

Launching an Attack



Keith Watson

INFORMATION SECURITY PROFESSIONAL

@ikawnoclast ikawnoclast.com



Module Overview



Launching the attack

Interpreting output

Post modules

Local exploits

Meterpreter



Attack Flow



Configure the exploit and payload



Launch the attack



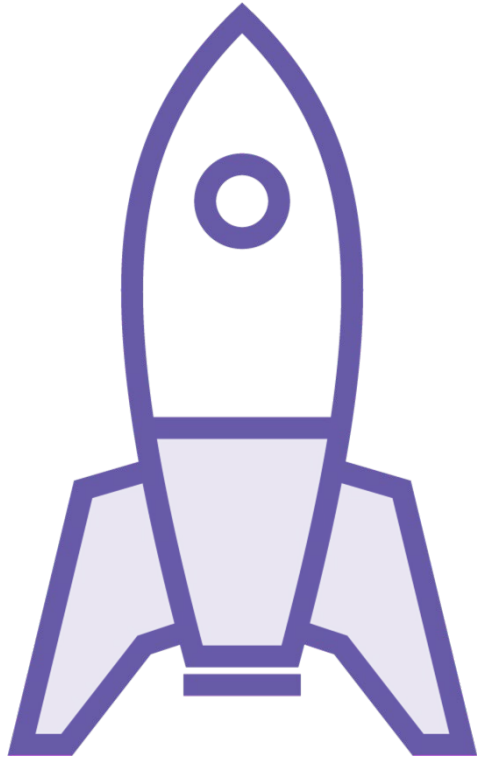
Review results / Interpret the output



Begin post exploitation activities



Launching the Attack



exploit



Globomantics Red Team Attacks/Tests

Goal-oriented approaches

- Find vulnerabilities
- Identify blind spots
- Exercise response
- Training

Notification

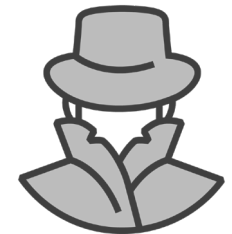
- Prior
- After
- None



Coordinated



Overt



Evasive or Covert

Interpreting the Output



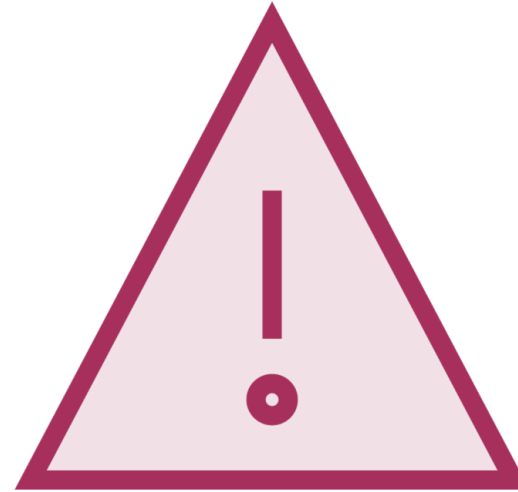
Message Output Types



Success



Status



Warning



Error

Success / Good Messages

[+]

An activity completed successfully

Expected response was received

Examples:

- [+] Payload successfully staged
- [+] Success, user is now SYSTEM
- [+] Received READY reply



Status Messages

[*]

Informational message

Progression of activities

Examples:

- [*] Backgrounding session 1
- [*] Upload completed
- [*] Searching LDAP directory



Warning Messages

[!]

Informational message

Potential errors/issues may occur

Examples:

- [!] Unable to detect platform
- [!] Skipping unrecognized report
- [!] Database not connected



Error Messages

[-]

Failure message

Cannot continue

Examples:

- [-] File Not Found
- [-] Unexpected value format
- [-] Root access rejected



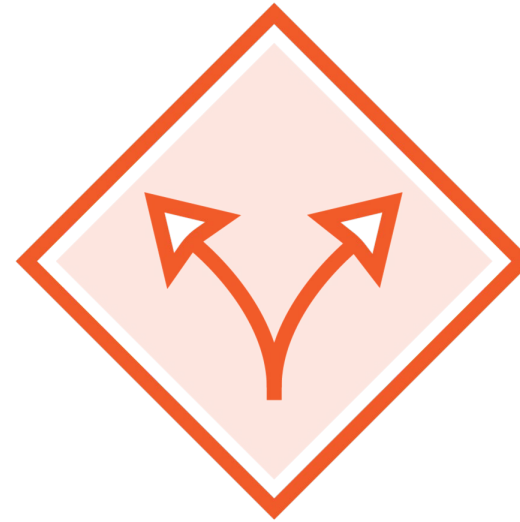
Handling Issues



Review and
understand the
messages



Check for
configuration
errors



Change
modules or
options as
needed

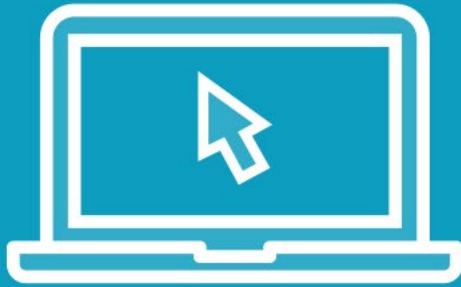


Try again

Launching the Attack



Demo



Launch exploits

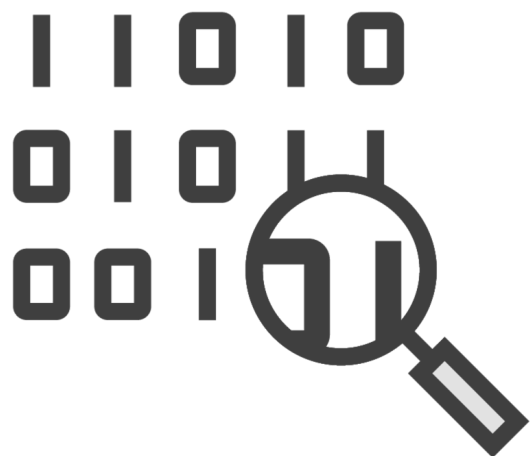
Review output



Post Modules and Local Exploits



Post Exploitation



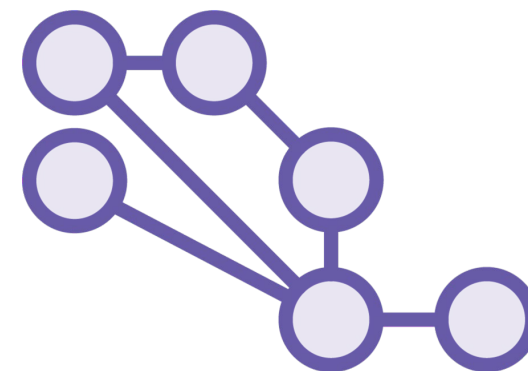
Explore



Exfiltrate



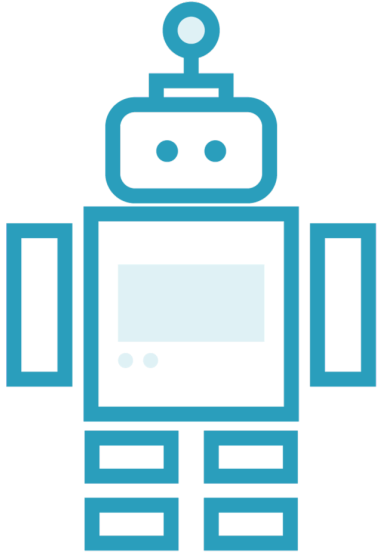
Persist



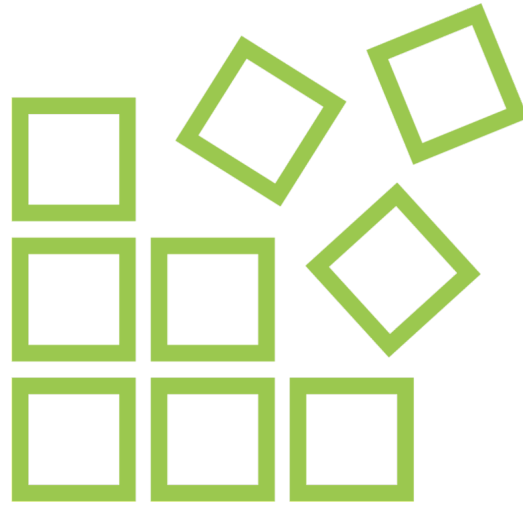
Pivot



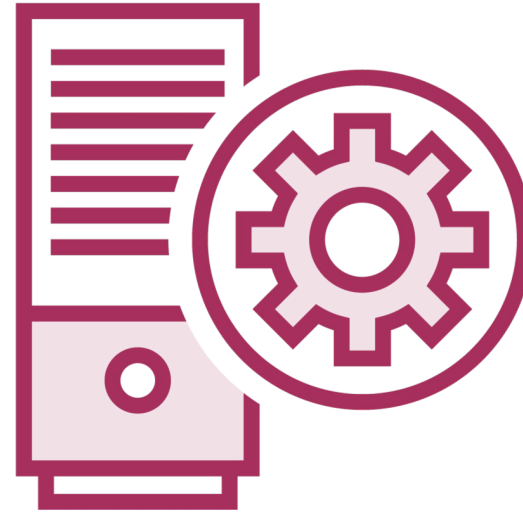
Post Modules



**Simplify and
automate**



**Gather
information**

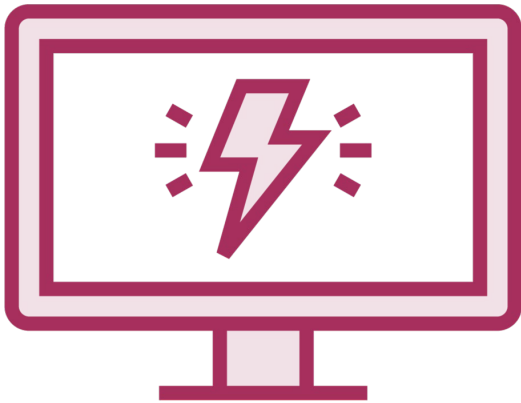


**Manage
the system**



**Escalate
privileges**

Local Exploits



Exploit internal
components



Operate as an
unprivileged
user

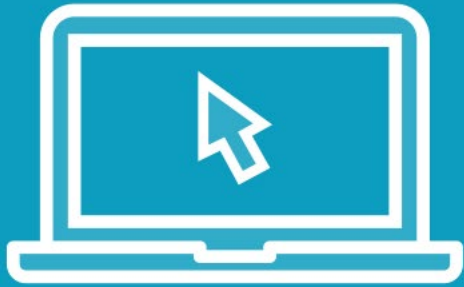


Open a session
with higher
privileges



Establish
persistence on
the target

Demo



Search

Select

Configure

Run / Exploit



Meterpreter



Meterpreter in Post Exploitation Operations



Explore targets

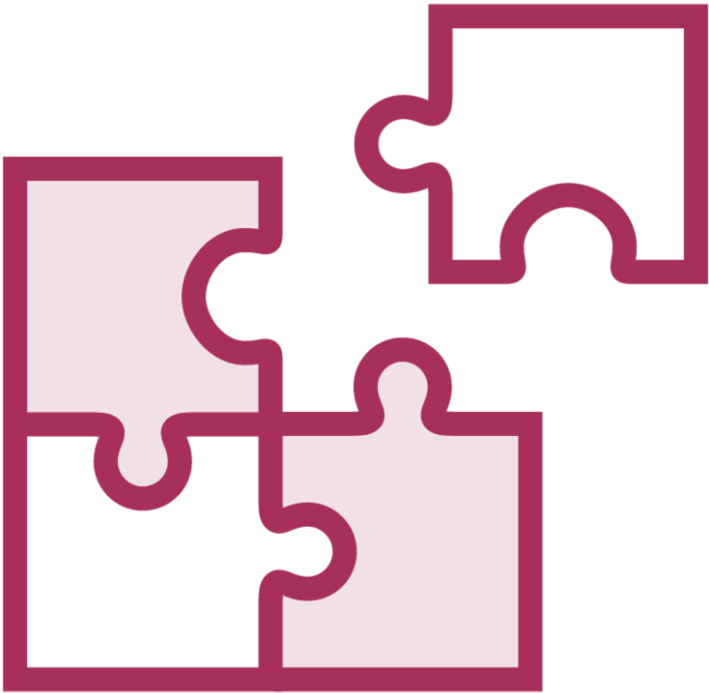
Monitor users

Establish persistence

Utilize local exploits and post modules

Pivot

Some Meterpreter Extensions



extapi

sniffer

espia

kiwi

lanattacks

incognito

networkpug

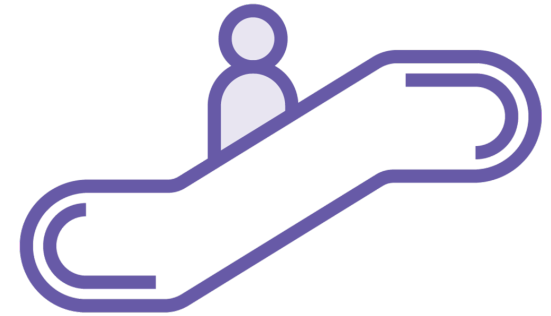
Privilege Escalation Library



`timestamp`

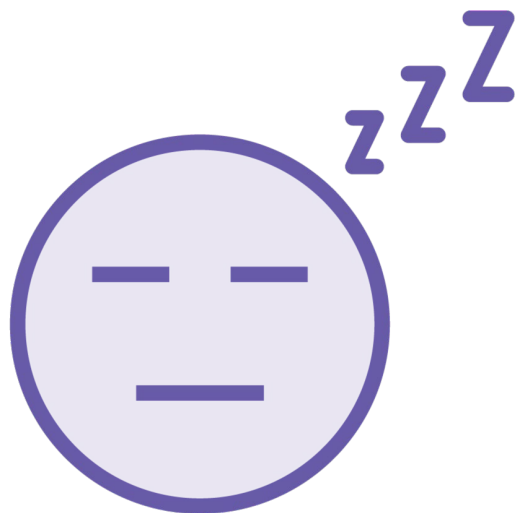


`hashdump`



`getsystem`

Targeting Users



idletime



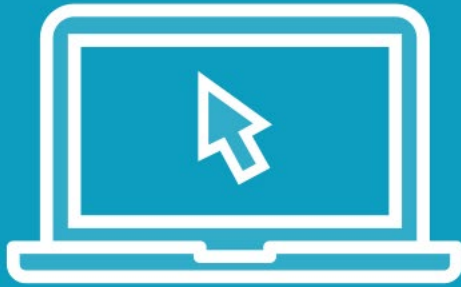
keyscan



record_mic



Demo



Find help

Explore the file system

priv library

incognito extension

Post modules

Focus on the user



Summary



Module Summary



Understanding Metasploit messages

Starting the exploit module

Post-exploitation activities

- Post modules
- Local exploit modules
- Meterpreter



Up Next:

Working with the Metasploit Framework

