

Sec Maniac.com

Metasploit Express omg

David Kennedy (ReL1K)

<http://www.secmaniac.com>

Twitter: Dave_ReL1K

Email: davek@social-engineer.org

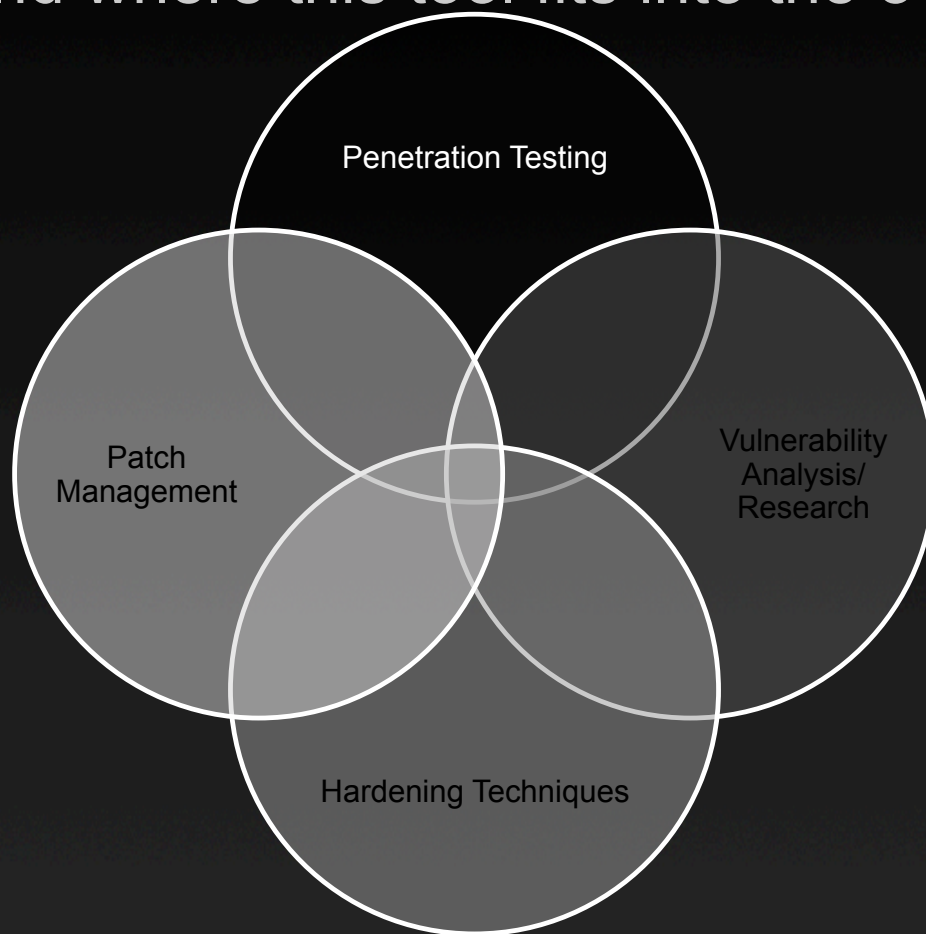


Metasploit Express

- Commercial based product created by the developers of Metasploit.
- \$3,000 per user license
- The ability to automate, and workflow penetration tests in a very efficient manner.
- Now one of my favorite assets on a penetration test...

Before we slap some tools in...

- Let's talk really quick about a vulnerability management program and where this tool fits into the overall food chain.



Penetration Testing

- Metasploit Express will not perform penetration tests for you.
- You need to be smart on this stuff and do it regularly.
- Penetration testing helps evaluate the effectiveness of your vulnerability management and incident response program.

Metasploit Express Basics

- Supported for Windows/Linux based operating systems.
- Ruby (rails) based as is the Metasploit Framework (primarily) web interface.
- 2 GHz+ processor 2 GB RAM available (increase accordingly with VM targets on the same device)
500MB+ available disk space 10/100 Mbps network interface card

What we'll be attacking...

- Metasploitable – Free vulnerable virtual machine created by the Metasploit team. Ubuntu based and has multiple attack vectors.
- Windows XP Service Pack 2 English Edition

```
#!/usr/bin/perl
import
socket
socket
socket
socket
socket
socket
buffer
```

Sec Moni@.com

So why Metasploit Express?

DEMOS

So why Metasploit Express?

- Full integration into the Metasploit Framework
- Amazing amount of automation and flexibility
- Customized report templates and reproducible results
- Additional features not offered within the Framework
- Cool factor and for 3K???? Comon...

The Double Whammy

- Metasploit Express is only going to get more integrated within NeXpose, Rapid7's vulnerability scanner.
- I can attest, we use NeXpose and are very impressed and pleased.
- NeXpose and MSF Express are tools, it will never replace a motivated hacker attempting to exploit weaknesses. Remember that.

Recommendations

- You need to know what your doing in this stuff, but practice makes perfect..
- You can get a two week copy by registering with Rapid7 and its free.
- I would recommend utilizing MSF Express and NeXpose in your vulnerability management program.

```
import socket
socket
socket
socket
socket
buffer
```

Sec Maniac.com

Questions? ☺

<http://www.secmaniac.com>

Twitter: dave_re1k

Email: davek@social-engineer.org