

Working with the Metasploit Framework



Keith Watson

INFORMATION SECURITY PROFESSIONAL

@ikawnoclast ikawnoclast.com



Module Overview



Managing data

Managing sessions

Repeating actions



Globomantics Red Team Support



Report accurately



Operate efficiently



Data Management



The Metasploit Database



Initializes on
first start



Reconnects on
subsequent
starts



Collects and
organizes data

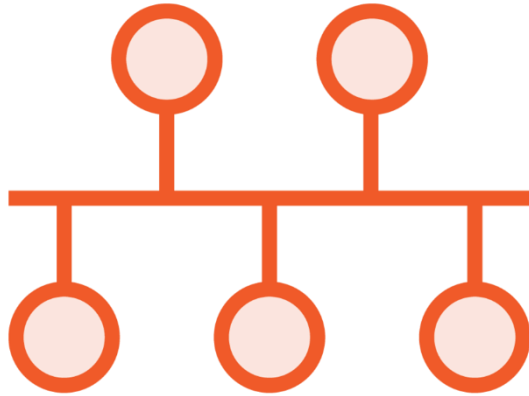


Imports and
exports data

Workspaces



Projects



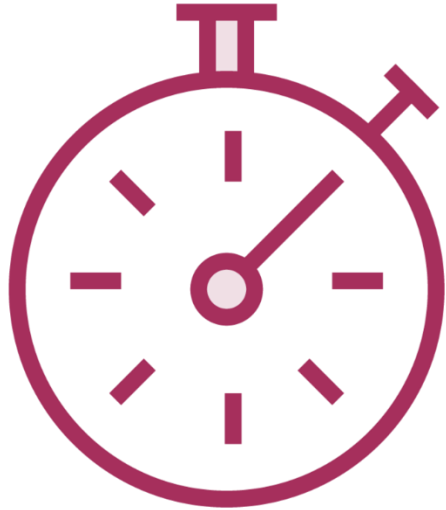
Networks or subnets



Locations



Importing Data



Nmap real-time data



Nmap XML scan data



XML and report data
from third party tools

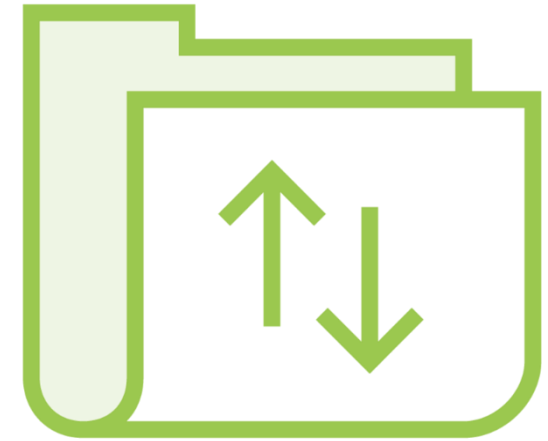
Exporting Data



Backing up

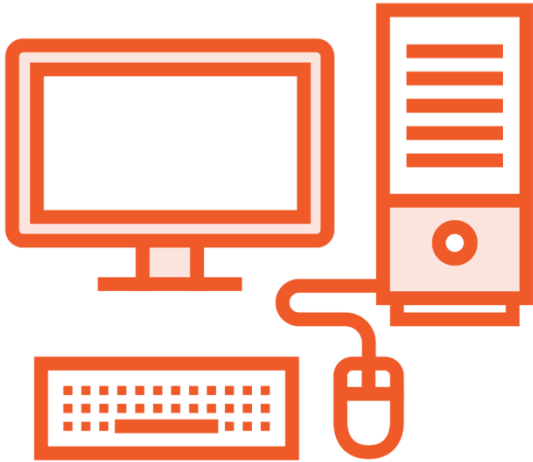


Archiving



Transferring data

Tags



Apply to hosts
or a range of hosts



Search for hosts
with a specific tag



Delete when
no longer needed

Demo



Create a workspace

Import nmap scan data

Export data to an archive

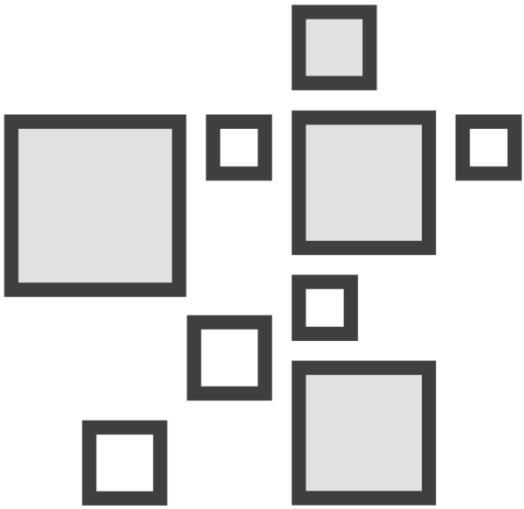
Tag hosts



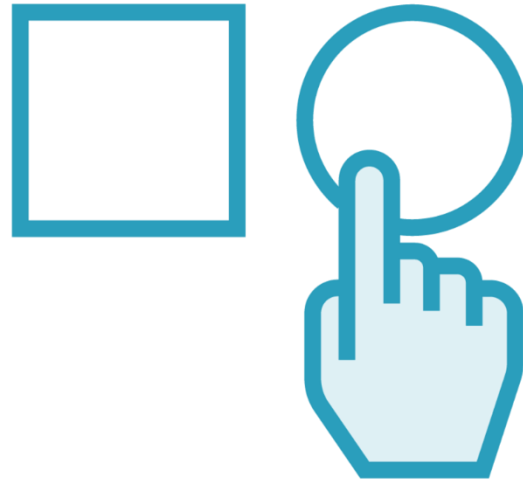
Session Management



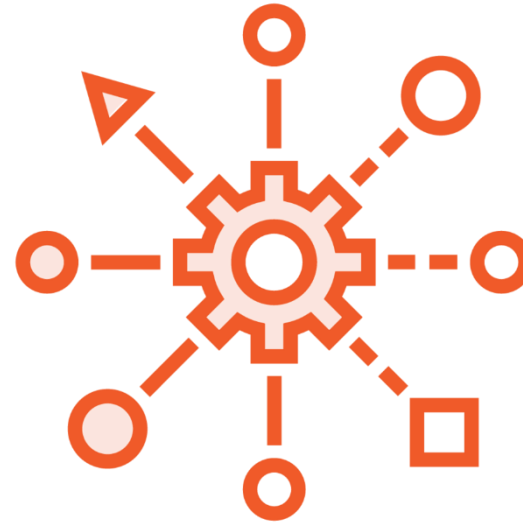
Sessions



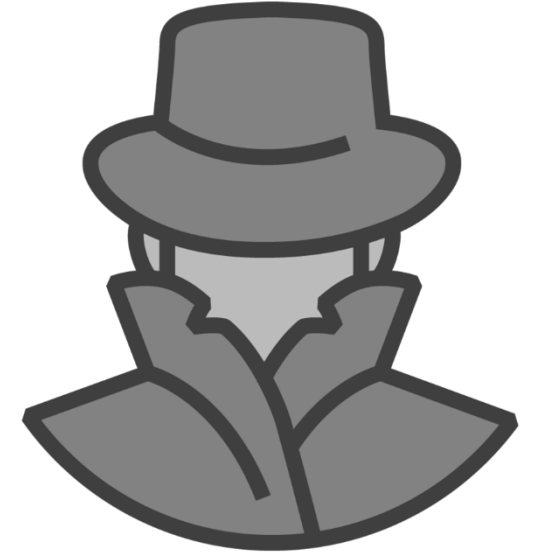
Open multiple
sessions



Switch between
sessions



Manage sessions



Facilitate post
exploitation

Managing Sessions



Escaping an open session: **^Z** (control-Z)



List running sessions



Terminate sessions



```
msf5 > sessions -l
```

```
msf5 > sessions -v
```

```
msf5 > sessions -x
```

```
msf5 > sessions -d
```

```
msf5 > sessions -n <name> <session number>
```

```
msf5 > sessions -u <session number>
```

Commands to Manage Sessions

List sessions

Apply a name to a session

Upgrade a shell based session to Meterpreter



```
msf5 > sessions -k <session number>
```

```
msf5 > sessions -K
```

Commands to Terminate Sessions

Terminate a specific session

Terminate all sessions



Demo



Examine existing sessions

Interact with an existing session

Execute a post module

Terminate sessions



Repeating Actions



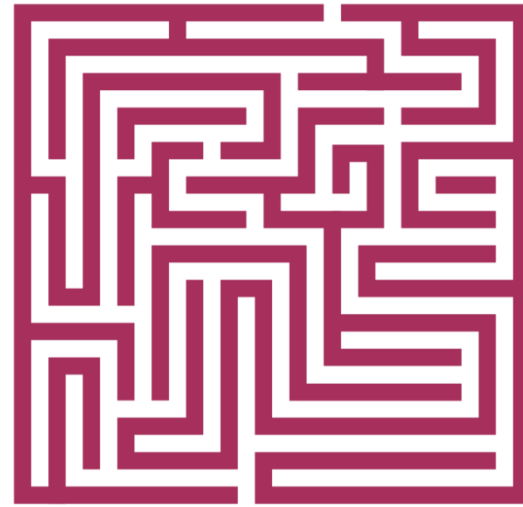
Reasons to Repeat Yourself



Same targets



Same tests

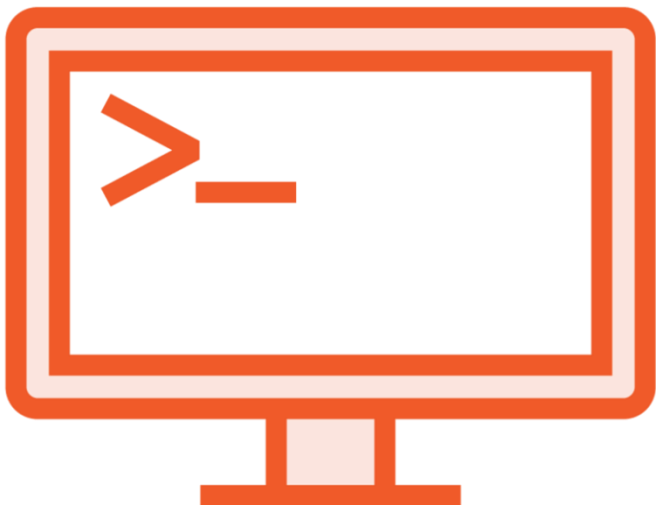


Tricky
vulnerability



Productivity

Scripting



Metasploit console



Meterpreter



Metasploit Console Scripting



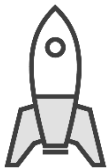
Record commands from the start: `makerc`



Execute commands from a script: `resource`



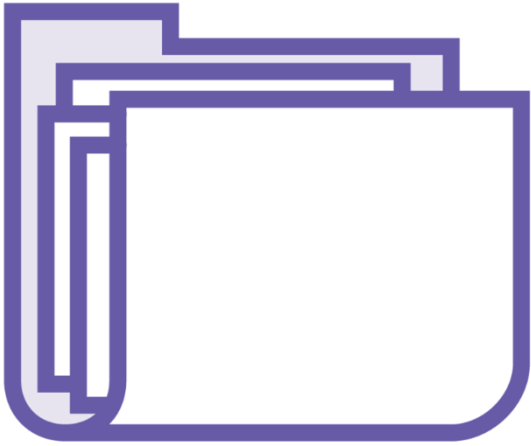
Embed Ruby code inside the script: `<ruby>code</ruby>`



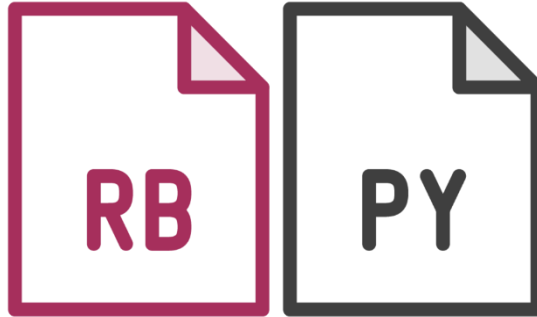
Launch Metasploit console resource scripts from the system



Meterpreter Scripting



Scripts are included



Written in Ruby
or Python



Custom scripts
can be created



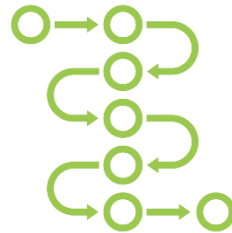
Repeat Commands

Used to repeat a command more than once

- Built for HeartBleed vulnerability testing



Indefinitely



Specific number of times



Specific amount of time



```
# msfconsole -r <resource_file>
```

```
msf5 > <multiple console commands>
```

```
msf5 > makerc <resource_file>
```

```
msf5 > resource <resource_file1> <resource_file2> ...
```

Commands for Metasploit Console Scripting

Execute a resource script from the system command line

Create a resource script from previously execute console commands

Execute resource scripts from inside the Metasploit console



```
meterpreter > run checkvm
```

```
meterpreter > run killav
```

```
meterpreter > run winenum
```

```
meterpreter > load python
```

```
meterpreter > python_import -f <file>.py
```

```
meterpreter > python_exec <code>
```

Commands for Meterpreter Scripting

Execute existing Meterpreter scripts

Load the Python extension

Import Python files or execute Python code



Summary



Module Summary



Managing data through databases

Managing sessions with targets

Repeating commands through resource scripts



Up Next:
Summary and Next Steps

