Nickle@NSC

INTRODUCE TO HACKING TECHNOLOGY

CNA

Campus
Network
Association

國立中正大學 校園網路策進會

Who is Nickle

- Nickle@CNA
- CCU CSIE
- A member of NSC group in CCU center

Agenda

- Introduction
  - What is the network security
- How to attack
  - The step of hacking
  - Common hacking technique
- How to defense
  - The policy and concept
  - Exploring the software
- Live demo

Introduction

- Network security
  - Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access
- Hacker (hacking)
  - White hacker
  - Gray hacker
  - Black hacker (cracker)
  - Script kiddies

How to attack

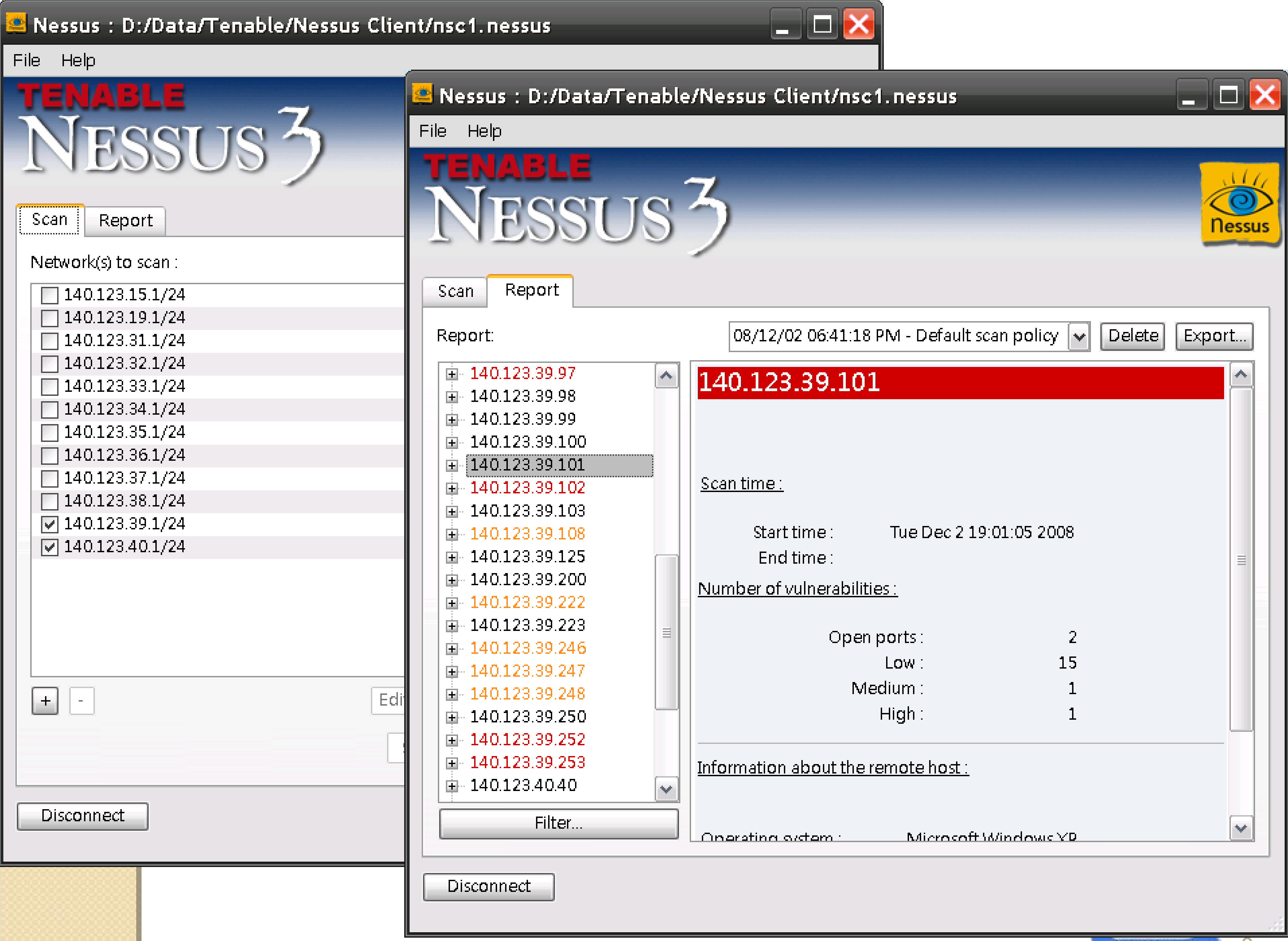
- The step of hacking
  - Information, tools and expliot gathering
  - Scanning
  - Analyzing
  - Hacking
  - Privilege elevation
  - Keep the account alive

Information, tools and exploit gathering

- Some website and forum
  - Packet storm
    - http://packetstormsecurity.org/
  - Milw0rm
    - http://milw0rm.com/
  - SecuriTeam
    - http://www.securiteam.com/
  - TheRegister
    - http://www.theregister.co.uk/
  - The Microsoft Security Response Center
    - http://blogs.technet.com/msrc/default.aspx

Scanning & Analyzing

- Vulnerability scanner
  - Nessus
    - http://www.nessus.org/
    - The common vulnerability scanner
  - SATAN
    - http://www.porcupine.org/satan/
  - Specific vulnerability scanner
    - Apache vulnerability scanner
    - SQL injection scanner
- Port scanner
  - nmap / superscanner



Network(s) to scan :

☐ 140.123.15.1/24
☐ 140.123.19.1/24
☐ 140.123.31.1/24
☐ 140.123.32.1/24
☐ 140.123.33.1/24
☐ 140.123.34.1/24
☐ 140.123.35.1/24
☐ 140.123.36.1/24
☐ 140.123.37.1/24
☐ 140.123.38.1/24
☑ 140.123.39.1/24
☑ 140.123.40.1/24

Report: 08/12/02 06:41:18 PM - Default scan policy

- 140.123.39.97
- 140.123.39.98
- 140.123.39.99
- 140.123.39.100
- 140.123.39.101
- 140.123.39.102
- 140.123.39.103
- 140.123.39.108
- 140.123.39.125
- 140.123.39.200
- 140.123.39.222
- 140.123.39.223
- 140.123.39.246
- 140.123.39.247
- 140.123.39.248
- 140.123.39.250
- 140.123.39.252
- 140.123.39.253
- 140.123.40.40

140.123.39.101

Scan time :

Start time : Tue Dec 2 19:01:05 2008
End time :

Number of vulnerabilities :

Open ports :	2
Low :	15
Medium :	1
High :	1

Information about the remote host :

Operating system : Microsoft Windows XP

Hacking

- We discuss this issue in the following chapter

Privilege elevation

- Keylogger
  - Log everything that you key in
- Dump the password
  - Mail client, Web password, Instant Message software, Windows account, … etc.
- Message analyzing
  - Instant Message logs, Sensitive database, … etc.

Keep the account

- Backdoor - Trojan horse
  - Install the backdoor in the target computer
- Rootkit
  - It replace the system instruction or kernel function with rootkit instruction which the function is still the same, but it will do something you don’t deserve.
- Even you should fixe the vulnerability of the target and protect your target from outside attack!!
  - Perfect Anti-virus+Firewall ?!

Common hacking technique

- Exploitation
- Cross-site scripting (XSS)
- SQL injection
- Sniffer
- Spoofing
- DoS / DDoS
- DNS Cache Poisoning
- Session hijacking
- Virus / Worm
- Man-in-the-middle attack / evil proxy
- Clickjacking
- iframe
- Phishing
- Rogue AP
- Social engineering

Exploitation

- Break into the system by employing the vulnerabilities
- The software or OS bugs
  - Buffer overflow
- The design principle defect
  - Authentication bypass

Cross-site scripting (XSS)

- The web designer does not check the input which the client send via input field on the web site
- So we can inject some code like javascrpt into the web page

```
<script>alert("Hi you have been hacked")</script>
```

- Demo

SQL injection

- The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed
- For example, if we check the username by:

```
statement = "SELECT * FROM users WHERE name = '" + userName + "';"
```

- And the input is:

```
a' or 't'='t
```

- The result is:

```
SELECT * FROM users WHERE name = 'a' OR 't'='t';
```

Sniffer

- If you are in the same broadcast domain of your target, you may hear all the network traffic of your target
- MSN sniffer, Password sniffer, Web sniffer, BBS sniffer

Common hacking technique

- Spoofing
- DoS / DDoS
- DNS Cache Poisoning
- Session hijacking
- Virus / Worm
- Man-in-the-middle attack / evil proxy
- Clickjacking
- iframe
- Phishing
- Rogue AP
- Social engineering

Common hacking technique

- Ready to start ?
- Wargame
  - http://wargame.cna.ccu.edu.tw/
  - http://www.hackthissite.org/
  - http://isatcis.com/
  - http://www.hack4u.org/
  - http://ambience.digitalshell.net/~llamatron/start.htm

How to defense

- The policy and concept
  - Convenience vs. security
  - Do not execute the unreliable software
  - Do not browse the unreliable web site (.cn)
  - Do not open the strange email
  - Do not install unnecessary service
  - Use the USB stick carefully
    - Close the auto run function
    - The magic key - SHIFT

How to defense

- Password
  - Do not use trivial password (abc, 123)
    - Combine the number, alpha and and symbol
    - Upper-case and lower-case
    - At least 6-8 digit
    - Do not use personal information as the password
  - Do not type your password on unreliable computer or write your password down
  - Change the password periodically
  - Do not send your password in plain text
    - BBS, FTP
- Password checker
  - http://0rz.tw/3b1HO

About password

- Complex but easy to remember
- 中文英打
- Example:
  - The password is:

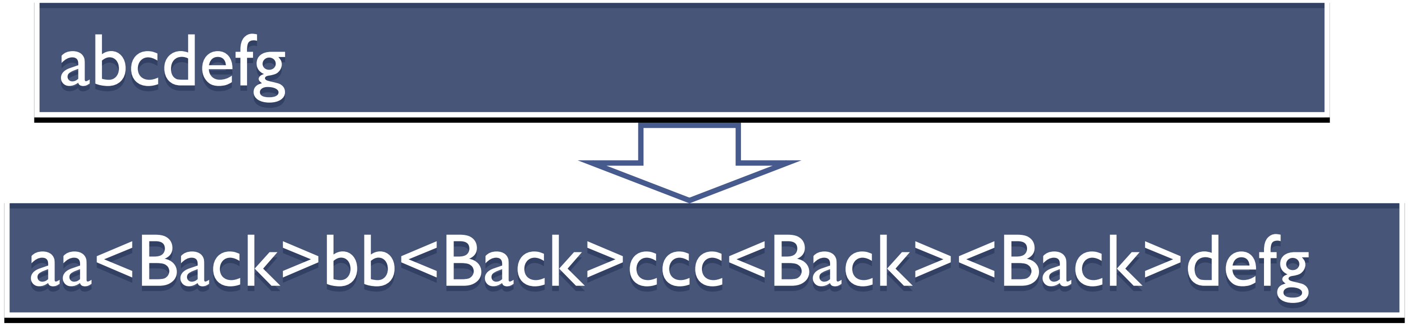
    國立中正大學
  - 注音輸入法是

    ㄍ ㄨ ㄛ ˊ ㄌ ㄧ ˋ ㄓ ㄨ ㄥ ㄓ ㄥ ˋ ㄉ ㄚ ˋ ㄒ ㄩ ㄝ ˊ
  - 切換成英文輸入是

    eji6xu45j/ 5/4284vm,6
  - 21-digit complex password~

About password

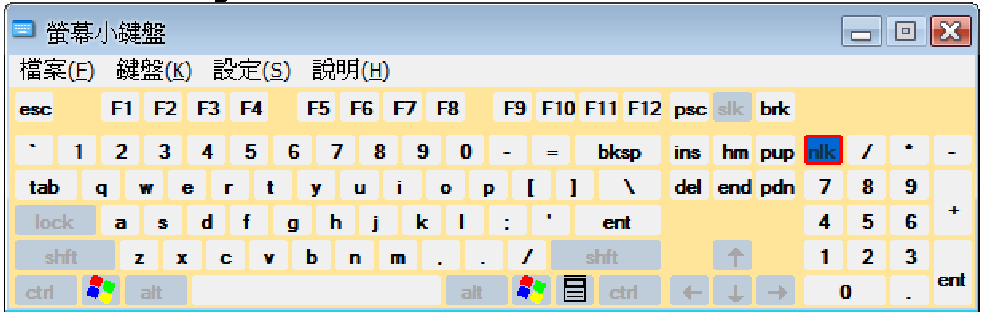
- Defense keylogger
  - Repeat-backspace



abcdefg

aa<Back>bb<Back>ccc<Back><Back>defg

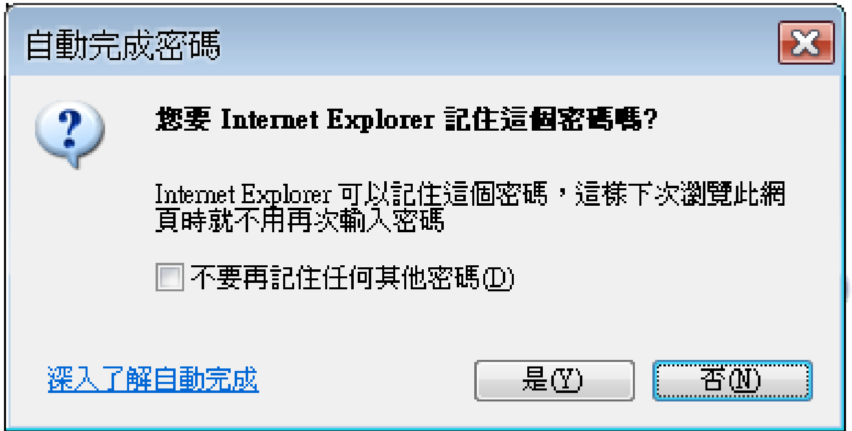
  - Copy-paste
    - Pre-saving the password into document and copy-paste while needed it
  - On screen keyboard



螢幕小鍵盤
檔案(F) 鍵盤(K) 設定(S) 說明(H)
esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 psc slk brk
` 1 2 3 4 5 6 7 8 9 0 - = bksp ins hm pup nlk / * -
tab q w e r t y u i o p [ ] \ del end pdn 7 8 9 +
lock a s d f g h j k l ; ' ent 4 5 6
shft z x c v b n m , . / shft 1 2 3
ctrl alt alt ctrl 0 . ent

About password

- Key in the password yourself, not software
  - Password record of IE、Firefox
  - Password and site record of FTP
  - Password record of mail client software
  - Password record of IM software
- Using biological password
  - Face Recognition
  - Fingerprint



自動完成密碼

您要 Internet Explorer 記住這個密碼嗎?

Internet Explorer 可以記住這個密碼，這樣下次瀏覽此網頁時就不用再次輸入密碼

□ 不要再記住任何其他密碼(D)

How to defense

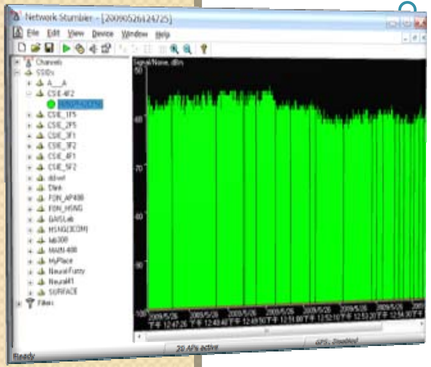
- Exploring the software
  - Install the Anti-virus software
  - Install the Firewall software
    - Windows firewall
  - Perform the full system scan periodically
  - Keeping update the anti-virus
  - Keeping update your Operation System
    - Windows Update
  - Be aware of the security advisory

How to defense

- Secure coding
  - strcpy() – buffer overflow
  - printf() – format string
  - Check the user input

Wireless

- Protocols: 802.11 a/b/g/n
- Character of wireless
  - Broadcast, easy to sniff
- Method of encryption
  - Link – WEP、WPA、TKIP…
  - Network – VPN、SSH tunnel
  - Authentication – SSID、RADIUS



Wireless

- WEP
  - Easy and fast
  - aircrack-ng
- WPA
  - Time matter
  - aircrack-ng
- Using wireshark、sniffer can peep the packets

Wireless

- Defense
  - Using longer encrypt key
    - 64bits -> 128bits
  - Hide the SSID broadcast
  - Only allow specify IP, MAC address to access the network
  - Do not use DHCP
  - Change your encryption key frequently
  - Do not use wireless to transmit private information

Reference

- http://en.wikipedia.org/wiki/Hacker_(computer_security)#External_links
- http://www.nessus.org/
- http://www.porcupine.org/satan/
- http://nmap.org/
- http://milw0rm.com/
- http://www.securiteam.com/
- http://www.theregister.co.uk/
- http://blogs.technet.com/msrc/default.aspx
- http://securityvulns.com/
- http://www.microsoft.com/taiwan/athome/security/privacy/password_checker.mspx

Thanks for your attention

- Any question?