/static/5035.php but it is little more than a summary found at the Microsoft Site. Obviously, none of these sites make reference to the power of nbname.exe, and the versatility the tool has for various NetBIOS network exploits.

8. How to protect against NBName.exe:

Standard security practices suggest that Windows networking ports and protocols should be blocked from external networks by a firewall or Access Control Lists and packet filters at the router level. The default port that NetBIOS uses is TCP/UDP 137, thus these ports should be denied at the firewall level.

Patches have been released for Windows NT and Windows 2000 systems. These are available from the links listed below from the Microsoft homepage.

Note: There are no patches available for Windows 9x systems. According to the creator of NBName.exe, as stated on the description

© SANS Institute 2000 - 2005 Author retains full rights.

page for the application, Microsoft responded to his queries about Windows 9x with the following:

> "Interestingly, nowhere in the bulletin does it mention Windows 9x, even though it is just as affected as any other platform using the NetBIOS protocol over TCP/IP. I asked them why this was and their response was basically that anyone concerned with "security" wouldn't be running Windows 9x anyway."

Given this response, it is recommended that anyone running Windows 9x systems on their corporate network should consider migration away from this operating system, as it appears that Microsoft is not concerned with updating security on that Operating System.

9. Source Code:

NBName.exe - http://pr0n.newhackcity.net/~sd/nbname.cpp

NetE.exe - http://pr0n.newhackcity.net/~sd/nete.cpp

NetB.exe - http://pr0n.newhackcity.net/~sd/netb.cpp

Donete.bat - http://pr0n.newhackcity.net/~sd/donete.bat

10. Conclusion

The NBName.exe application is a thoroughly designed tool that can be used to analyze and manipulate NetBIOS networks. The operating system that is almost exclusively vulnerable to this tool is the various versions of Microsoft Windows. Patches have been released that fix some of the newer versions of the OS, but further investigation reveals that these patches are only partially effective against attack; specifically those exploits that make use of NetBIOS Name Spoofing. The patches do not address the enumeration and mapping that nbname.exe is capable of. Weaknesses in the protocol are the cause of these more manipulative attacks, and thus relying on the NetBIOS protocol for networking leaves the systems that rely on it prone to attack.

11. Additional Information & References:

1. PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: RFC 1001: PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS
http://www.faqs.org/rfcs/rfc1001.html

© SANS Institute 2000 - 2005 Author retains full rights.

2. RFC 1002: PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS
http://www.faqs.org/rfcs/rfc1002.html

3. NetBIOS API and NetE.exe
http://pr0n.newhackcity.net/~sd/netbios.html

4. CERT® Vulnerability Note VN-2000-03
Topic: Denial of Service Attack in NetBIOS Services
http://www.cert.org/vul_notes/VN-2000-03.html

5. Microsoft Security Bulletin (MS00-047)
Patch Available for "NetBIOS Name Server Protocol Spoofing" Vulnerability
http://www.microsoft.com/technet/security/bulletin/ms00-047.asp

6. Common Vulnerabilities and Exposures
CVE-2000-0673 CVE Version: 20001013
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0673

© SANS Institute 2000 - 2005, Author retains full rights.