

# Preparing an Attack

---



**Keith Watson**

INFORMATION SECURITY PROFESSIONAL

@ikawnoclast ikawnoclast.com



# Module Overview



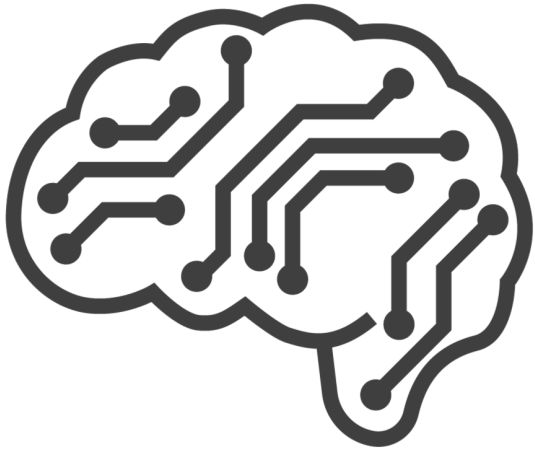
**Vulnerabilities**

**Selecting exploits**

**Configuring exploits and payloads**



# Vulnerabilities



Memory safety

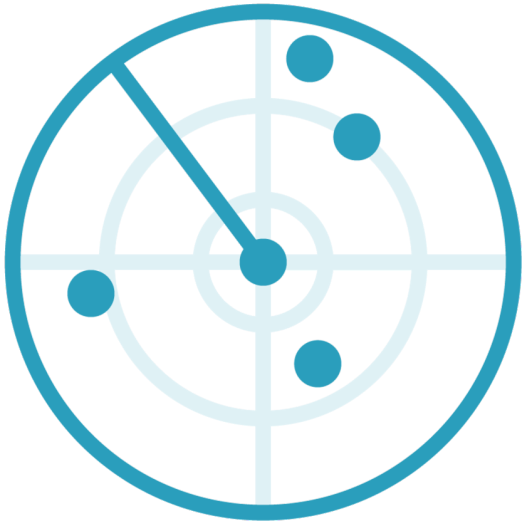


Privilege escalation

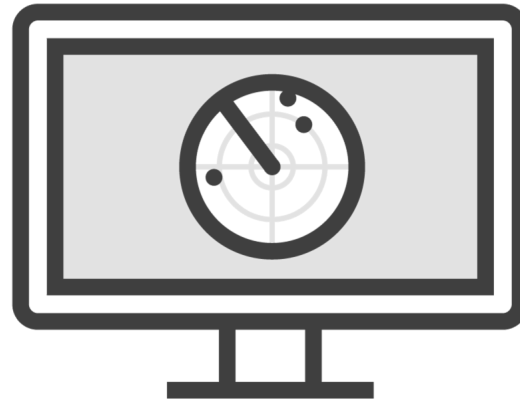


Input validation

# Vulnerability Detection



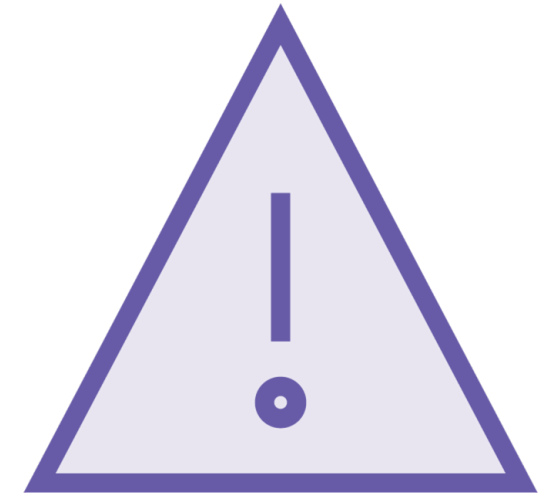
Service  
scanning



Vulnerability  
scanning



Vulnerability  
search



0-day  
knowledge

# Globomantics Red Team Testing Approaches

Globomantics utilizes its Red Team in a variety of penetration testing scenarios



## Proactive

- During development
- Prior to production



## Validation

- Compliance
- Control validation



## Exercises

- Red v. blue
- Purple

# Searching and Selecting Exploits

---



# Searching for Exploit Modules

search

Name or description

Author

Date

Platform or arch

Port

Rank

Identifier

Check



# Viewing Exploit Module Information

`info path/exploit`

**Basic information**

**Available targets**

**Check supported**

**Basic options**

**Payload information**

**Description**

**References**





# Selecting an Exploit



use

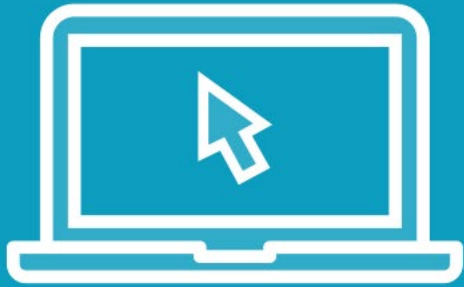
- by full path name
- by search index number

show

- info
- options
- payloads



# Demo



Help

Search

Select



```
msf5 > search type:-exploit apache  
msf5 > search target:windows platform:-x86 type:-post  
msf5 > use ircd  
msf5 > use teamviewer  
msf5 > search
```

## Continue Experimentation

**Negate search parameters with “-”**

**Search with the use command**

**Show cached search output**

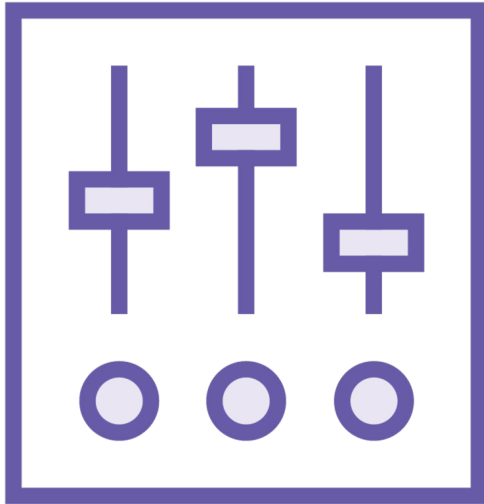


# Configuring Exploits and Payloads

---



# Configuring Exploit Modules



Options



Targets



Payloads

# Module Option Details

show options

Name

Current setting

Required

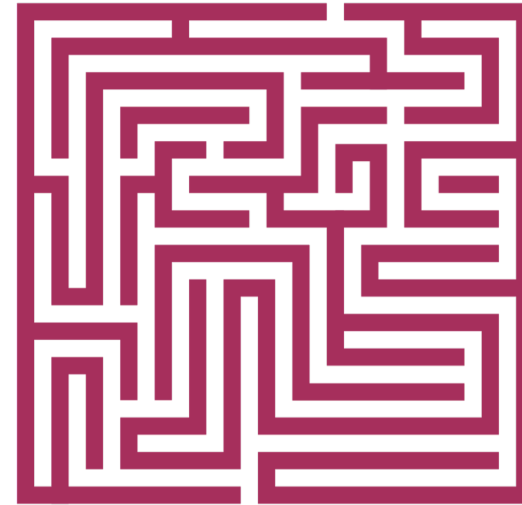
Description



# Module Options



Basic options



Advanced options



# Exploit Targets

**show targets**

**One or more targets**

**Automatic targeting**

**Specific**

- Operating system
- Version, service pack, release, language
- Processor type or environment
- Exploit protection
- Techniques





# Check Functions

**check**

**Is the exploit module configured correctly?**

- Is RHOSTS correct?

**Is the target service responding?**

**Is the target vulnerable?**

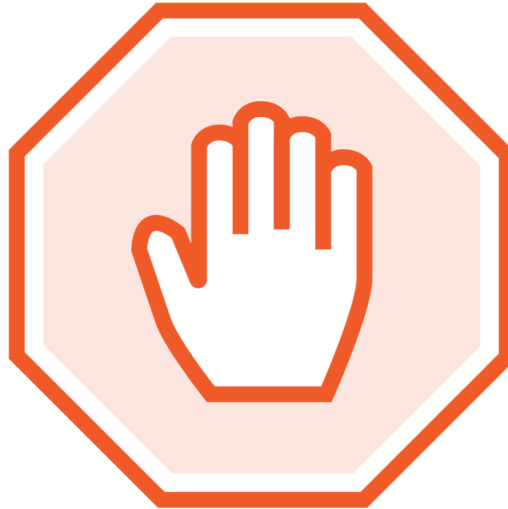
**Will the exploit likely work?**



# Payloads



Automatically  
selected

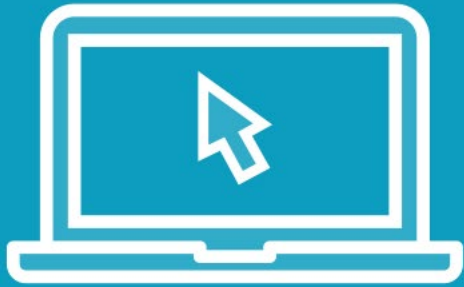


May be limited by the  
vulnerability exploited



Have configurable  
options

# Demo



## Help

## Information

- Exploit
- Payload
- Targets

## Configuration



# Summary

---



# Basic Attack Configuration Steps



## Find the exploit module to use

- Select with `use path/exploit`

## Review and set exploit options

- set RHOSTS *<target system>*
- set target *<index>*
- set payload *<index>* (if needed)

## Review and set payload options

- set LHOST *<local IP or adapter>*
- set LPORT *<local port>*

# Module Summary



**Finding help information inside Metasploit**

**Searching for exploit modules for our target**

**Selecting and configuring the exploit module needed**



# Up Next: Launching an Attack

---

