Cyber Attack for Management

The Armitage Project

ISSA DC / 18 Jan 11
Today...

- Your speaker
- On Hacking...
- What is Armitage?
- Demonstration
- Q&A
Your Speaker...

- Systems Administrator
- NOSC Crew Commander
- Cyber Ops R&D Team Lead
- Red Team Member
- Penetration Tester
Hacking is like... magic
It’s easier than you think...

A CRYPTO NERD’S IMAGINATION:

His laptop’s encrypted. Let’s build a million-dollar cluster to crack it.

No good! It’s 4096-bit RSA!

Blast! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:

His laptop’s encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.

Cartoon: XKCD by Randall Munroe: http://xkcd.com/538
Hacking is a Process

- Scan / Import Hosts
  - Remote Exploit
  - Use Credentials / Pass the Hash
    - Escalate Privileges
      - Dump Hashes
      - Setup Pivoting
  - Client Side Attack
    - Explore System / Steal Data
On Hacking

• It’s like magic...
• It’s easier than you think
• It’s a process
Metasploit

• A Penetration Testing and Exploit Development Framework

http://www.metasploit.com
=| msf v3.0
+ -- --|= 5 exploits 72 payloads
-| 2 encoders 2 nops
msf exploit(test/multi/aggressive) > exploit -h
Usage: exploit [options]

Launches an exploitation attempt.

OPTIONS:
- | <opt> The payload encoder to use. If none is specified, ENCODER is used.
- | <opt> The NOP generator to use. If none is specified, NOP is used.
- | <opt> A comma separated list of options in VAR=VAL format.
- | <opt> The payload to use. If none is specified, PAYLOAD is used.
- | <opt> The target index to use. If none is specified, TARGET is used.
- | Do not interact with the session after successful exploitation.

msf exploit(test/multi/aggressive) > exploit -z
[*] Sending 124 byte payload...
[*] Sending stage (2838 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (73739 bytes)...
[*] Upload completed.
[*] Trying to use connection...
[*] Meterpreter session 1 opened (10.254.0.4:59360 -> 10.254.0.4:12345)
[*] Started logging session interaction.
[*] Session 1 created in the background.
msf exploit(test/multi/aggressive) > session -1

Active sessions
==========

<table>
<thead>
<tr>
<th>Id</th>
<th>Description</th>
<th>Tunnel</th>
</tr>
</thead>
</table>
| 1  | Meterpreter 10.254.0.4:59360 -> 10.254.0.4:12345

msf exploit(test/multi/aggressive) > session -i 1
[*] Starting interaction with 1...

meterpreter > use stdapi
Loading extension stdapi...success.
meterpreter >
What is Armitage?

- A GUI for Metasploit
  - Recommends exploits
  - Configures modules
  - Aids Post Exploitation
  - Friendly to Command-line Users
What is Armitage?

- A GUI for Metasploit
- Goal: Avoid this...
What is Armitage?

• Usable for your penetration tests?

Image courtesy of @guerilla7 on Twitter.
What is Armitage?

• Usable for your penetration tests

Image courtesy of @guerilla7 on Twitter.
Stop, Demo Time!

- Scanning
- Exploitation
- Post Exploitation
- Maneuver
Today...

- Your speaker
- On Hacking...
- What is Armitage?
- Demonstration
- Q&A
Go get it...

• Website
  – http://www.fastandeasyhacking.com

• Twitter
  – @armitagehacker

• Email
  – contact@fastandeasyhacking.com