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

Practical Assignment
Version 2.1 (revised April 8, 2002)

SMBdie'em All – Kill That Server

By

Craig Kirby

ABSTRACT

In late August 2002, a remote vulnerability in the Windows SMB protocol was released in a Microsoft Security bulletin. An exploit was released a few days later that would cause Windows NT/2000/XP machines to crash. This GCIH practical is a hypothetical narrative of a disgruntled worker who does not get a promotion he expected and downloads and runs the exploit for several days against his employer. The exploit was verified on a Windows NT Server and Windows 2000 Server running inside VMware 3.2.0 Build 2230.

The paper satisfies Option 1 - Exploit in Action assignment and begins with Part I - The Exploit, giving an overview of the Windows SMB protocol, the exploit and references. The rest of the paper contains Parts II and III within the narrative that details the incident's discovery and handling process.

The narrative describes the company's newly formed IT distributed computing department and the disgruntled worker, details the network layout and the incident's discovery by the IT Security Incident Response team. The paper closes with an Executive Summary of the incident.

SMBdie

Vulnerability:

Microsoft Network Share Provider SMB Request Buffer Overflow
aka Unchecked Buffer in Network Share Provider Can Lead to Denial of Service

BugTraq: 5556
CVE: CAN-2002-0724
Microsoft Security Bulletin: MS02-045

Operating System:

- Microsoft Windows NT 4.0 Workstation
- Microsoft Windows NT 4.0 Server
- Microsoft Windows NT 4.0 Server, Terminal Server Edition
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Windows XP Professional

Vulnerable Protocol:

The SMB protocol is used by all Microsoft's Windows operating systems, since
Windows for Workgroups v3.11, to share network resources such as files and
printers. It is a request-response protocol where the client requests resources
from a server.

Exploit Description:

The exploit sends a specially crafted SMB packet request to a server causing it
to crash. The specially crafted SMB packet is actually a buffer overrun and the
server cannot handle it and crashes with a blue screen of death. The exploit can
be run by either using a user account or using an anonymous connection.

Variants:

Two SMB exploit programs exist (SMBdie and smbnuke) but they exploit the
vulnerability the same way. There are no publicly available variants for this
particular vulnerability.

References:

Microsoft Security Bulletin MS02-045
        http://www.microsoft.com/technet/security/bulletin/MS02-045.asp

Core Security Advisory #CORE-20020618
	http://www.corest.com/common/showdoc.php?idx=262&idxseccion=10

BugTraq Vulnerability Number 5556
	http://online.securityfocus.com/bid/5556

IIS X-Force Advisory #9933
	http://www.iss.net/security_center/static/9933.php

CERT Vulnerability Note VU#311619
	http://www.kb.cert.org/vuls/id/311619

CERT Vulnerability Note VU#342243
	http://www.kb.cert.org/vuls/id/342243

CERT Vulnerability Note VU#250635
	http://www.kb.cert.org/vuls/id/250635

CVE Candidate #CAN-2002-0724
	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0724

SMBdie Exploit
	http://packetstorm.decepticons.org/0208-exploits/SMBdie.zip

SMBdie'em ALL – KILL THAT SERVER

Background:

Three years ago a desktop support guru, who we'll call Terry, was hired into a company with over 20,000 employees. The organization is a Fortune 1000 company that has been around for 85 years. It is very efficient in its business practices and stacks up strong against its competitors. It offers many "one of a kind" solutions for consumers and truly has a niche in the market.

Terry was a very sharp guy and could learn new technology overnight without any real effort. He would usually stay at work late to complete tasks, even if that meant working up to 16 or 18 hours a day. He always helped out his teammates and was considered a walking knowledgebase, so that anyone could ask him computer related questions, and he would almost always know the answer. His interests in technology had no bounds and he strived to learn new things. Several managers quickly recognized his potential value to the company, and realized that he had been misplaced in his current position, desktop support. He could be contributing a lot more by using his skills in an area that was lacking in innovation and expertise. Within a few months of being hired on, he was promoted to be a Windows NT administrator.

For the past few decades, the IT organization at this company had been relying entirely on mainframe technology to power their systems. About a year before Terry was hired, the organization started taking serious notice to the fact that more and more of their competitors were beginning to outperform them by employing new technology. The methods and solutions that came with the new technology brought more efficiency and control to the IT environment. They realized they needed to take the chance, and should request the budget from their business owners, to start embracing distributed computing. The technology was foreign to them, and they did not have experts in their workforce to give them the valuable information to make the right decisions, or take the right precautions.

Management at the organization started seeing the negative results of their lack of planning, organization, or control of their IT environments. They had a vision of how the organization should be run, but they didn't know how to implement it. They hired an outside consulting firm to help them jumpstart the effort to transform their organization into one that employed the principles they envisioned. The downside was that this consulting firm was in the position to cater to the priorities of the organization, giving management what they thought they wanted, instead of what they truly needed. They did not have to worry about securing what they built, nor cared if it ran efficiently, as long as what they gave their client looked good, and met the deadline. The consultants helped the

organization build their LAN and WAN infrastructure along with the Windows NT 4 domain as well as the operating system installations on their servers.

Like many companies, after the terrorist attacks on September 11th, 2001, management realized they needed to get serious about security. They were particularly concerned about the security of their client data, which included legal and financial information and transactions. If this data was attacked, there could be major financial and/or legal repercussions for the organization. Their mainframe environments were already securely protected, but the new distributed infrastructure would be a challenge. Research brought minimal results, since there were very few distributed computing security policies written.

They needed to establish an expert IT Security group for their distributed systems to give them the kind of tools and methods that would maintain the integrity, and protect the vulnerability of their data. The newly formed IT Security group consisted of an Incident Response team, a Vulnerability Assessment team and an ID Management team. Before then they had a rather weak security group that did not have the budget to buy IDS (intrusion detection system) sensors, which would properly monitor the entire network. Now with the appropriate budget, and more headcount, the IT Security group was able to adequately monitor the network. They began performing vulnerability assessments, but the systems were large and still quite unorganized, so it would take some time to complete the assessments. They also started recommending changes to the administrators. These changes would first need to be discovered, analyzed, then budgeted, and finally implemented. It was slow going, but it was a good start.

In an effort to protect the company's liability for any damage done or illegal activities performed by the employees, Human Resources required all current and new employees to sign a waiver stating they would use the computers for business only. However, there was no policy established by the company regarding specific needs such as password change policy, no regulation or procedures to implement new servers, or guidelines or parameters for implementing any new technology. It was almost anarchy. Each IT department was allowed to implement and use whatever they wanted to, without proper planning by the IT organization, or fear of consequences.

Terry was involved in many projects at the company's Call Center that dealt with the network, VPN, NT administration, and special projects. This allowed him to become acquainted with many of the vulnerable areas of the system. Over the course of about 3 years, he was able to document all the shortcuts, backdoors and service accounts that the systems depended on. These were created in the effort to complete projects quickly, to meet the deadlines set by upper management. Terry's role inherently required a trusted source, which Terry had proven himself to be, and therefore, no one hesitated in allowing him to have this information to perform his duties. But the lack of planning and precautionary steps for each of these projects, along with the lack

of consideration of going back to take out the backdoors and replace them with reliable processes resulted in allowing the vulnerabilities to keep piling up.

Terry always had an agenda to help the company fix these holes, but unfortunately, his current manger did not appreciate Terry's skills or recognize the value he had been intended to contribute to this team when he was promoted. His manager never considered his recommendations, nor did he pass them up to management, since he did not understand the benefit they would present. Instead, he assigned daily tasks for Terry to do that did not take advantage of Terry's growing expertise. The tasks were lame and mundane, and began to wear on Terry's motivation. He no longer had the drive to work and co-workers around him were starting to see his attitude change for the worst. He started to come in late to work and leave early. Sometimes he wouldn't show up for key meetings and his excuses were always the same. Even with all of this he was tolerated because he did great work, very efficiently and fast. Terry's other co-workers were very discouraged about his attendance and professionalism and complained many times to his manager and Human Resources.

After being an NT administrator for two and a half years Terry felt he was stuck in his current position working for the same manager. He was ready to leave his position and look for another internal IT position that would provide more of a challenge to him. With the recent establishment of the IT Security team he thought that would be a perfect position. This new IT Security position would require relocation to the company's headquarters and IT data center, which was located in a large metropolitan city. His promotion included a pay increase for the difference in cost of living of moving to the headquarters location, which was 1200 miles away. While Terry's attendance and professionalism was lacking, his technical performance was superb; plus he had befriended the current manager of IT Security in a previous project. The IT Security manager said he was a shoe-in for a position paying salary of $25,000 more than he was making currently.

Several months went by and a few phone calls later Human Resources and IT Security were ready for Terry to start. On August 23rd, 2002 he got a call from the Director's of IT Security Administrative assistant saying to come on out as soon as possible. Terry was so excited that he traded in his old car for a new SUV and on Monday he left on the long drive to the headquarters. After two days of driving he got there on Tuesday night and stayed at another NT administrator's house.

Terry showed up for his new job on Wednesday but found out that his friend, the IT Security manager, was no longer manager and actually moved to another department just a few days before. A new IT Security manager was there and he was new to the company. Terry was a little disappointed but figured it would be alright. About a week of being in the new location and beginning to work on Security policies and procedures his manager gave him the offer letter

for the promotion, indicating his new salary. Terry's mouth dropped because the offered salary was thousands of dollars short of the amount he had agreed to with the old IT Security manager. The new manager said he knew nothing about the old agreement and Terry went marching to the Human Resources department demanding help.

Human Resources contacted the Director of IT Security and they agreed that they would not raise the salary. To cover herself, the HR manager lied and said she had advised Terry of what was going on during the whole relocation process. Terry did not recall anybody advising him especially anybody from Human Resources. What was decided is that Terry could stay with the current salary offered or he could drive 1200 miles back to his previous location, the company would pick up all the expenses incurred, and he would have his old position back. He was very upset as he had been looking forward to the increase in pay since he had just bought a brand new $30,000 SUV. He definitely did not want to stay but he also did not want to go back to his old position. After a few days of thinking about it, he packed up everything into his SUV and drove back to his old location. Human Resources decided to let him stay at home on stress leave for a month to let him get his life back in order after the long roundtrip drive between locations. Terry's NT id was deactivated for the month he was at home. Terry was quite shaken and upset over the whole move and miscommunication.

* * *

Network Diagram and Description:
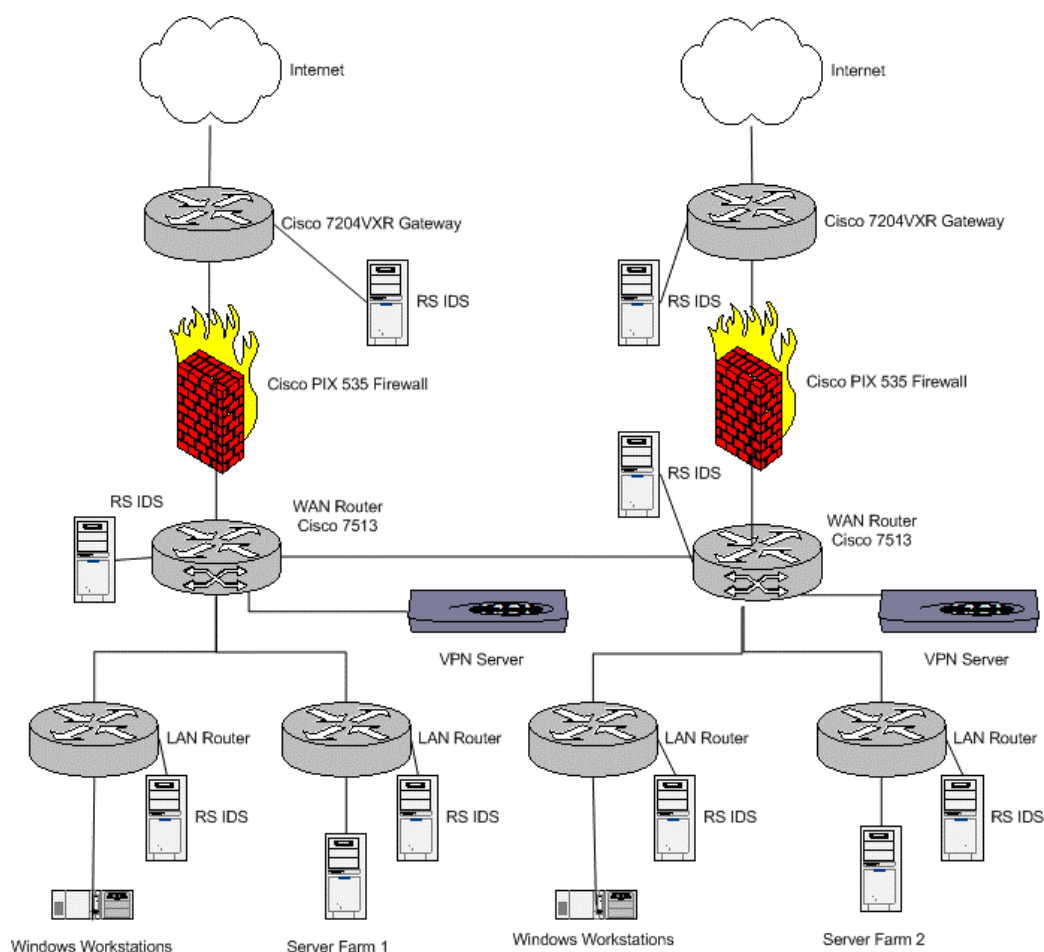
- *Gateways:* Cisco 7204VXR Gateway, IOS version 12.2

- *Firewalls:* Cisco PIX 535 Firewall, IOS version 12.2. Deny all, allow by exception.

- *Intrusion Detection Systems:* Internet Security Systems RealSecure version 7.0 on Windows 2000 servers.

- *WAN Routers:* Cisco 7513, IOS version 12.2

- *LAN Routers:* Cisco 2514, IOS version 12.2

- *VPN Servers:* Nortel Contivity 4600 Secure IP Services Gateway

- *Server Farm 1:* Contains a total of 170 Windows servers (114 Windows NT servers and 56 Windows 2000 servers). This is the first server farm

that was implemented with distributed computing at the organization, and contains mostly older projects. As projects move forward, these servers are being upgraded and migrated over to the second server farm for a scheduled renovation of the server room they are in now. By August of 2002, all Windows NT servers had been upgraded to Service Pack 6a and all Windows 2000 servers were at least at Service Pack 1. Individual security patches and hotfixes were not applied unless there was a performance issue with the server and it was deemed that the patch would help.

- *Server Farm 2:* Contains a total of 290 Windows servers (26 Windows NT servers and 264 Windows 2000 servers). This is the new server farm hosting all the new projects. By August 2002, all Windows NT servers were at Service Pack 6a and all Windows 2000 servers were at least at Service Pack 1. Again, individual security patches and hotfixes were not applied unless there was a performance issue with the server and it was deemed that the patch would help.

- *User Segment 1:* Headquarters workstation segment containing 2000 Windows 98, Windows NT and Windows 2000 users.

- *User Segment 2:* Remote Call Center containing 2500 Windows 2000 users.

* * *

Description and Diagram of the Initial Attack:

Early Thursday morning, September 5th 2002, while Terry was still on leave, three non-critical Windows servers got blue screens of death for no reason. Initially the NT team was stumped. These servers had blue screens of death in the past but not all of them within the same hour or even the same day. After a simple reboot the servers came right back online and continued to perform as if nothing was wrong or had happened to them. The team wrote down, on a piece of paper, each of the blue screen error codes.

Not much research went into finding what caused these blue screens, because the NT team suspected it was a result of the Netfinity Director [1] upgrade that had been performed on these servers the Saturday before, during the scheduled weekly change control window. A few hours later that same morning, all the same servers got another blue screen of death along with an additional four servers. At this point it was decided to stop all the Netfinity Director services that had received the upgrade over the weekend. One of the NT administrators wrote a script to stop all the Netfinity Director services throughout the company.

---

[1] http://www-1.ibm.com/servers/eserver/xseries/systems_management/director_4.html

It took about 45 minutes for the script to be written and finished executing. Several hours went by and there were no more blue screens of death, so they assumed that it was the Netfinity Director upgrade.

Later that afternoon, the NT team lead contacted IBM to get some answers, and asked if any other companies had this experience. IBM said they did not have a record of any other client having the same or similar problems. To verify whether it was in fact a Netfinity Director problem, and to aide in troubleshooting the issue, IBM instructed the NT team lead to downgrade the servers to the previous version of Netfinity Director.

The NT team lead did not bother to contact the IT Security group because he and his team members were convinced that it was a problem with the Netfinity Director upgrade; the thought of it possibly being an attack did not cross any of their minds. After all, they thought any attack from the Internet or an internal source would have been picked up by the IDS sensors, wouldn't it?

That same Thursday night, all of the Netfinity Director services were left turned off and disabled all night on all of the Windows servers. Friday morning came and the NT administrators found twenty Windows NT and Windows 2000 boxes that had crashed with a blue screen of death, all within an hour of each other. Each of these servers had different purposes, and ran applications and services for different responsibilities. In addition, the servers were split into two different server farms. There was no apparent connection that could have caused them to all crash together within the same hour. Now the NT administrators began to get nervous. They were under pressure from management to get the issue resolved and restore the system to full availability. Was Netfinity Director the problem after all? Their confusion over the illusive cause of the problem drove the NT administrators to begin asking other departments for assistance.

The first group they approached was the IT Security Incident Response team. The Response team treated the blue screens of death as an attack from the first word. They took the initiative and secretly installed four RealSecure IDS sensors and a few Honeypots in the server farm. They were hoping they would find something suspicious coming across the wire. They also took digital pictures of the remaining Windows NT and 2000 blue screens for evidence.

Windows 2000 Blue Screen of Death:

```
*** STOP: 0x0000001E (0xC0000005,0x804B818B,0x00000001,0x00760065)
KMODE_EXCEPTION_NOT_HANDLED

*** Address 804B818B base at 80400000, DateStamp 384d9b17 - ntoskrnl.exe
Beginning dump of physical memory
Physical memory dump complete. Contact your system administrator or
technical support group.
```

Windows NT Blue Screen of Death:

```
*** STOP: 0x0000001E (0xC0000005,0x801891F7,0x00000001,0x00760065)
KMODE_EXCEPTION_NOT_HANDLED*** Address 801891f7 has base at 80100000 - ntoskrnl.
exe

CPUID:GenuineIntel 6.8.a irql:1f   SYSVER 0xf0000565

Dll Base DateStmp - Name                    Dll Base DateStmp - Name
80100000 37e8005b - ntoskrnl.exe            80010000 36c49893 - hal.dll
80001000 3738c634 - atapi.sys               802dc000 3784f875 - SCSIPORT.SYS
8001d000 31ed06b4 - buslogic.sys            80008000 36c4a0ae - Disk.sys
8000c000 375704e5 - CLASS2.SYS              802e5000 36e5f31c - intlfxsr.sys
8038c000 37c5705c - Ntfs.sys                f5a88000 31ec6c8d - Floppy.SYS
f5a98000 36c4a0a5 - Cdrom.SYS               f5d0e000 36c4ac16 - Fs_Rec.SYS
f5dc9000 31ec6c99 - Null.SYS                f5c7c000 37850196 - KSecDD.SYS
f5dca000 36c49d58 - Beep.SYS                f5ac8000 36c49f40 - i8042prt.sys
f5c84000 37792481 - mouclass.sys            f5c8c000 3779244a - kbdclass.sys
f5ae0000 36c49ce5 - VIDEOPRT.SYS            f5ca0000 3cadf71d - vmx_svga.sys
f5ca4000 36c49de6 - vga.sys                 f5af8000 37499980b - Msfs.SYS
f5800000 37b8c458 - Npfs.SYS                f4fff000 37c57060 - NDIS.SYS
a0000000 37e86733 - win32k.sys              f5b70000 3cadf722 - vmx_fb.dll
f4ff3000 31ec6e6c - TDI.SYS                 f47ce000 37c57064 - tcpip.sys
f47af000 37c57066 - netbt.sys               f5af4000 31ec6e04 - amdpcn.sys
f479e000 382b6ad7 - afd.sys                 f5b40000 376883f06 - netbios.sys
f5910000 378502e9 - Serial.SYS              f470d000 37af3126 - rdr.sys
f46d2000 37c57062 - srv.sys                 f4696000 37c6d082 - mup.sys
f4626000 377801b1 - Cdfs.SYS                f5a90000 3c7e6601 - npf.sys

Address  dword dump  Build [1381]                         - Name
f4769ab8 801891f7 801891f7 00000001 00760065 80137602 f4769ae8 - ntoskrnl.exe
f4769ac4 80137602 80137602 f4769ae8 8013b15f f4769af0 00000000 - ntoskrnl.exe
f4769acc 8013b15f 8013b15f f4769af0 00000000 f4769af0 f4769f6c - ntoskrnl.exe
f4769af4 80142eee 80142eee f4769f6c f4769b9c f4769f6c f4769b9c - ntoskrnl.exe
f4769b0c 80142f02 80142f02 f4769f6c f4769ba0 801345bb f4769d80 - ntoskrnl.exe
f4769b18 801345bb 801345bb f4769d80 f4769f6c f4769bbc f4769b9c - ntoskrnl.exe
f4769b2c 8013b114 8013b114 00760065 00760065 f4769d94 8014e408 - ntoskrnl.exe
f4769b3c 8014e408 8014e408 f4769e24 807f7dc8 801732b9 807ed728 - ntoskrnl.exe
f4769b48 801732b9 801732b9 807ed728 801727b6 809b8d18 00000000 - ntoskrnl.exe
f4769b50 801727b6 801727b6 809b8d18 00000000 000000e4 80a265c0 - ntoskrnl.exe
f4769b94 801192db 801192db 00000001 00000000 f4769d64 801192f2 - ntoskrnl.exe
f4769ba4 801192f2 801192f2 f4769bbc 00760065 00760065 - ntoskrnl.exe
f4769bfc 801369fa 801369fa 801927ca 801358be e13b8dc0 801353d4 - ntoskrnl.exe
f4769c00 801927ca 801927ca 801358be e13b8dc0 801353d4 e13b8dc0 - ntoskrnl.exe
f4769c04 801358be 801358be e13b8dc0 801353d4 e13b8dc0 9cdc0100 - ntoskrnl.exe
f4769c0c 801353d4 801353d4 e13b8dc0 9cdc0100 f4769e24 808f9008 - ntoskrnl.exe

Beginning dump of physical memory
Physical memory dump complete.  Contact your system administrator or
technical support group.
```

Interviews of the NT administrators and IT Operations were conducted by the Incident Response team to get the facts and time line straight. Terry was one of the NT administrators interviewed, over the phone, and he seemed concerned and said that the causes were probably the Netfinity Director upgrade. The rest of the day, Friday, went rather smoothly compared to the past 36 hours; there weren't any more blue screens of death. Since they had not received any other explanation from any of the other departments, and because they were unaware of the steps the security team had taken besides interviews, the NT team documented all of the previous crashes as a Netfinity Director problem. Saturday's change control window came around and Netfinity Director was downgraded on all servers. The Netfinity services were re-enabled and the network seemed safe.

Meanwhile, the Incident Response team was still on the case and was researching on the Internet, using all of the information they had, which was just a few digital pictures of a blue screen on Windows NT and Windows 2000 servers. There was no other evidence or signature left behind on the servers from these possible attacks. After doing some searching on BugTraq and Google, they found something that looked like it could be the cause. One of the pages linked to an advisory sent out by Microsoft on August 22, 2002, Microsoft's Security Bulletin MS02-045.[2] It said that an attacker could send a specially crafted SMB packet request to a server causing it to crash with a blue screen of death. The SMB packet could be sent by either using a user account over the network, or using an anonymous connection. They finally found an exploit written to take advantage of this vulnerability on Sunday when they found SMBdie on PacketStormSecurity.org [3] that was posted on August 26th, 2002.

* * *

Protocol Description:

The SMB (Server Message Block) protocol is used by several different products including Windows, Samba, LAN Server and Manager for OS/2 and a few others. Microsoft has been using SMB since Windows for Workgroups v3.11 to share networked resources such as files and printers. SMB runs on the Application and Presentation level of the OSI model. It can be used over TCP/IP, NetBEUI and IPX/SPX. The Windows NT/2000/XP service that listens for SMB requests is the Lanman server service.

How the exploit works:

The exploit consists of establishing a valid SMB session to a Windows NT/2000/XP system, and then sending a specially crafted transaction packet to request the NetServerEnum2, NetServerEnum3 or NetShareEnum functions. In

---

[2] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-045.asp
[3] http://packetstormsecurity.org/0208-exploits/SMBdie.zip

the SMB transaction packet, if either or both "Max Param Count" and "Max Data Count" values are equal to zero, then the server miscalculates the length of the first buffer. This causes the next chunk in the heap to be overwritten. Once the first buffer is released then the heap will be in an inconsistent state and will cause a blue screen of death.

<div align="center">* * *</div>

The Incident Response team set up a Windows 2000 server and a Windows NT server to conduct testing with the SMBdie exploit. No patches or service packs were installed and SMBdie was fired up. The IP address and NETBios name of the host is required for the exploit to work. Once the test machines' names and IP addresses were entered, they hit the Kill button.

Screenshot of SMBdie exploit:
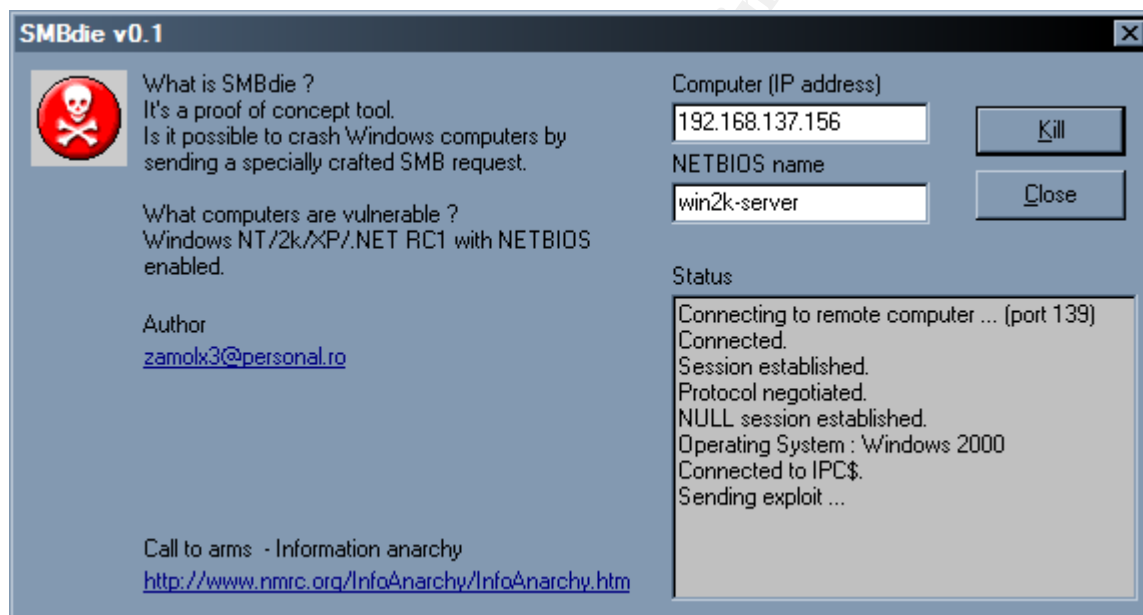
Signature:

Internet Security Systems Security Alert [4] recommended adding the following user-defined event to their RealSecure IDS sensors:

alert tcp any any -> any 139 (msg: "DoS SMB";flags: A+;
content:"|504950455c4c414e4d414e00|";)

This string was the hex equivalent of "PIPE\LANMAN " as that is the string used in the SMBdie exploit. The security team verified the string by sniffing the

---

[4] http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21061

network on their test machines while they ran the exploit and also while establishing legitimate SMB connections. They certainly did not want to cause confusion by having the wrong signature defined in the IDS sensor, causing a bunch of false-positives.

Bad SMB Packet:

```
* 00 50 56 43 | D3 01 00 D0 | BC EE 03 08 | 08 00 45 00 [.PVC.........E.]
* 00 97 93 4C | 40 00 3F 06 | 4E 89 0A B0 | 34 CA 0A B0 [...L@.?.N...4...]
* 0F 62 80 5D | 00 8B 59 69 | 2B 78 7E 5A | 96 22 80 18 [.b.]..Yi+x~Z."..]
* 16 D0 63 DA | 00 00 01 01 | 08 0A 00 10 | BC 4D 00 00 [..c.........M..]
* 0C 0E 00 00 | 00 5F FF 53 | 4D 42 25 00 | 00 00 00 00 [....._.SMB%.....]
* 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 08 00 [................]
* 04 24 08 00 | 00 00 0E 00 | 13 00 00 00 | 00 00 00 00 [.$..............]
* 00 00 00 00 | 00 00 00 00 | 00 00 13 00 | 4C 00 00 00 [............L...]
* 5F 00 00 00 | 00 5C 50 49 | 50 45 5C 4C | 41 4E 4D 41 [_....\PIPE\LANMA]
* 4E 00 68 00 | 57 72 4C 65 | 68 00 42 31 | 33 42 57 7A [N.h.WrLeh.B13BWz]
* 00 01 00 E0 | FF          |             |             [.....]
```

Good SMB Packet:

```
* 00 50 56 C0 | 00 08 00 50 | 56 71 80 41 | 08 00 45 00 [.PV....PVq.A..E.]
* 00 A2 05 6C | 40 00 80 06 | 60 FB C0 A8 | 89 9C C0 A8 [...l@...`.......]
* 89 01 04 08 | 00 8B A3 03 | 30 E0 58 0A | A7 FC 50 18 [........0.X...P.]
* 42 79 B8 7D | 00 00 00 00 | 00 76 FF 53 | 4D 42 25 00 [By.}.....v.SMB%.]
* 00 00 00 18 | 08 07 00 00 | 00 00 00 00 | 00 00 00 00 [................]
* 00 00 08 03 | 01 B8 08 02 | 06 E0 0E 00 | 1A 00 00 00 [................]
* 08 00 68 00 | 00 00 00 00 | 00 13 88 00 | 00 00 1A 00 [..h.............]
* 5C 00 00 00 | 00 00 07 00 | 00 00 5C 00 | 50 00 49 00 [\.........\.P.I.]
* 50 00 45 00 | 5C 00 4C 00 | 41 00 4E 00 | 4D 00 41 00 [P.E.\.L.A.N.M.A.]
* 4E 00 00 00 | 00 00 68 00 | 57 72 4C 65 | 68 44 4F 00 [N.....h.WrLehDO.]
* 42 31 36 42 | 42 44 7A 00 | 01 00 68 10 | 00 02 00 00 [B16BBDz...h.....]
```

How to protect against it:

There were several recommendations listed on Core Security Technologies' website. The best recommendation was to apply Microsoft's

Unchecked Buffer in Network Share Provider patch for both operating systems. During the tests the Security team applied the Microsoft patches to both servers and ran the exploit again. Neither of the servers crashed, and the exploit status window said that the exploit did not work. The patch for Windows NT/2000/XP replaces one file, xactsrv.dll, located in the %systemroot%\system32 folder, with a version that is not susceptible to this exploit.

Other recommendations were to block all TCP ports 139 but that was obviously not suitable, because that port is used by legitimate file and print sharing on Windows servers and clients across the network. Disabling the Lanman server service was also an inappropriate option for many of their Windows servers because they would lose their ability to share resources over the network. The last recommendation was to disable null sessions. That would only deny anonymous users from crashing the Windows machines, but any authenticated users would still be able to crash the system. The Security team decided that this registry change would only be a partial fix, and might cause unforeseen problems on domain controllers and file servers. It also would not stop authenticated users from using this exploit to crash a server.

Suggested Workaround Registry Change:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA "restrictanonymous" should be set to 1 to disable null sessions.

Preparation:

The Security Incident Response team had been established only nine months before this incident occurred. The team consisted of three members and two of them were new employees to the company. The third member had been employed for a few years and had about a year of security experience under his belt. There weren't many policies or procedures written for security at the organization but one of the first they defined was the incident handling process. The incident handling process required that the team:

- Support active intrusion detection
- Maintain the intrusion detection infrastructure
- Disseminate information on protective measures to take against existing or upcoming security threats.
- Provide information on upcoming technology that may pose security threats.

The three members of the Incident Response team used the principles they had learned in Security classes, and incorporated an outline they had learned from a SANS Institute course which one of them had taken. The course book SANS Institute Track 4.1 Incident Handling gives six primary phases of incident handling:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Identification:

The Incident Response team approached the NT team lead with their findings about the vulnerability and the exploit they thought was used. He confirmed that the Microsoft patch had not been installed any on servers, because the vulnerability patch alert was rather new and they did not consider it critical at the time. They were always rather late applying patches and unless it was required for production performance, patches were not to be applied for fear of negative impact on performance. The Incident Response team requested the team lead to come up with a plan to patch the servers, and instructed him not to tell anyone else on his team of the findings. At this point they were pretty sure it was an inside job and the NT team lead agreed not to tell anyone even though he was put into a tight spot of either stabilizing the environment or letting Security catch the attacker. It would take some time to patch 460 servers so he started developing a plan to secretly patch the servers in the shortest amount of time.

The blue screens of death started back up again on Sunday afternoon at a rapid pace. Servers on the network were going down in batches of twenty to thirty at a time. The RealSecure IDS sensors were able to pick up the signature of the attack, and traced it down to a workstation on the first floor of the IT building in which the Security team was based. This proved that the SMBdie exploit was being used and it was definitely an internal attacker on their network.

Containment:

The Incident Response team lead ran to his desk and got the jump bag which included:

```
Two dual boot laptops (Windows 2000 and Linux)
ZIP 250 drive w/ disks
Micro tape recorder
Disposable and digital camera
CD with full of Windows and Linux utilities
Backup software
Forensic software
4 port hub and patch cables
Incident Handling Forms
Zip lock bags
```

```
Marker pens
Notebook
```

The other two team members hurried down to the first floor, but when they got to the identified Windows NT workstation, no one was sitting in front on it. So they asked the people sitting nearby if anyone had been using the computer at any time that day. Their responses were all "no." They assumed it must have been remotely controlled during the attack, so they used their security authority to confiscate the workstation, by pulling the cables and bringing it to their security lab. They plugged their laptop into another network jack and did a reverse name lookup on the workstation's IP address to find the NetBios name of the workstation. Then they replaced the suspected workstation with one of their own test desktops, booted up, renamed the NetBios name, and assigned it a static IP address, using the same name and IP address as the confiscated workstation. The test desktop already had a sniffer installed and running, so now they had a trap waiting for the attacker to make a connection again.

The Incident Response team made two Ghost forensic copies of the hard drive from the confiscated workstation by doing the following. They first installed a second unformatted hard drive as a secondary master. Then using a Windows 98 boot disk and Symantec's Ghost Enterprise v7.5 [5] a copy of the original hard drive was made. They ran Ghost with the "-id" switch to enable Ghost's forensic mode.

Command line for Ghost:

```
Starting Windows 98...


Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1998.

A:\>ghost -clone,mode=copy,src=1,dst=2 -sure -id_
```

---

[5] http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=3

Ghost in action:
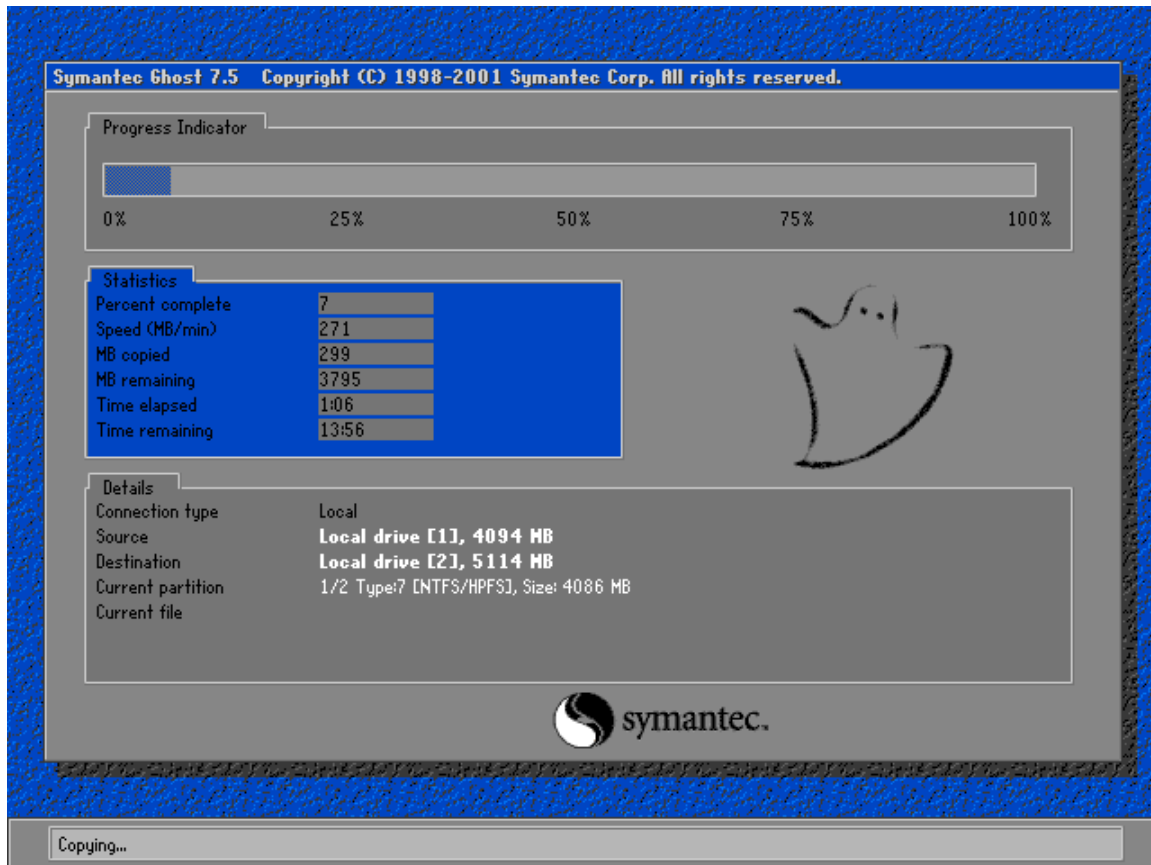
The same process to copy the first hard drive was done again to get a second copy of the original drive. Before the second hard drive copy was started, the team lead (the most experienced member of the team) installed the first copy as the secondary master hard disk into his investigation computer and inserted his bootable NTFSPro [6] DOS boot disk. After NTFSPro was loaded, what would be the C:\ drive of the confiscated workstation was assigned to the E:\ drive on the test desktop. He was then able to see the last logoff times for each NT profile by checking the dates for each profile's NTUSER.DAT using a simple DIR command.

---

[6] http://www.winternals.com/products/repairandrecovery/ntfsdospro.asp

Output sample of the DIR command used:

```
E:\WINNT\Profiles>dir /s ntuser.dat
 Volume in drive E has no label.
 Volume Serial Number is xxxx-xxxx

 Directory of E:\WINNT\Profiles\Administrator

08/13/02  09:59a             1,048,576 NTUSER.DAT
               1 File(s)      1,048,576 bytes

 Directory of E:\WINNT\Profiles\Default User

12/27/01  01:05a               237,568 NTUSER.DAT
               1 File(s)        237,568 bytes

 Directory of E:\WINNT\Profiles\urscrewed

09/08/02  02:12p               237,568 NTUSER.DAT
               1 File(s)        237,568 bytes

     Total Files Listed:
               3 File(s)      1,523,712 bytes
                         2,599,956,480 bytes free
```

The first two NTUSER.DAT files had file date/time stamps that were well over a week old. The last NT profile had an NTUSER.DAT file that had been modified that day, about 65 minutes earlier. Unfortunately "urscrewed" (see above screen output) was a local account and not a domain account so they could not trace it to a real user. It was obviously a message that the attacker expected to be found. The team lead navigated through the file system, using DOS, searching for anything that would help determine whether the exploit had been used from this computer. Apparently a remote control software called VNC [7] had been used, because he found WINVNC.EXE in the root of the E:\ drive. Once the second Ghost forensics copy was done, the original hard drive was put into a plastic bag and locked in the IT Security evidence closet. The second copy was placed into a box and stored in another evidence closet.

The next step was to find the exploit or any other information that would help lead them to the attacker through this workstation, which appeared to be the smoking gun. Unfortunately, the Incident Response team did not have a copy of the forensic software, EnCase [8] yet as the Purchasing department messed up the order and nothing was done about it. EnCase would have enabled them look at the file system beyond the operating system level. They could then find recently deleted files, data that was thought to be overwritten, and it would help them collect the information correctly, in a legal forensic format. It is generally accepted by the court system as reliable evidence. There was no time to

---

[7] http://www.realvnc.com
[8] http://www.encase.com

complain so they used a freeware utility, called Restoration [9], to retrieve all
recently deleted files. One of the files recovered was the exploit executable
SMBdie.exe, and the other was a text file full of server names. This was proof
that they'd found the workstation, and the exploit, that had been used to attack
their servers.

Screenshot of Restoration:
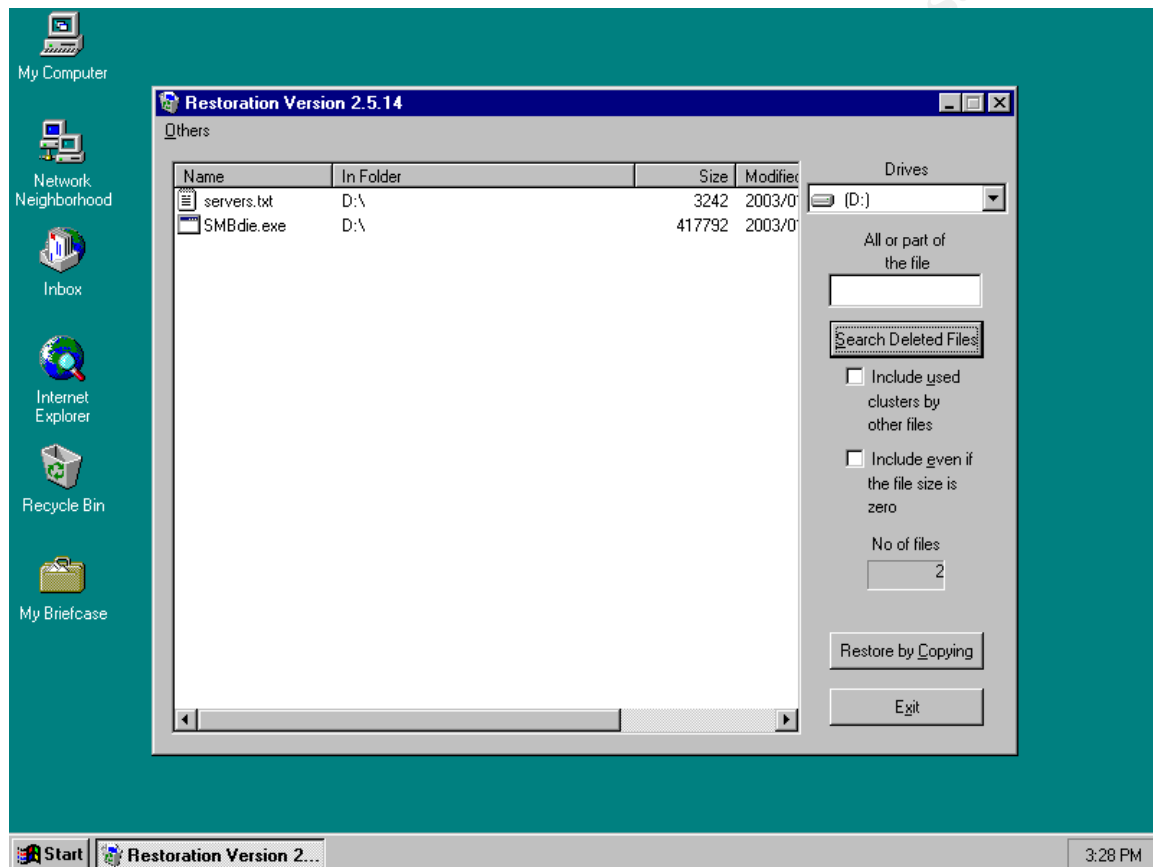
        As luck would have it, not more than an hour after they had verified that
the SMBdie exploit had been used, an alert was triggered on the test desktop left
downstairs on port 5900. It was the attacker trying to establish a VNC
connection to his would-be slave workstation, and instead fell right into the trap.
The sniffer captured the IP address, 192.168.16.148, that was trying to establish
a VNC connection over TCP port 5900. That IP address was assigned to the
VPN network segment. A Security team member called the member on the
Networking team who was in charge of the Nortel Contivity VPN servers. He
gave her the IP address caught in the sniffer, as well as the date and time that

---

[9] http://hccweb1.bai.ne.jp/~hcj58401

the VNC connection was attempted. She parsed the logs, looking for that IP address, and found the user name and source IP address:

```
09/08/2002 16:08:51 0 Security [01] Session: IPSEC[cmcrtj02]:19907 RESTRICTED FILTER 1 deny TCP any EQ 256 any GT 1023
09/08/2002 16:08:51 0 Security [01] Session: IPSEC[cmcrtj02]:19907 RESTRICTED FILTER 1 deny TCP any EQ 257 any GT 1023
09/08/2002 16:08:51 0 Security [01] Session: IPSEC[cmcrtj02]:19907 RESTRICTED FILTER 1 permit IP any any
09/08/2002 16:08:51 0 Security [01] Session: IPSEC[cmcrtj02]:19907 OUT FILTER 1 permit IP 192.168.16.10 0.0.0.0 any
09/08/2002 16:08:51 0 Security [11] Session: IPSEC[cmcrtj02]:19907 authorized
09/08/2002 16:08:51 0 Security [12] Session: IPSEC[cmcrtj02]:19907 physical addresses: remote xxx.xxx.xxx.xxx  local 192.168.6.172
09/08/2002 16:08:51 0 Security [12] Session: IPSEC[cmcrtj02]:19907 assigned IP address 192.168.16.148, mask 255.255.240.0
09/08/2002 16:08:51 0 ISAKMP [02] ISAKMP SA established with xxx.xxx.xxx.xxx
```

Security did a user name lookup on the Windows domain and found that the user name, cmcrtj02, belonged to a real employee in the company's management building next door. They located his phone number and gave him a call. He was a manager on the business side that was known to spend all day in meetings. It did not make sense that he would be sitting at his desk, crashing IT's NT servers. Their conversation with him was short and went well. It was necessary to check out his laptop to make sure it was not being hijacked in any way. There could have been a clue as to why his NT user name was being used.

One of the junior Incident Handlers walked over to the next building to look at this manager's laptop. About forty-five minutes later, she returned and said there was nothing unusual on his laptop including non-authorized administrator accounts or remote control software. The NT Security Audit logs also showed no unusual activity. The Security team figured that perhaps his password was too simple and could have been easily guessed. They knew that whenever the Help Desk technicians created new ids or reset passwords, they always assigned the same default password, "compinc1". They tried to log into one of their test machines using the manager's user name and the default password, and it worked! Their hearts just sank as they thought this could get out of hand, and considered all of the possible damage that could be done if even only a portion of users did not change their passwords after being set up or after having their password reset. The company had no password policy. For distributed systems they had very few policies and the only real policy that any of the employees could remember was to be sure to use the company's network and computers for "company business only."

Permission was given to run LC4 (aka L0phtCrack) [10], against the NT domain controller to verify how many users had an easily guessable password such as the default password given by the Help Desk. They made their own LC4 password dictionary with multiple variations of "compinc1" such as "compinc123" and "compinc01". In just five minutes all three Incident Handlers were completely shocked when LC4 completed its dictionary compare. Out of approximately 20,000 employees almost 15,000 of them had a derivative of "compinc1" for their password.

---

[10] http://stake.com/research/lc/index.html

Another problem was with the user naming convention. User names were way too simple to guess. The first three letters were statically set for every user: "cmc". Then the next three letters were the initial of the first name, last letter of the first name, and first initial of the last name. Finally the last two characters were a sequential number starting from 01. If there were a user name "cmcttr01," and an employee was hired with the same initials, the next user name would be "cmcttr02". If the hacker was familiar with the password guidelines and naming convention then they would be able to successful find valid accounts to log on to the network.

What made it even easier for a hacker to enter the network is that the authentication for a VPN session was purely based on a valid NT user name and password. There were no RSA securID key cards or other means to authenticate or lock out incoming VPN users. It was inherently insecure from the start.

The next stop was the website for the American Registry for Internet Numbers [11]. It showed that the Internet IP address from the VPN logs belonged to NetZero's dial-up pool. The Security team searched through the Nortel Contivity VPN logs again to locate more users establishing VPN connections from the Juno/NetZero network. They found several user names. Some of these users could have been real users, but they had to treat them all as possible breaches from the same attacker. The decision was made to block the entire Juno/NetZero network (64.136.0.0/18) from accessing their VPN servers. It would only impact a small number of users, if any, since all employees were already given a free dial-up account with another Internet Service Provider (ISP).

Eradication and Recovery:

An early Monday morning call to Juno/NetZero was next on the agenda. The representative was cooperative, and was able to trace down the user name that was using the IP address found by the Security team. She was also able to verify that the other IP addresses in the VPN logs had all been used by the same Juno/NetZero user name with the attacker's free account. Based on the account's terms of agreement, the representative terminated the NetZero account. However, regarding the user, all that she was able to tell Security was that the call originated in the Southern California area and that Juno/NetZero would be in contact with them if they discovered any further information regarding the user on the account.

The NT team lead had come up with a plan to distribute the patch to all of their servers. He first tried to use the company's Tivoli Software Distribution implementation method but he quickly realized its inflexibility, so he created his own way of distributing the patch. He wrote a DOS batch file that would apply the patch remotely, and then schedule a reboot of the remote server with a

---

[11] http://www.arin.net

remote shutdown/reboot utility, which he could run at a scheduled time. Below is the DOS batch file, the feeder file and reboot batch file. He also used Sysinternals' PSExec [12], PSShutdown [13], and Microsoft's NT and 2000 patches for this vulnerability, which he found links to in the Microsoft Security Bulletin.

Feeder file:

----[Servers.txt]----
W2Kservername1
NT4servername2
NT4servername3
----[Servers.txt]----

Batch file used for distribution:

----[Patch.bat]----
for /f %%i in ('type servers.txt') do call :OS %%i
goto :EOF
:OS
set server=%1
if "%server:~0,3%"=="W2K" (copy Q326830_W2K.exe \\%server%\c$\qpatch.exe&&set params=-n -z -u)
if "%server:~0,3%"=="NT4" (copy Q326830i.exe \\%server%\c$\qpatch.exe&&set params=-n -z -q)
if "%params%"=="" (echo %server% - Error&goto :EOF)
psexec \\%server% -u domain\username –p password qpatch.exe %params%
set params=
----[Patch.bat]----

Batch file used to reboot the boxes:

----[Reboot.bat]----
for /f %%i in ('type servers.txt') do psshutdown -f -r \\%%i
----[Reboot.bat]----

         With these batch files he was able to patch hundreds of servers in no time. By the afternoon most of the critical servers had been patched and rebooted for business to carry on. These were mainly application servers; the file and print servers were set aside as non-critical servers.

         By Tuesday, all the servers were patched by the lone NT lead. The IT Security Vulnerability Assessment team scanned the server farms with Nessus [14], just to make sure all of them were patched. The IDS sensors also successfully picked up the Nessus scans so there was no doubt the next attempt would be caught. None of the servers crashed from the Nessus tests and

---

[12] http://www.sysinternals.com/ntw2k/freeware/psexec.shtml
[13] http://www.sysinternals.com/ntw2k/freeware/psshutdown.shtml
[14] http://nessus.org

everything checked out just fine. Juno/NetZero had not called back and Security was still speculating on who the attacker was.

One other precaution taken was to limit the access VPN users had on the company's network. By default all of the company's VPN user accounts had access to everything in the network. The Incident Handling team consulted with their VPN expert and she verified that the VPN server could be changed to allow VPN users access to the server farms only, without affecting the business side at all. That would work as long as the attacker was not using a server to hop off of. Accessing the server farms was all that was needed by the employees anyhow, except for the network and NT administrators. The change was implemented, and all of the current connected VPN users were booted off for the change to take effect.

Description and diagram of the second attack:

Later in the afternoon on Tuesday, an IDS sensor picked up the signature for the SMBdie exploit attacking a few servers and the originating IP was an internal IP address. The IP address was from the remote Call Center, specifically the network of the onsite IT staff. Security ran a simple NbtStat command to retrieve a little more information on the computer that was attacking, and it returned the computer name, the domain and the current user name logged on to it. The fact is they were lucky that this attacker did not run a software firewall on the computer or else it would have returned nothing; the attacker had made a blunder.

NbtStat output:

```
          NetBIOS Remote Machine Name Table

   Name              Type          Status
   ---------------------------------------------
   WL-4235534    <00>  UNIQUE      Registered
   DOMAIN        <00>  GROUP       Registered
   WL-4235534    <03>  UNIQUE      Registered
   DOMAIN        <1E>  GROUP       Registered
   WL-4235534    <20>  UNIQUE      Registered
   CMCTEST06     <03>  UNIQUE      Registered

   MAC Address = xx-xx-xx-xx-xx-xx
```

The computer was a member of the company's NT domain and the user account was a domain account. The computer naming convention at this company started with "WL-", for Workstation Laptop, and the rest of the name was the serial number for each machine. The computer hacking the company had the same workstation naming convention, and the Security team verified that
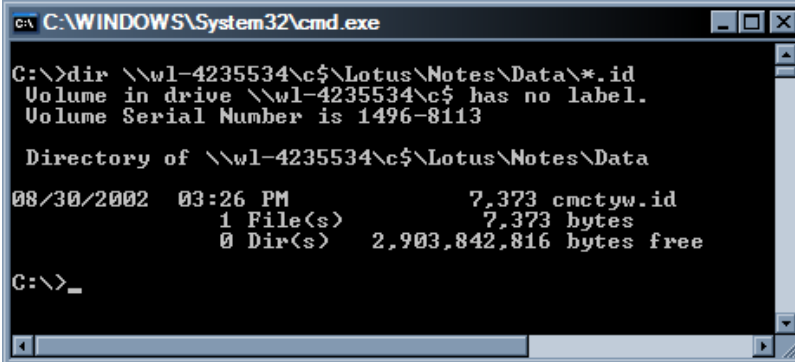
the serial number belonged to their company using the company's asset tracking software. In their asset tracking records they found that the laptop belonged to Terry, who was still at home on stress leave. He was allowed to keep his laptop while he was away from work.

After verification that the computer doing the attacking was actually company property, the decision was made to look at the file system further and remote control the laptop. First off was a quick look at the file system. They assumed that Terry might have locked down the laptop to just a few user ids so they changed the password for the account that was returned by using the NbtStat command, cmctest06. They mapped the C$ admin share using the "net use" command. They found several administrative documents written by Terry and they also found his Lotus Notes id file.

Output of the Net Use command mapping the C$ share:

```
net use * \\WL-4235534\c$ /user:cmctest06 *
Type the password for \\WL-4235534\c$:
Drive W: is now connected to \\WL-4235534\c$.
```

Screenshot of DOS screen showing Terry's Lotus Notes id file:


```
C:\>dir \\wl-4235534\c$\Lotus\Notes\Data\*.id
 Volume in drive \\wl-4235534\c$ has no label.
 Volume Serial Number is 1496-8113

 Directory of \\wl-4235534\c$\Lotus\Notes\Data

08/30/2002  03:26 PM              7,373 cmctyw.id
               1 File(s)          7,373 bytes
               0 Dir(s)   2,903,842,816 bytes free

C:\>_
```
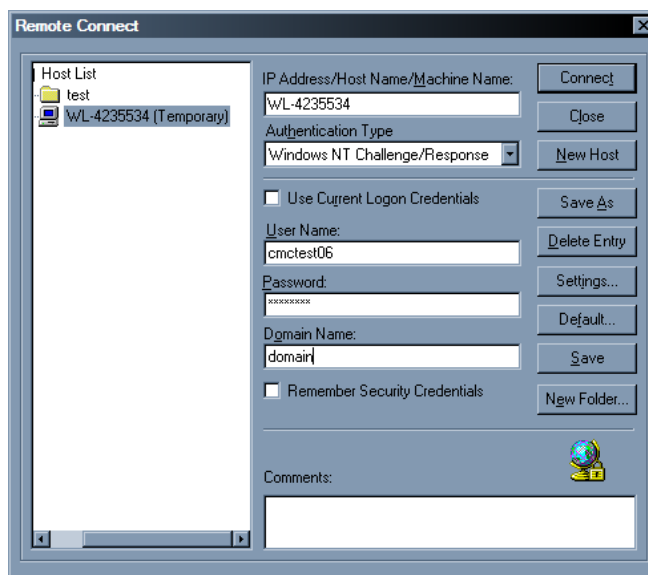
The second verification plan was to view what was happening on the laptop. DameWare [15] would be used to establish a "View Only" remote control session to the laptop. IT Security's DameWare was already configured not to notify the end user that somebody had connected their computer.
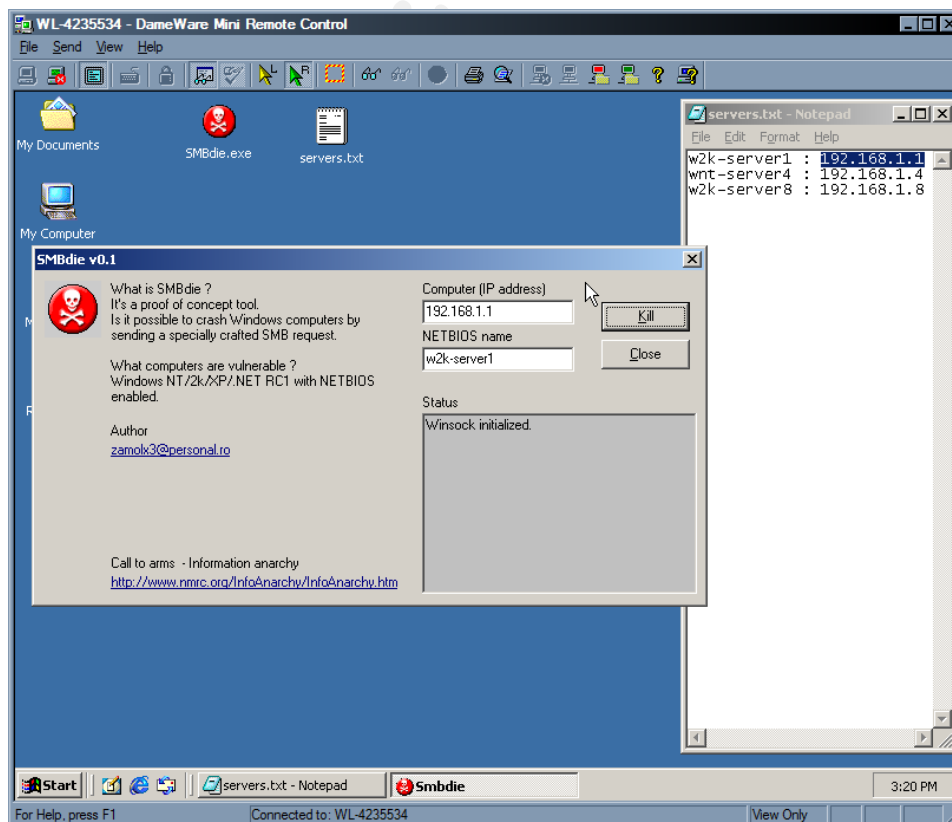
---

[15] http://www.dameware.com

Screenshot of DameWare:

The following screenshot shows Terry attacking servers using the SMBdie exploit. Notepad was open with a list of servers along with IP addresses. The server names and IP addresses were needed to use the SMBdie exploit.

Screenshot of Terry's laptop viewed through Dameware:

The junior Security handler made calls to the Networking group and the onsite NT team lead in the Call Center to track down Terry and his laptop. The Networking group was able to find out what physical network port the attacking computer was plugged into, but they also found something interesting. There were two MAC addresses assigned to the same physical port. This would indicate that there was a device such as a hub or bridge connected to this port, and that multiple computers were connecting through it.

The junior handler asked the Call Center's onsite NT team lead to look at the Cisco switch to look at the physical port and trace the wire back to the computer. The onsite NT team lead traced the wire back and it lead right to the highest ranking IT employee in the Call Center, a Director. The Director was on vacation and her laptop was not in the room but they found that she had an unapproved 802.11b wireless access point (WAP) sitting in the corner of her office, powered on. The Security team had never been informed of this 802.11b WAP device nor would they have approved it if they had known about it. The NT administrator onsite looked outside the window at the parking lot but he could not visually see Terry or his vehicle nearby. Terry could have been there, because the NT team lead did not know that Terry had traded in his old Ford Probe for a new SUV.

The Incident Handling team was satisfied that they had enough evidence for termination and conviction; they asked the NT administrator onsite to pull the power plug on the WAP. With the evidence they had, they went to the IT Security Director and Human Resources. They agreed that there was enough evidence to terminate Terry. At the time they did not want to press charges, even though he had caused several days of instability in the NT environment. The company was worried that the hacking incident would be more bad press that they could not afford.

Terry's manager went to Terry's house to tell him that he was fired and to collect the laptop. He carried a mini-audio tape recorder because he wanted to coerce Terry into confessing to the attacks, sealing the case tight. As soon as Terry was presented with all the evidence and a brief false lecture about what the company was going to do to Terry, he quickly confessed. The entire confession was caught on audio tape. The laptop and audio tape was shipped back to the Incident Handling team at the IT building. The audio tape was copied and the original was sent over to the Legal department as evidence. The copy was kept with the Incident Handlers.

Even though a forensics investigation was not needed on Terry's laptop, one was done anyhow. Two forensics Ghost copies were done using the same steps outlined before, except that a laptop to IDE hard drive adapter had to be used. The original hard drive was put into a plastic bag and locked in the IT

Security evidence closet. Several searches on the file system were done to find any documents modified or accessed in the past few weeks. The SMBdie exploit was found along with other older Windows exploits. A copy of the NetZero software needed to establish a dial-up connection was also found. The next stop was to search for previous VPN connections log entries in the NT Event Log Viewer. Those times were compared with known server crashes. Every connection log entry matched with a time period in which servers had crashed or there had been an attempt to crash them.

It was determined later that the WAP did not have Wireless Encryption Protocol (WEP) or MAC filtering enabled. The Incident Handling team was congratulated for finding the attacker. There were many changes in store for this IT department.

Lessons Learned:

The main reason this attack was so successful is because the NT and Networking teams had not realized that they needed to plan or reconfigure their systems to be more secure a long time ago. Several things were learned by this breach.

- The company's security processes and procedures needed to be established and they needed to discontinue the bad practice of loosely followed standards.

- All company assets that were assigned to an employee on stress leave or a terminated employee should be collected before the employee leaves the building. This would require keeping accurate and current accounts of the hardware given out to all employees.

- A password change policy should be established. Many users have not changed their passwords in over three years.

- A better naming convention for users should have been chosen that does not rely on three static letters, the initials of the user and a sequential number. Initials plus employee number should have been chosen instead, and contractors should have been assigned a number.

- When new users are created or passwords are reset, a randomly generated password should be used instead of using the same password for everyone.

- RSA SecurID key cards should have been used in addition to user/group authentication for VPN access.

- Network access over VPN should have been restricted to just the server farms.

- NT administrators need to test and apply security patches to servers and workstations as soon as they are released.

- The Security Incident Response team needs to refine and update their skills by attending classes and conferences.

- A Wireless (802.11x) policy should be written and enforced banning Access Points and Wireless Cards from the network.

- NT Security Auditing logs should be enabled to verify any successful or failed logon attempts.

LIST OF REFERENCES

Computec. "Computec - Software - Denial of Service - smbnuke-smbdie.c." URL: http://www.computec.ch/software/denial_of_service/smbnuke (Feb 18, 2003).

Microsoft. "Microsoft Security Bulletin MS02-045." Unchecked Buffer in Network Share Provider Can Lead to Denial of Service (Q326830). V1.0. August 22, 2002. URL: http://www.microsoft.com/technet/security/bulletin/MS02-045.asp (Feb 18, 2003).

CORE Security Technologies. "Vulnerability report for Windows SMB DoS." August 22, 2002. URL: http://www1.corest.com/common/showdoc.php?idx=262&idxseccion=10 (Feb 18, 2003).

Internet Security Systems. "Internet Security Systems Security Alert." August 29, 2002. URL: http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21061 (Feb 18, 2003).

SANS Institute, 4.1 Incident Handling Step-by-Step and Computer Crime Investigation, 2001, 2002. Page 2 – 5.

Richard Sharpe. "Just what is SMB?" V1.2. October 8, 2002. URL: http://samba.anu.edu.au/cifs/docs/what-is-smb.html (Feb 18, 2003).

EXECUTIVE SUMMARY

Summary:

Early morning on Thursday, September 5th, 2002, several production servers started crashing. Initially the cause was thought to be a software upgrade, but the IT Security Incident Handling team gathered evidence that pointed to a disgruntled employee who was at home on stress leave. The system administrators patched all production servers and the employee was terminated once the evidence was handed over to Human Resources. Incident closed.

Details:

Approximately 5:54am on Thursday, September 5th, 2002, three servers crashed within a few minutes of each other. Several hours later the same servers and four additional servers crashed. There was no explanation for these servers crashing other than a failed software upgrade the weekend before.

On Friday, the IT Security Incident Handling team was asked to investigate these crashes. Network sensors were placed throughout the server farms in hopes of seeing any possible attacks.

IBM, the vendor of the upgraded software, was contacted and their suggestion was to downgrade the software on all servers that were upgraded, on the following Saturday night. On Sunday it proved that this did not work as servers continued to crash.

The Incident Handling team discovered a possible method of attack by researching on the Internet. They found an attacking tool called SMBdie. After further testing with this tool, they determined that it produced the same results in a secure lab. Interviews were done with the System Administrators and it was found that all of the servers throughout the company were vulnerable to such an attack.

Before all the servers were patched more attacks were attempted but they were successfully were traced back to a remote controlled workstation on the first floor of the IT building. A forensics investigation showed that the attacking tool, SMBdie, was found on the workstation's hard drive.

A trap was set for the attacker if he/she returned to this confiscated workstation. Two hours after finding the remote controlled workstation the trap sprung. The trap determined that the attacker was using a Juno/NetZero dial-up account to VPN into the network. Juno/NetZero's entire network was then

blocked from accessing the VPN segment. A phone conversation was initiated with Juno/NetZero and it showed promise but nothing ever came out of the conversation. They never called back with a trace on their network to the user's house.

The account used for the VPN connection belonged to a manager in the headquarters building. It was determined that his id was being used by the attacker because the manager's password was an easily guessed password. The manager's NT user name was easy to guess as he has a common name, Robert Jones, and the attacker knew the standard naming convention for NT user names.

Microsoft released a patch that stops the attacking tool from crashing Windows NT and 2000 servers. By Tuesday morning all servers were patched.

The network sensors triggered on a SMBdie attack later that Tuesday afternoon. It was the attacker again trying to crash more servers. He was unsuccessful as all servers were patched. The attack was successfully traced back to the Call Center.

The Incident Handlers were able to get onto the attacker's computer after it was determined to be a company asset. Evidence was collected and showed that this laptop belonged to an employee who was on a month long stress leave. The System Administrators at the Call Center found a wireless access point that allowed the attacker to enter the network.

Once the evidence was turned over to Humans Resources the employee was terminated. The manager of the attacker taped the conversation he had with the attacker when he went to pick up his laptop. The manger showed the attacker the evidence and he confessed that he did it and why. After the conversation the audio tape was stored away with all the evidence in the Legal department just incase the attacker should decide to sue on wrongful termination.