METASPLOIT

Somesh Rasal
Information Security Analyst
https://www.linkedin.com/in/somesh-rasal/

Basic Terminology

Vulnerability:-The weakness which allows an attacker to break into a system.

Exploit:-code which allows an attacker to take advantage of vulnerable system.

Payload:- actual code which runs on system after exploitation.

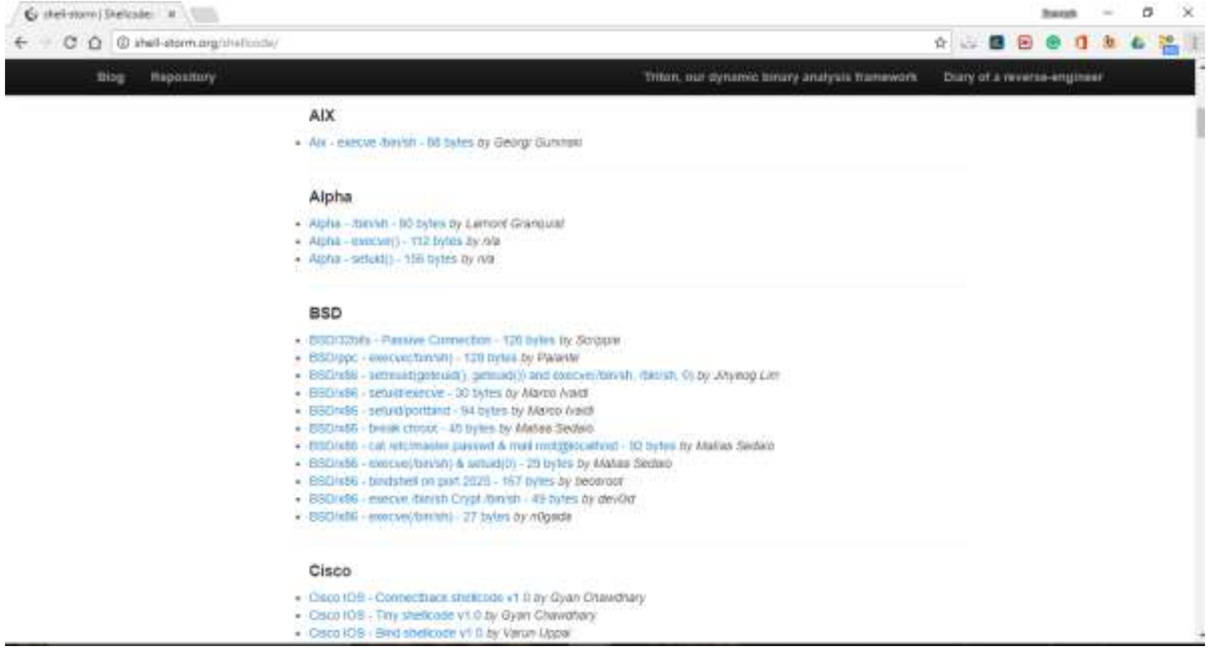
Typical Process of attack

1. Scan IP Address to get port and services running on them.

2. identify a vulnerable service find a public/private exploit.

3. launch exploit compromise post exploitation plan.

Exploit Resources


shell-storm | Shellcode
shell-storm.org/shellcode/
Blog
Repository
Triton, our dynamic binary analysis framework
Diary of a reverse-engineer

AIX

- Aix - execve /bin/sh - 88 bytes by Georgi Guninski

Alpha

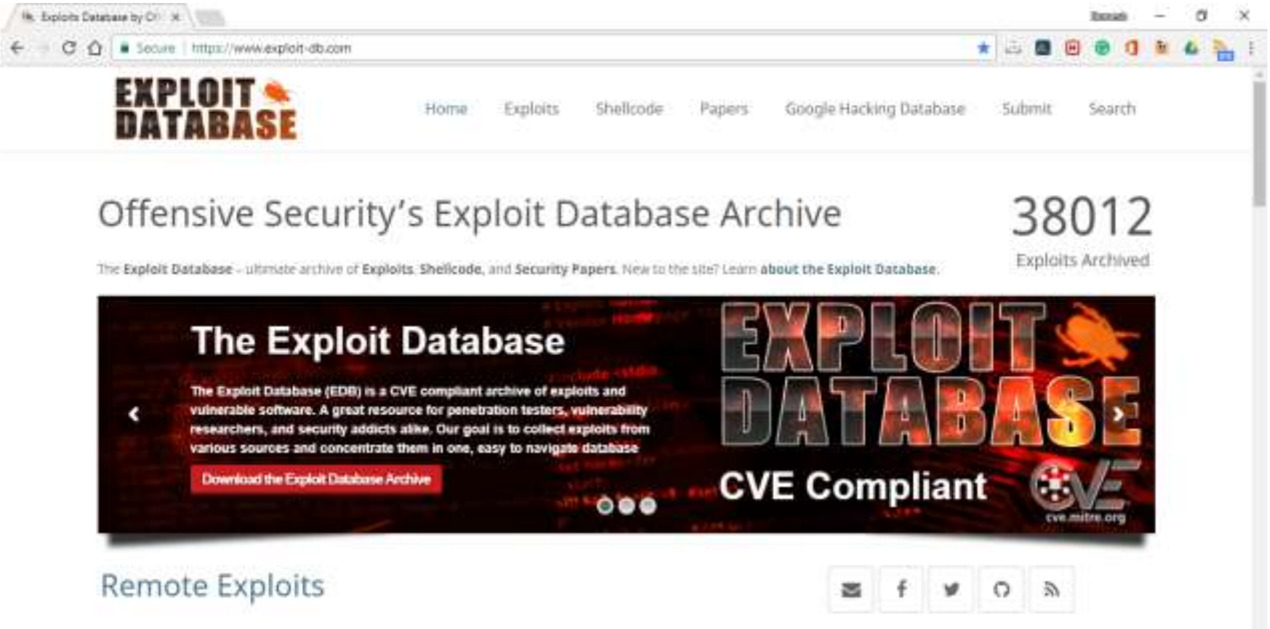
- Alpha - /bin/sh - 80 bytes by Lamont Granquist
- Alpha - execve() - 112 bytes by n/a
- Alpha - setuid() - 156 bytes by n/a

BSD

- BSD/32bits - Passive Connection - 120 bytes by Scrippie
- BSD/ppc - execve(/bin/sh) - 128 bytes by Palante
- BSD/x86 - setreuid(geteuid(), geteuid()) and execve(/bin/sh, /bin/sh, 0) by Jihyeog Lim
- BSD/x86 - setuid/execve - 30 bytes by Marco Ivaldi
- BSD/x86 - setuid/portbind - 94 bytes by Marco Ivaldi
- BSD/x86 - break chroot - 45 bytes by Matias Sedalo
- BSD/x86 - cat /etc/master.passwd & mail root@localhost - 92 bytes by Matias Sedalo
- BSD/x86 - execve(/bin/sh) & setuid(0) - 29 bytes by Matias Sedalo
- BSD/x86 - bindshell on port 2525 - 167 bytes by beosroot
- BSD/x86 - execve /bin/sh Crypt /bin/sh - 49 bytes by dev0id
- BSD/x86 - execve(/bin/sh) - 27 bytes by n0gada

Cisco

- Cisco IOS - Connectback shellcode v1.0 by Gyan Chawdhary
- Cisco IOS - Tiny shellcode v1.0 by Gyan Chawdhary
- Cisco IOS - Bind shellcode v1.0 by Varun Uppal



Offensive Security's Exploit Database Archive

38012

Exploits Archived

The **Exploit Database** - ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn **about the Exploit Database**.

The Exploit Database

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database

Download the Exploit Database Archive

Remote Exploits

www.shell-storm.org/shellcode/

www.exploit-db.com

Challenges In Individual Exploit

- ➢ Multiple exploits for single task.
- manage, update, customize is not so easy
- ➢ To customize payload or rewrite mat be required of the exploit program.
- time consuming, High skill set required
- ➢ testing and exploit research is tedious without a framework.
- end up reinventing the wheel

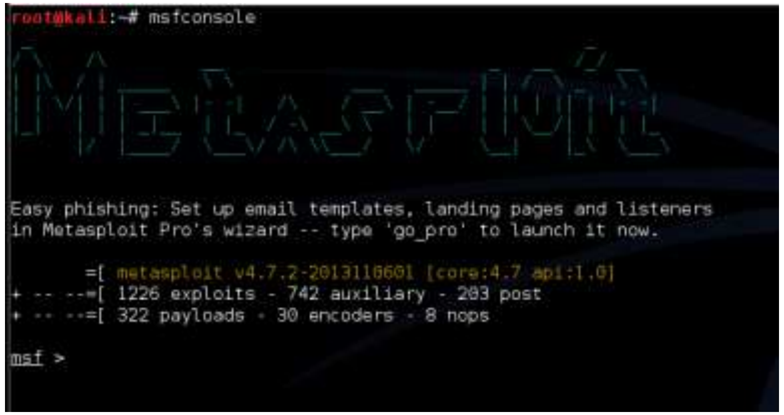
Metasploit Framework

- Started By H.D.MOORE in 2003
- Acquired by Rapid7
- Remain open source and free for use(Commercial version available)
- Written in ruby
- Can be used for :
- penetration Testing
- Exploit research
- developing IDS signature

Metasploit For Pentester

- Over tested exploits
- Over payloads
- Encoders
- Metasploit offers plug and play of payloads with exploits
- This alone is huge advantage
- Tons of other features for better and faster pentesters
- Meterpreter
- Web shells

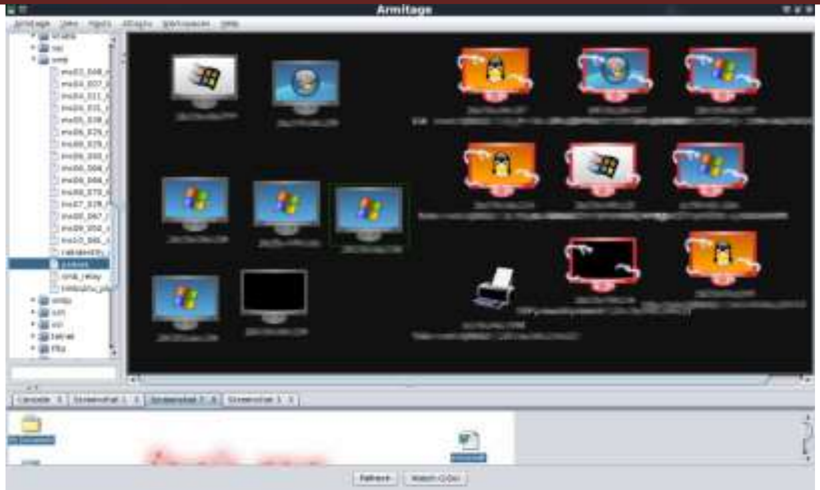
Metasploit Access Methods

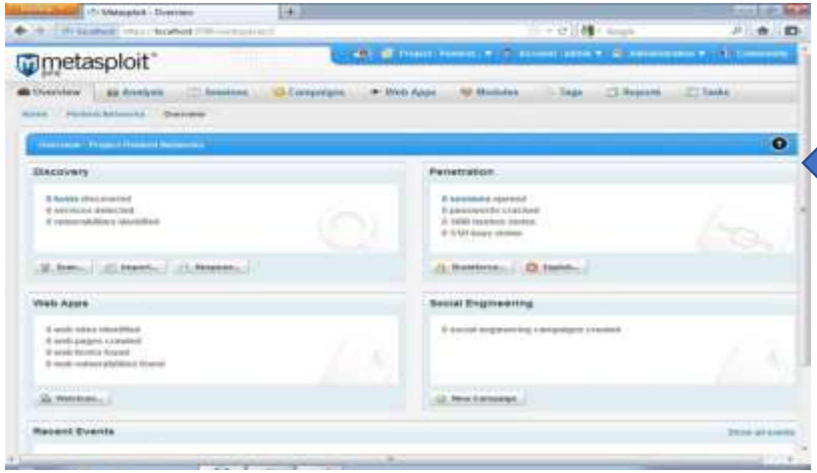


```
root@kali:~# msfconsole

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.7.2-2013110601 [core:4.7 api:1.0]
+ -- --=[ 1226 exploits - 742 auxiliary - 203 post
+ -- --=[ 322 payloads - 30 encoders - 8 nops

msf >
```

Msfconsole

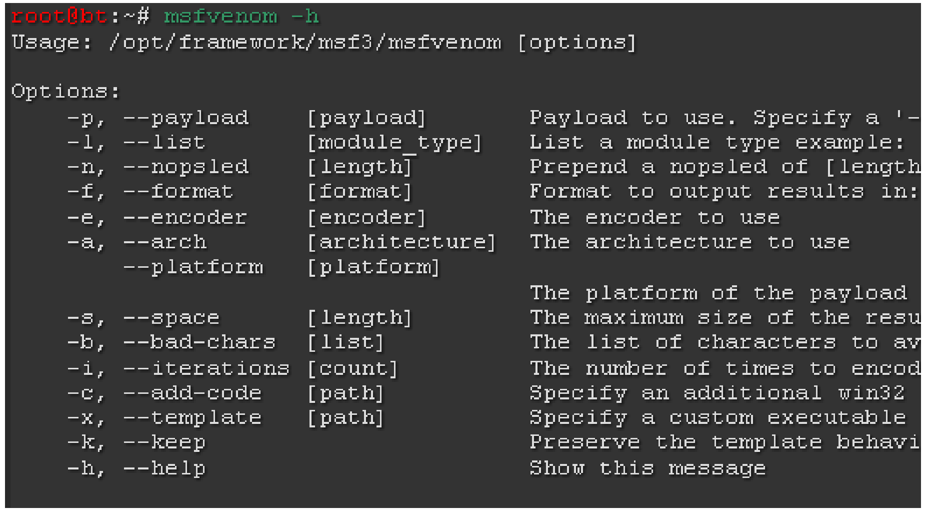
Armitage





Web Interface

msfvenom



```
root@bt:~# msfvenom -h
Usage: /opt/framework/msf3/msfvenom [options]

Options:
    -p, --payload    [payload]       Payload to use. Specify a '-
    -l, --list       [module_type]   List a module type example:
    -n, --nopsled    [length]        Prepend a nopsled of [length
    -f, --format     [format]        Format to output results in:
    -e, --encoder    [encoder]       The encoder to use
    -a, --arch       [architecture]  The architecture to use
        --platform   [platform]
                                     The platform of the payload
    -s, --space      [length]        The maximum size of the resu
    -b, --bad-chars  [list]          The list of characters to av
    -i, --iterations [count]         The number of times to encod
    -c, --add-code   [path]          Specify an additional win32
    -x, --template   [path]          Specify a custom executable
    -k, --keep                       Preserve the template behavi
    -h, --help                       Show this message
```

Basic Commands

- Check: There aren’t many exploits that support it, but there is also a **check** option that will check to see if a target is vulnerable to a particular exploit instead of actually exploiting it.
- Help: The **help** command will give you a list and small description of all available commands.
- Info: The **info** command will provide detailed information about a particular module including all options, targets, and other information.

Basic Commands

- Load: The **load** command load plugin from Metasploit's ***plugin*** directory.
- Resource: The **resource** command runs resource (batch) files that can be loaded through msfconsole.
- Search: The msfconsole includes an extensive regular-expression based **search** functionality.

For More Commands

https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

Demo-Ubuntu

Demo-Windows 7

Limitations of using specific payload

- The payloads can do specific task only
- Add user
- Bind shell on specific port
- Most exploits include a remote shell creating payload.
- Disadvantages :-
- Limited commands run by the shell
- creation of new process every time

Then what we need…

A payload which:

- avoid creation of new process.
- should not create new file on disk.
- which allows to extend functionality remotely.
- Allows to write scripts at runtime and can leverage inside.

We need Meterpreter!

Study Resources(Tutorials)

Pentesting with Metasploit

http://www.pentesteracademy.com/course?id=10

Expert Metasploit Penetration Testing

https://www.udemy.com/expert-metasploit-penetration-testing-series/

Study Resources(Books)

Metasploit – The Penetration Tester’s Guide

https://goo.gl/MqqkSW

Metasploit Penetration Testing Cookbook

https://goo.gl/dBDzqD

Mastering Metasploit

https://goo.gl/9oNfZz

References

- https://www.metasploit.com/
- https://www.offensive-security.com/metasploit-unleashed/
- https://en.wikipedia.org/wiki/Metasploit_Project
- https://github.com/rapid7/metasploit-framework

Any Queries?

Thank you!