Global Information Assurance Certification Paper

Security concerns with Microsoft Networking or SMB

Elizabeth Shores
May 27, 2001

Introduction

A weakness is a threat that someone takes advantage of and it becomes a vulnerability. Weaknesses are part of all operating systems. Hardening the systems is the term for attempting to remove well known and preventable vulnerabilities. The only way to have a truly secure machines is for it to be a stand alone. Whenever multiple machines are connected any vulnerabilities become a potential threat. All machines on a network should have current patches applied and as many vulnerabilities removed as possible. Many documents give details on hardening different operating systems. *Appendix A* list some web sites with information on hardening a NT system. Some vulnerabilities cannot be removed because it is required for functionality. If a risk cannot be removed then it should at least be reduced. This is a brief introduction to one type of vulnerability, its exploitation and why applying protection is important.

What is an exploit?

An exploit takes advantage of vulnerabilities inherent in all operating systems. Exploits can be divided into two categories, local or network hacking attacks. Some examples of local attacks are Trojan horses, application's weakness, password grabbing, or obtaining direct access. Examples of network attacks are denial of service, snooping, man in the middle, or web server attacks. The vulnerability and the exploitation that this paper address is the "Man in the Middle" attack. This exploit works as the name implies. A hacker inserts a computer in the communication path between two unsuspecting computers. From this position the attacker can disrupt communication or capture information.

The "Man in the Middle" attacks discussed in this article refers to Server Message Block (SMB), part of Microsoft Networking. This vulnerability is used to attacks Microsoft operating systems with SMBRelay. SMBRelay is an application created by Sir Dysti, a member of Cult of the Dead Cow (cDc). This is the same group responsible for Back Orifice and BO2K. Both are remote control programs used on Windows operating systems. The problem with these programs is they can be hidden and used without the computer user being aware. SMBRelay also can be hidden on a Windows system waiting for a user to connect. It exploits the SMB to enable access by acting as a "man in the middle."

Why does SMBRelay work?

The SMBRelay exploit takes advantage of weakness left in Windows NT for backward compatibility. Different mechanisms are used in these attacks, such as SMB Hijacking, SMB Downgrade (force clear text passwords) and SMB encrypted handshake interception. SMB is an application level protocol used for authentication and file sharing, RPC and CIFS (Common Internet File System). SMB rides on top of NetBios over TCP/IP (NBT) session. It is also carried by UDP. Defending against it is difficult because it binds to port 139, which is needed for NetBios sessions.

Security weaknesses are increased with SMB and CIFS because it includes NULL session, WINS, and network chatter. The protocol gives away too much information and offers too much trust to client machines. A null session is access without a user-name. This is frequently done between machines that exchange RPC through named pipes. A null session means that an anonymous connection can obtain information such as a complete user list. This makes it easier for a hacker because they only have to capture the password. Another weakness is the lack of logging. Microsoft tracks access by computer name and not an IP address. An IP address may be forged but forging a computer name is easier. This makes it hard to use the security principle that if it cannot be prevented then it must be detected.

SMBRelay succeeds because many networks use the older NT LAN Manager (NTLM) authentication instead of the newer NTLMv2. Password-cracking software, like L0phtcrack, exposed security vulnerabilities in NTLM. Microsoft released NTLMv2 in Windows NT 4.0 Service Pack 4 (SP4) which would remove this risk. The problem is most networks do not deploy the newer version. Installation of NTLMv2 requires all machines, both server and clients, be configured. The server should only accept the stronger authentication. NTLMv2 does offer support for Windows 9.x but time and resource are required for deployment. The SMB protocol has also been ported to other operating systems such as UNIX and LINUX. One application for UNIX to use SMB is Samba. When multiple platforms connect, such as Unix or Windows 9.x, WinNT/2K, authentication is usually configured at the lowest level.

Three methods used in SMBRelay

SMBRelay uses different methods for exploitation of Microsoft network machines. Three of these are SMB Hijacking, SMB Downgrade and SMB encrypted handshake interception. Each provides a different way to exploit a design flaw in the SMB protocol.

Method A - SMB Hijacking

SMB hijacking is used to take over a session established between two computers. SMBRelay intercepts a connection from one machine on port 139 and connects back to the target machine on the same port. Packets are sent to the intended receiver, with modification as

necessary. Packets continue to be relayed between the two unsuspecting machines. The relay passes authentication traffic to its destination as a proxy. Once the session authenticates the hijacker can disconnects the user's system and assumes control. The intruder then can use the relay system to obtain access to network resources as the hijacked user.

Method B - SMB Downgrade method

If multiple choices are offered, as with SMB, there is always a method to force things to the lowest level. For backward compatibility, Windows NT supports eight variations of authentication. The oldest variant uses plain-text passwords. By default the client machine suggests the level of security, even if the server suggests a more secure variant. An intercepted request for a session receives a reply that it only understands a clear-text password. The unsuspecting client sends a clear-text password that the hijacker uses for authentication. The password is captured on the wire without any of the parties knowing that the security was lowered.

Method C - SMB encrypted handshake interception

User authentication with Microsoft networking is performed with a challenge/response protocol. This exchange sends password encrypted but it still has security flaws. Even encrypted authentication can be intercepted and used for improper access. The vulnerability exists because of the way that Microsoft stores passwords making them weaker. To retain backward compatibility two passwords versions are stored. One is a LM-hash and the other is NT-native. The NT-native uses MD4 and LM-hash uses a variant of DES. DES is no longer considered secure. Microsoft continues to weaken the password with the storage method. First passwords are converted into all uppercase letters. Next the password is divided into two halves with seven characters each. If necessary the fourteen characters are padded with zeros or Nulls. This creates recognizable patterns. These handling methods weaken the password and make it easier for a program like L0pthCrack to decipher. This is one reason that NTLMv2 should be deployed, so that systems will accept only one form of authentication. Given enough time any password can be decrypted. That is why passwords should be changed periodically.

Additional problems with SMB protocol

CERT® has in the past issued advisories about Trojan Horse programs that also use SMB for an attack. One such program is ExploreZip described in CERT® alert CA-1999-06. This program could delete files that are writeable via SMB/CIFS file sharing. The program searches through the network neighborhood and deletes files that are shared and writeable, even if the shares are not mapped on the infected computer.

Another problem with SMB was identified in November 2000 is Microsoft Network Monitor Multiple Buffer Overflow Vulnerabilities. It is a method of using the native tool to create an exploit. Multiple stack overflows in various function calls may allow a remote attacker to gain control of Network Monitor, execute arbitrary code and gain control of a victim host.

Both examples may be difficult for an amateur to execute but it displays that new vulnerabilities are always being created. These are just a couple of vulnerabilities that use SMB as a method of attack. One was in 1999 the other in 2000. There are many more examples available. With very little research a hacker can obtain information on existing exploits. A known vulnerability can be expanded to be used differently. The report of exploitation with SMBRelay was written in an article April 2001. So although it has been published repeatedly that there are problems with SMB it still causes problems. As stated by the creator of SMBRelay, most of the vulnerabilities are design flaws. It took him less than two weeks to write the program. It has been some time since NTLMv2 was available but it does not get deployed enough to eliminate the problems associated with SMB.

Conclusion

Most of these "Man in the Middle' attacks are known weakness that reappears as new vulnerabilities. One reason the exploits succeed is that systems are not regularly patched. A system with all the latest patches applied is an initial defense against host attacks. Anyone running a Microsoft platform must become familiar with sites that keep current on security vulnerability. One good site where current security bulletins are available is //http:www.microsoft.com/security.

Risk can be decreased but not eliminated with the use of NTLMv2 to strengthen authentication. Currently, NTLMv2 prevent SMBRelay from hijacking user sessions, but may not stop future exploits of Server Message Block (SMB) relays. A better method for prevention against man-in-the-middle attacks is firewalls at the desktop and servers. For additional information from Microsoft on NTLMv2 review the following Microsoft knowledge base articles. http://support.microsoft.com/support/kb/articles/Q147/7/06.asp
http://support.microsoft.com/support/kb/articles/Q239/8/69.asp

This information is aimed at Microsoft networking but other platforms are just as vulnerable. All systems must be current with installation of patches. All resource owners should review their systems regularly to verify that each machine has risk reduce and the system is harden. They should not assume that a firewall is the only level of defense necessary. Multiple layers are better.

References

Thomas C Greene, ***Exploit devastates WinNT/2K security***
http://www.securityfocus.com/headlines/11116

Mark Joseph Edwards, ***SMBRelay: Another Good Reason to Protect Your Internal Network***
http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=20845

Hans Hedbom, ***A Comparison of the Security of Windows NT and UNIX***
http://www.securityfocus.com/library/2086

Randy Franklin Smith, ***Inside SP4 NTLMv2 Security Enhancements***
http://www.win2000mag.com/Articles/Incex.cfm?ArticleID=7072

Bill Stout, ***Known NT Exploits***
http://www.emf.net/~ddonahue/NThacks/ntexploits.htm

Unknown Author
http://pr0n.newhackcity.net/~sd/smbrelay.html

Appendix A

The following is a list of web sites that offer information on hardening NT systems. Each item suggested should be reviewed to determine how it affects business requirements for operations.

The following articles are available from Microsoft.
Windows NT 4.0 Member Server Configuration
Checklist Windows Domain Controller Checklist
Windows NT C2 Configuration Checklist
http://www.microsoft.com/technet/security/tools.asp>

Securing Windows NT (3.5 - 4): Part 1 & Part 2
http://secinf.net/info/misc/boran/nt1.html
http://secinf.net/info/misc/boran/nt2.html

CERT® Security Improvement Modules
http://www.cert.org/security-improvement/#nt

CERT® Coordination Center Windows NT Configuration Guidelines
http://www.cert.org/tech_tips/win_configuration_guidelines.html

CIAC_2317_Windows_NT_Managers_Guide.pdf
http://www.ciac.org/cgi-bin/index/documents

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event