Methodology of a Hacker

Matthew Schmid

Telemus Solutions, Inc.

Today's Topics

- Introduction
- FBI Cyber Crime Report
- Information Warfare Techniques
  - Information gathering
  - Social engineering
  - Network reconnaissance
  - Finding and exploiting vulnerabilities
  - Controlling and maintaining access
- Top 10 Security Vulnerabilities

Introduction

- Telemus Solutions, Inc.
  - Government and commercial security
  - Protecting the critical infrastructure
- Capabilities
  - Physical and IT vulnerability assessments
  - Security consulting
  - Systems engineering
  - Custom software development
  - Research and development

FBI Cyber Crime Survey (2005)

Over 5,000 respondents with over 87% experiencing one or more incidents

1. Total financial losses and the reported number of incidents have declined
2. Website attacks and wireless attacks have increased
3. Insider attacks occur about as often as external attacks
4. Defense is focused on the perimeter and antivirus / antispyware solutions
5. Security awareness continues to improve

Information Warfare Techniques

Information Gathering

- WHOIS lookup
  - Find information about ownership and registration of networks
- Newsgroup postings
  - Learn what problems the system administrator is dealing with
- Google hacking
  - Find unintentionally published information
- Dumpster diving
  - Find account names, passwords, network info
  - Improperly disposed media

Example: WHOIS HealthTechNet.org

IPv4 whois information for 204.227.246.38

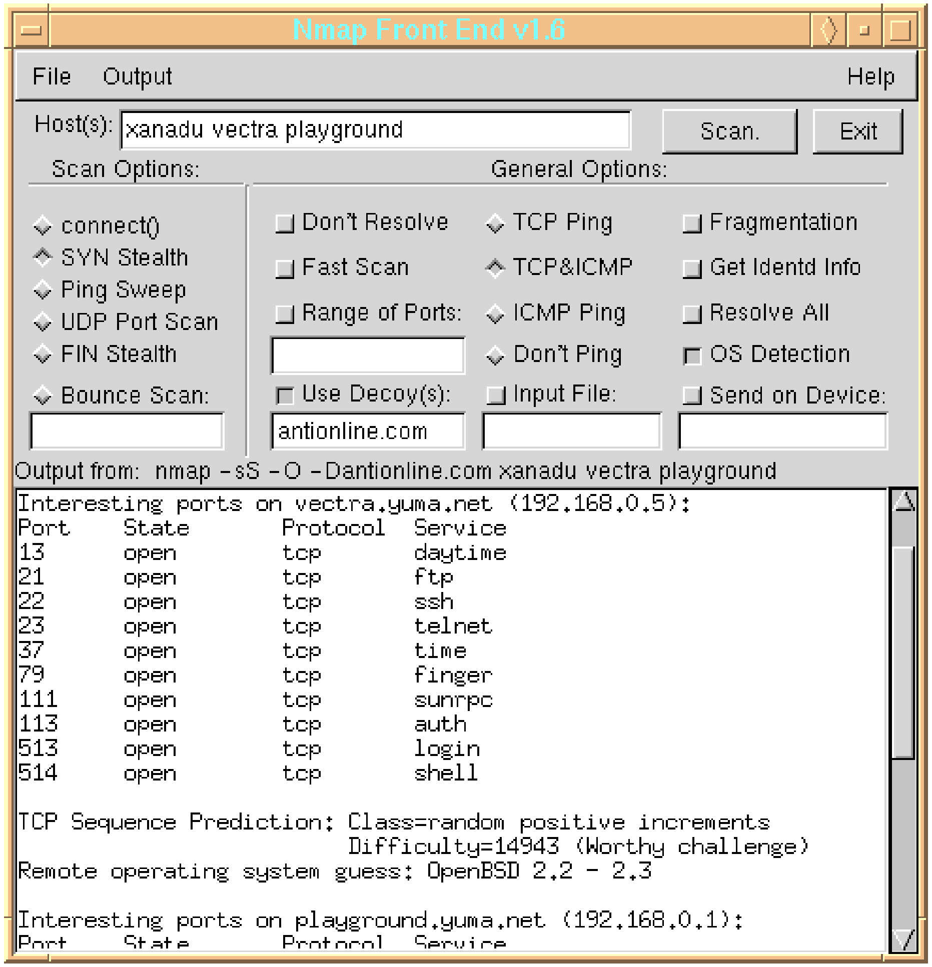
```
OrgName:               Pillsbury Madison & Sutro, Inc.
NetRange:              204.227.224.0 - 204.227.255.255
CIDR:                  204.227.224.0/19
NameServer:            SFNS01.PILLSBURYWINTHROP.COM
NameServer:            LANS01.PILLSBURYWINTHROP.COM
NameServer:            VANS01.PILLSBURYWINTHROP.COM
NameServer:            NYNS01.PILLSBURYWINTHROP.COM
smtp.shawpittman.com          208.200.185.221

OrgTechName:           Network Engineering Group
OrgTechPhone:          1-415-477-4917
OrgTechEmail:          hostmaster@pillsburywinthrop.com
```

Social Engineering

- Using gathered information to trick employees into compromising the organization’s security
  - Provide accounts/passwords
  - Modify machine settings
  - Provide physical access
- Getting users to introduce a vulnerability to the system
  - Removable media
  - Email attachments
  - Active web content

Network Reconnaissance

- Network and service mapping
  - Find out what servers are up/down
  - Identify operating systems
  - Identify open services and versions
- Tools
  - Port scanners
  - Network mappers
  - OS fingerprinters



Host(s): xanadu vectra playground

Scan Options:

○ connect()
● SYN Stealth
○ Ping Sweep
○ UDP Port Scan
○ FIN Stealth
○ Bounce Scan:

General Options:

□ Don't Resolve
□ Fast Scan
□ Range of Ports:
☒ Use Decoy(s): antionline.com
○ TCP Ping
● TCP&ICMP
○ ICMP Ping
○ Don't Ping
□ Input File:
□ Fragmentation
□ Get Identd Info
□ Resolve All
☒ OS Detection
□ Send on Device:

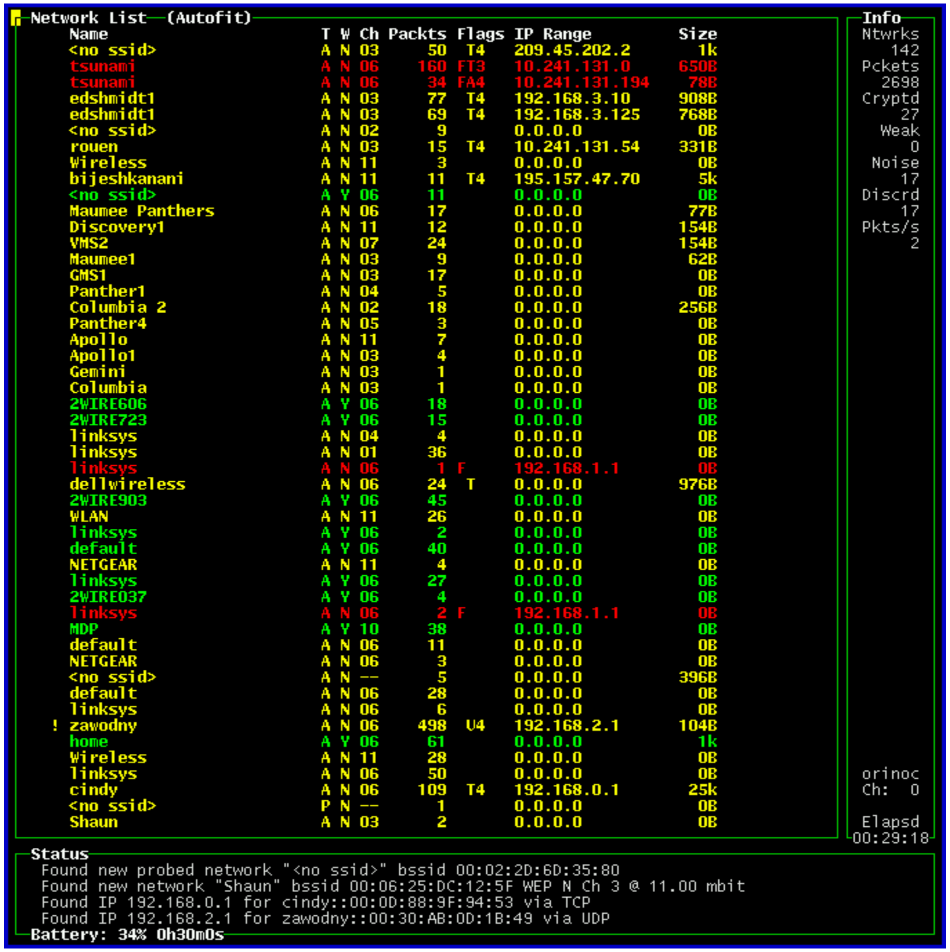
Output from: nmap -sS -O -Dantionline.com xanadu vectra playground

```
Interesting ports on vectra.yuma.net (192.168.0.5):
Port     State       Protocol  Service
13       open        tcp       daytime
21       open        tcp       ftp
22       open        tcp       ssh
23       open        tcp       telnet
37       open        tcp       time
79       open        tcp       finger
111      open        tcp       sunrpc
113      open        tcp       auth
513      open        tcp       login
514      open        tcp       shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Interesting ports on playground.yuma.net (192.168.0.1):
Port     State       Protocol  Service
```

Copyright© 2006 Telemus Solutions, Inc.
Proprietary

Wireless Networks

- Topology
  - □ Where is it connected?
- Access Points
  - □ No security
  - □ Default accounts
  - □ WEP vulnerabilities
  - □ Rogue access points
- Wireless on the laptop
  - □ Associations with other APs
  - □ Ad-hoc networks



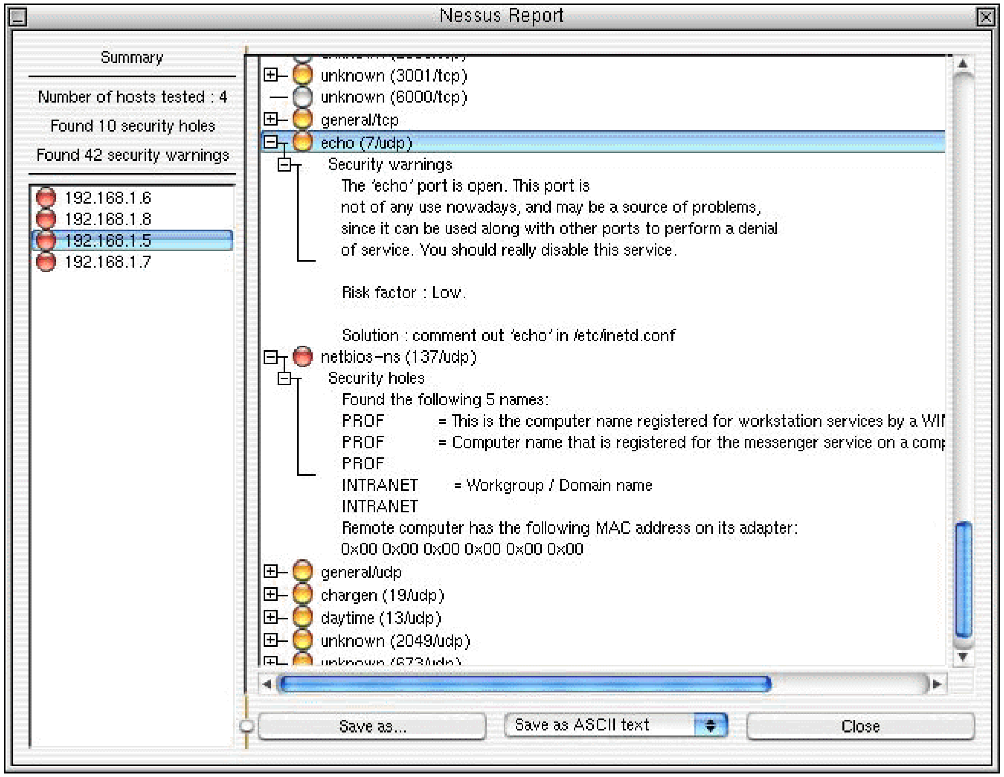
```
Network List—(Autofit)
      Name                       T W Ch Packts Flags IP Range          Size
      <no ssid>                  A N 03     50  T4   209.45.202.2        1k
      tsunami                    A N 06    160 FT3   10.241.131.0      650B
      tsunami                    A N 06     34 FA4   10.241.131.194     78B
      edshmidt1                  A N 03     77  T4   192.168.3.10      908B
      edshmidt1                  A N 03     69  T4   192.168.3.125     768B
      <no ssid>                  A N 02      9       0.0.0.0             0B
      rouen                      A N 03     15  T4   10.241.131.54     331B
      Wireless                   A N 11      3       0.0.0.0             0B
      bijeshkanani               A N 11     11  T4   195.157.47.70       5k
      <no ssid>                  A Y 06     11       0.0.0.0             0B
      Maumee Panthers            A N 06     17       0.0.0.0            77B
      Discovery1                 A N 11     12       0.0.0.0           154B
      VMS2                       A N 07     24       0.0.0.0           154B
      Maumee1                    A N 03      9       0.0.0.0            62B
      GMS1                       A N 03     17       0.0.0.0             0B
      Panther1                   A N 04      5       0.0.0.0             0B
      Columbia 2                 A N 02     18       0.0.0.0           256B
      Panther4                   A N 05      3       0.0.0.0             0B
      Apollo                     A N 11      7       0.0.0.0             0B
      Apollo1                    A N 03      4       0.0.0.0             0B
      Gemini                     A N 03      1       0.0.0.0             0B
      Columbia                   A N 03      1       0.0.0.0             0B
      2WIRE606                   A Y 06     18       0.0.0.0             0B
      2WIRE723                   A Y 06     15       0.0.0.0             0B
      linksys                    A N 04      4       0.0.0.0             0B
      linksys                    A N 01     36       0.0.0.0             0B
      linksys                    A N 06      1 F     192.168.1.1         0B
      dellwireless               A N 06     24  T    0.0.0.0           976B
      2WIRE903                   A Y 06     45       0.0.0.0             0B
      WLAN                       A N 11     26       0.0.0.0             0B
      linksys                    A Y 06      2       0.0.0.0             0B
      default                    A Y 06     40       0.0.0.0             0B
      NETGEAR                    A N 11      4       0.0.0.0             0B
      linksys                    A Y 06     27       0.0.0.0             0B
      2WIRE037                   A Y 06      4       0.0.0.0             0B
      linksys                    A N 06      2 F     192.168.1.1         0B
      MDP                        A Y 10     38       0.0.0.0             0B
      default                    A N 06     11       0.0.0.0             0B
      NETGEAR                    A N 06      3       0.0.0.0             0B
      <no ssid>                  A N --      5       0.0.0.0           396B
      default                    A N 06     28       0.0.0.0             0B
      linksys                    A N 06      6       0.0.0.0             0B
    ! zawodny                    A N 06    498  U4   192.168.2.1       104B
      home                       A Y 06     61       0.0.0.0             1k
      Wireless                   A N 11     28       0.0.0.0             0B
      linksys                    A N 06     50       0.0.0.0             0B
      cindy                      A N 06    109  T4   192.168.0.1        25k
      <no ssid>                  P N --      1       0.0.0.0             0B
      Shaun                      A N 03      2       0.0.0.0             0B
```

```
Info
Ntwrks
   142
Pckets
  2698
Cryptd
    27
  Weak
     0
 Noise
    17
Discrd
    17
Pkts/s
     2

orinoc
Ch:  0

Elapsd
00:29:18
```

```
Status
 Found new probed network "<no ssid>" bssid 00:02:2D:6D:35:80
 Found new network "Shaun" bssid 00:06:25:DC:12:5F WEP N Ch 3 @ 11.00 mbit
 Found IP 192.168.0.1 for cindy::00:0D:88:9F:94:53 via TCP
 Found IP 192.168.2.1 for zawodny::00:30:AB:0D:1B:49 via UDP
Battery: 34% 0h30m0s
```

Vulnerability Discovery

- Identify issues
  - □ Match service information to known vulnerabilities
  - □ Scan specific machines for vulnerabilities
- Tools
  - □ OS vulnerability scanners
  - □ Web vulnerability scanners



Nessus Report

Summary

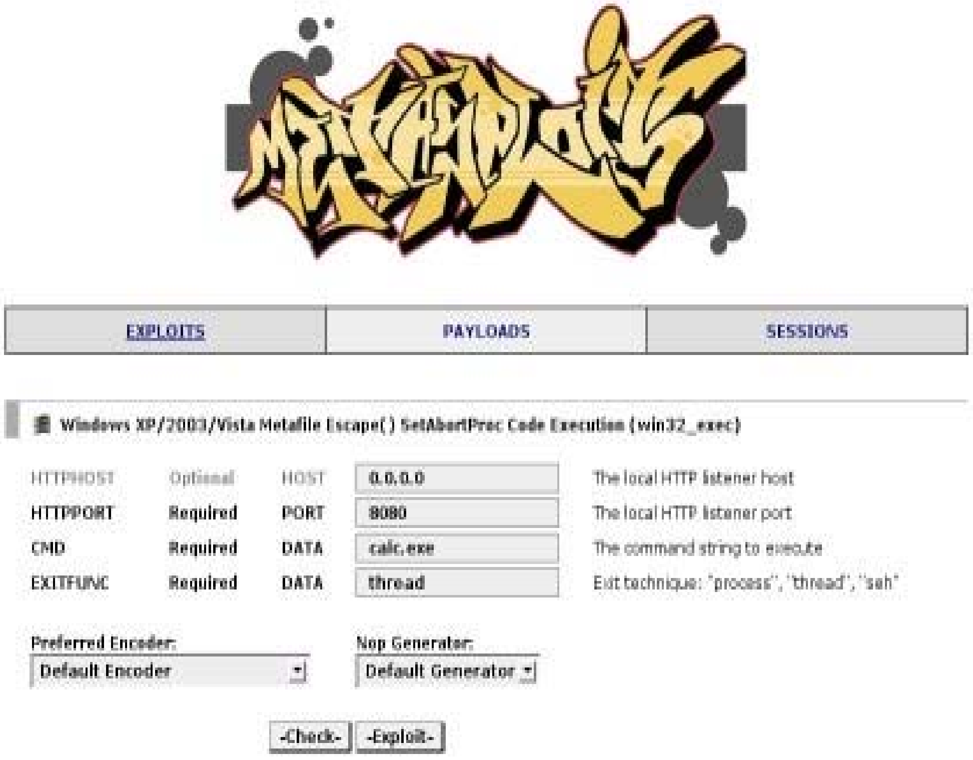
Number of hosts tested : 4
Found 10 security holes
Found 42 security warnings

```
192.168.1.6
192.168.1.8
192.168.1.5
192.168.1.7
```

```
⊞— unknown (3001/tcp)
 —  unknown (6000/tcp)
⊞— general/tcp
⊟┬ echo (7/udp)
  ⊟┬ Security warnings
      The 'echo' port is open. This port is
      not of any use nowadays, and may be a source of problems,
      since it can be used along with other ports to perform a denial
      of service. You should really disable this service.

      Risk factor : Low.

      Solution : comment out 'echo' in /etc/inetd.conf
⊟┬ netbios-ns (137/udp)
  ⊟┬ Security holes
      Found the following 5 names:
      PROF          = This is the computer name registered for workstation services by a WII
      PROF          = Computer name that is registered for the messenger service on a comp
      PROF
      INTRANET        = Workgroup / Domain name
      INTRANET
      Remote computer has the following MAC address on its adapter:
      0x00 0x00 0x00 0x00 0x00 0x00
⊞— general/udp
⊞— chargen (19/udp)
⊞— daytime (13/udp)
⊞— unknown (2049/udp)
⊞— unknown (673/udp)
```

Compromising the Target

- Exploit a vulnerability to gain access to the machine
- Tools
  - Exploit frameworks
  - Shellcode builders
  - Automated attack tools
  - Remote password crackers



Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution (win32_exec)

HTTPHOST	Optional	HOST	0.0.0.0	The local HTTP listener host
HTTPPORT	Required	PORT	8080	The local HTTP listener port
CMD	Required	DATA	calc.exe	The command string to execute
EXITFUNC	Required	DATA	thread	Exit technique: "process", "thread", "seh"

Preferred Encoder: Default Encoder

Nop Generator: Default Generator

Controlling the Host

- Privilege escalation
- Backdoors
  - Allow the attacker to easily return
- Trojan horses
  - Disguise malicious programs
- Rootkits
  - Subvert the operating system itself
- Erasing tracks

Example: Titan Rain

- Foreign attacks against a broad sector of USG and defense contractors in 2004/2005
  - Most targets were unaware of compromise
- Highly sophisticated attacks against perimeter defenses
  - Exhibited well-planned attack methodology
  - Customized tools and exploits
- Goals were data gathering and continued access
  - Organizations are still struggling to recover

Gathering Data

- Documents of all kinds from compromised machines
- Documents from file servers
- Network traffic
- Keyboard loggers
- Email messages
- Recovering deleted data

Example: Department of Veterans Affairs

- Employee had millions of records with personal information on his computer and external drive
- Computer and drive were stolen in a burglary
- Incident cost huge amount of time, money, and bad publicity
- Equipment was eventually recovered

Expanding Control

- Leverage new resources to target other machines
  - Open shares
  - Unprotected hosts
  - Routers and firewalls
  - Network sniffing
  - Intranets
  - Control systems
  - Affiliated networks

Conclusions

Top 10 Security Vulnerabilities

1. Unpatched vulnerabilities in services
2. Weak authentication and passwords
3. Out-of-date antivirus/antispyware software
4. Unnecessary administrative privileges
5. Poorly configured access controls and file sharing
6. Inadequate wireless security
7. Mis-configured routers and firewalls
8. Lack of policy and education
9. Zero-day exploits
10. Flawed recovery procedures

Summary

- Seemingly unimportant data can be leveraged by an attacker
- Perimeter security is critical, but not sufficient
- Effective security is a combination of technical solutions and good policies

Thank You

Matthew Schmid, CISSP

mschmid@telemussolutions.com

Telemus Solutions, Inc.

http://www.telemussolutions.com