

# Metasploit Framework Capabilities

---



**Keith Watson**

INFORMATION SECURITY PROFESSIONAL

@ikawnoclast ikawnoclast.com



# Module Overview



**Intelligence Gathering**

**Network Scanning**

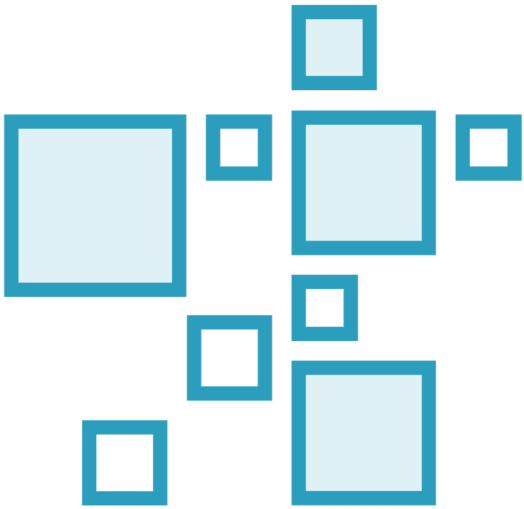
**Vulnerability Scanning**

**Exploitation**

**Post Exploitation**



# Components and Terminology



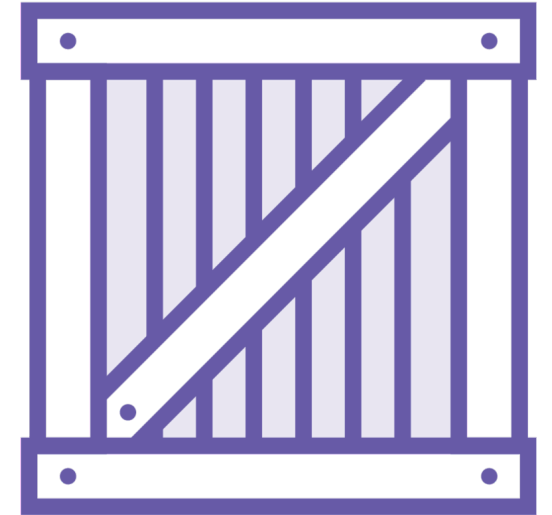
Modules



Scanners



Exploits



Payloads



# Command Line Interface

```
      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c      c000000000000x.
      :000000000000000k,    ,k000000000000000:
      '000000000k00000:  :000000000000000000'
      o00000000.MMMM.o0000o0000l.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
      .00000000.MMM.;MMMMMMMMMMMM;MMMM,00000000.
      c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
      o000000.MMM.0000.MMM:0000.MMM,000000o
      l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d00o'WM.0000o0000x0000.MX'x00d.
      ,k0l'M.0000000000000.M'd0k,
      :kk;.0000000000000.;0k:
      ;k000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v5.0.91-dev-68c4ef34a490be101cb95dfc6cd603cc26f68049]
+ -- --=[ 2022 exploits - 1099 auxiliary - 343 post           ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops              ]
+ -- --=[ 7 evasion                                           ]

Metasploit tip: To save all commands executed since start up to a file, use the makerc command

msf5 > 
```



# Globomantics Red Team

The Metasploit Framework is a key tool in our arsenal.



# Intelligence Gathering

---



# Intelligence Gathering

The process of collecting accurate information about the targets surreptitiously.



# Active or Passive

## Active

Interacting with the targets

Identifying active systems

Identifying active services

Creating accounts on applications

Directly gathering information

*Overt*

## Passive

Avoiding interactions with the targets

Finding information about the systems

Finding information about the services

Reading about the application

Searching other sources for information

*Covert*





# Active Intelligence Gathering



Network scanning



Port scanning



Service version scanning



Service configuration scanning



Fuzzing



# Passive Intelligence Gathering



`whois`



`host`, `nslookup`, and `dig`



`auxiliary/gather/enum_dns`



`auxiliary/gather/shodan_search`



`auxiliary/gather/ssllabs_scan`



# Network Scanning

---

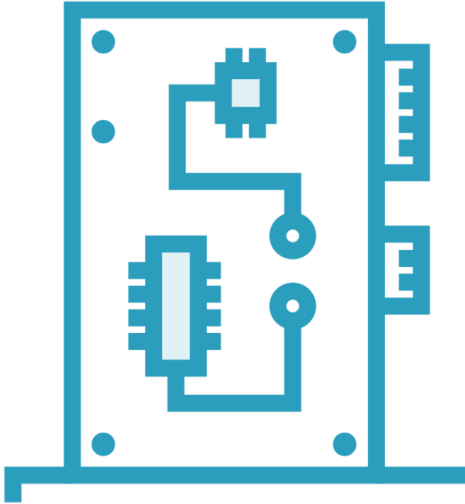


# Auxiliary Scanning Modules

```
msf5 > use auxiliary/scanner/  
Display all 573 possibilities? (y or n)
```



# Local Network Scanning



`auxiliary/scanner/discovery/  
arp_sweep`



`auxiliary/scanner/discovery/  
ipv6_neighbor`



# TCP and UDP Port Scanning



`auxiliary/scanner/portscan/syn`



`auxiliary/scanner/portscan/tcp`



`auxiliary/scanner/discovery/udp_sweep`



# Service Scanning



`auxiliary/scanner/ftp/ftp_version`



`auxiliary/scanner/http/http_version`



`auxiliary/scanner/smb/smb_version`



`auxiliary/scanner/ssh/ssh_version`



# Nmap and Metasploit



## **Nmap can be run independently**

- Gather data from a separate team
- Import scans into Metasploit database

## **Nmap can be run inside msfconsole**

- Incorporate data directly

## **Nmap hosts and services database**

- Searchable



# Vulnerability Scanning

---



# Metasploit Modules



“No authentication” auxiliary modules



Login auxiliary modules



Exploit modules that check for the vulnerability

# Third-Party Vulnerability Scanning



Data ingestion



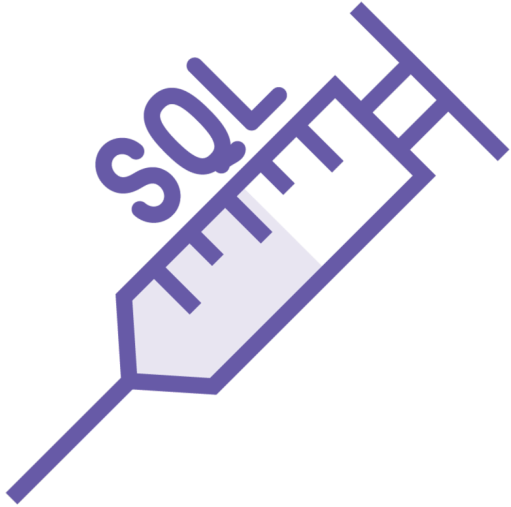
Scan configuration



Scan management



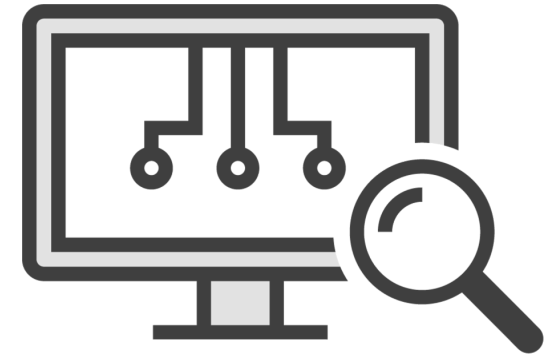
# Open Source Scanning Tools



SQLMap



WMap



OpenVAS

# Commercial Scanning Products



Tenable Security Nessus



Rapid7 Nexpose

# Exploitation

---



# Methods of Attack

## Active

Target specific systems with known and exploitable weaknesses in available services

Connect to vulnerable service on the target

Send exploits to the service

*Execute payload on the target*

## Passive

Target specific users with suspected and common weaknesses in available clients

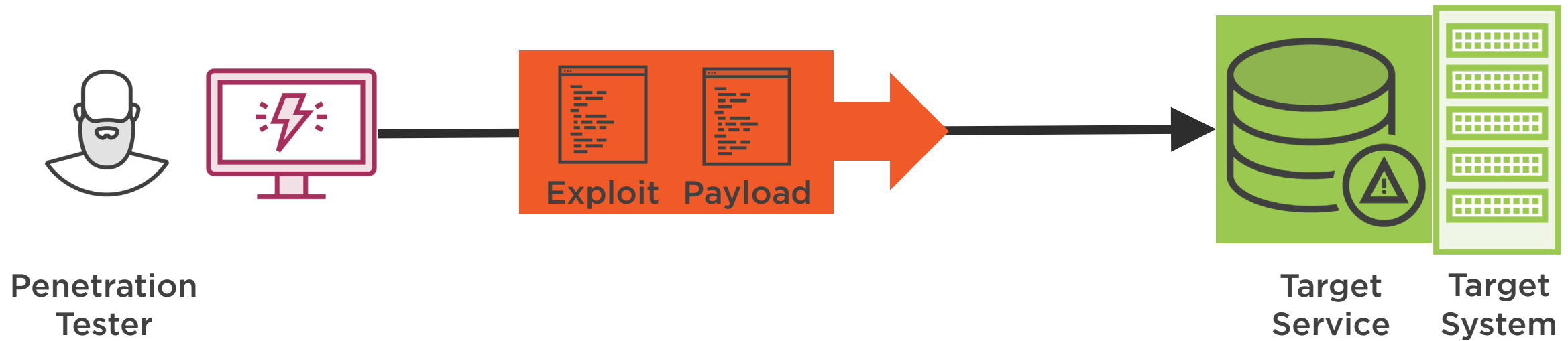
Wait for clients to connect to our server

Feed exploits to vulnerable clients

*Execute payload on the target*

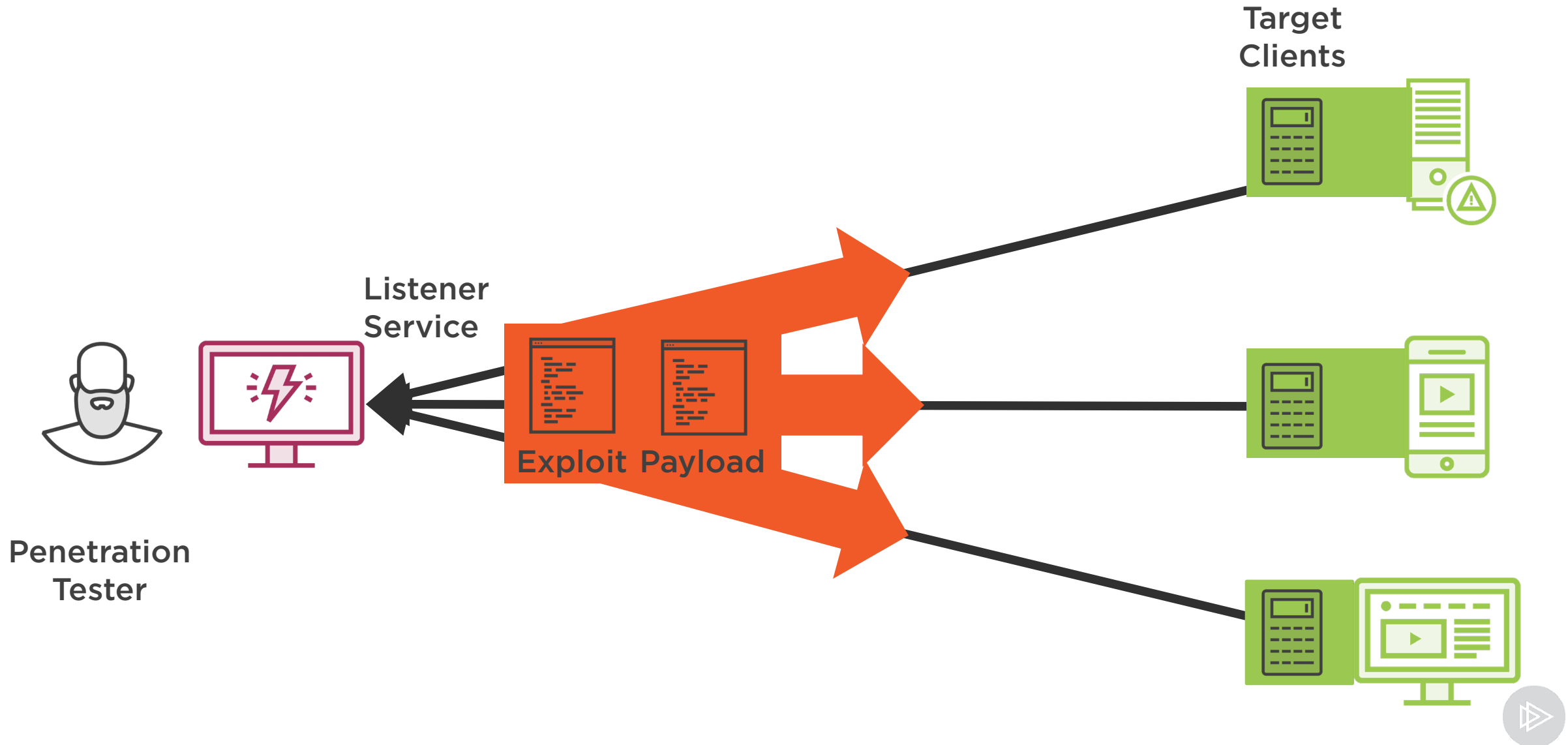


# Active Attack





# Passive Attack



# Passive Attack Vectors



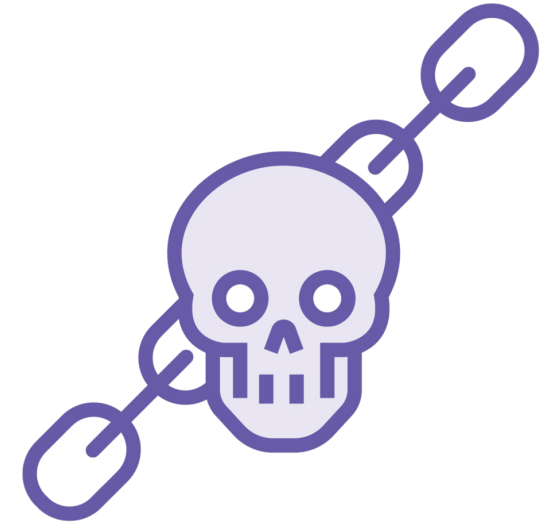
Phishing email



Fake advertising  
“malvertising”



Compromised  
web site



Enticing link

# Payload Actions

Start a  
shell

Execute a  
command

Download files  
and execute

Start an  
interpreter

Interact with  
the user

Start  
Meterpreter



# Post Exploitation

---



# Post Modules



Gather network, system, and application information



Gather password hashes or credentials



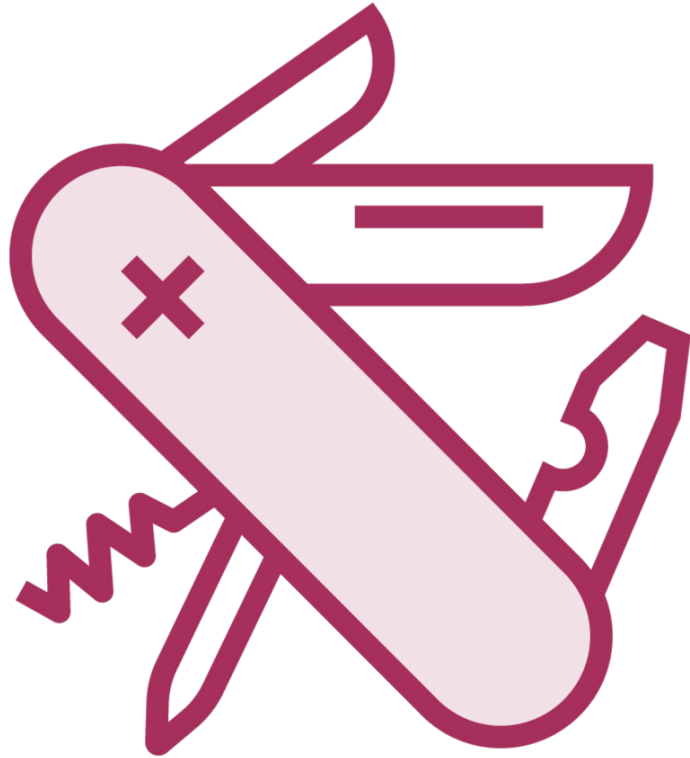
Modify the system



Escalate privileges



# Meterpreter



**Meterpreter is the *Metasploit Interpreter***

**Post exploitation toolkit and environment**

- Full command set, scripting, modules
- File search, extraction, and upload
- Process examination and manipulation
- Password hash collection
- Packet capture, routing, and forwarding

# Summary

---



# Module Summary



**Gather target details**

**Scan networks and services**

**Scan for vulnerabilities**

**Exploit vulnerabilities**

**Explore compromised systems**





Up Next:

Metasploit Framework Architecture

---

