

Attacking Targets with Metasploit

INTERPRET METASPLOIT FRAMEWORK OUTPUT



Kevin Cardwell

PRESIDENT, CYBER2ALBS LLC

www.cyber2labs.com



Overview



Investigate module output

Clarify exploit content

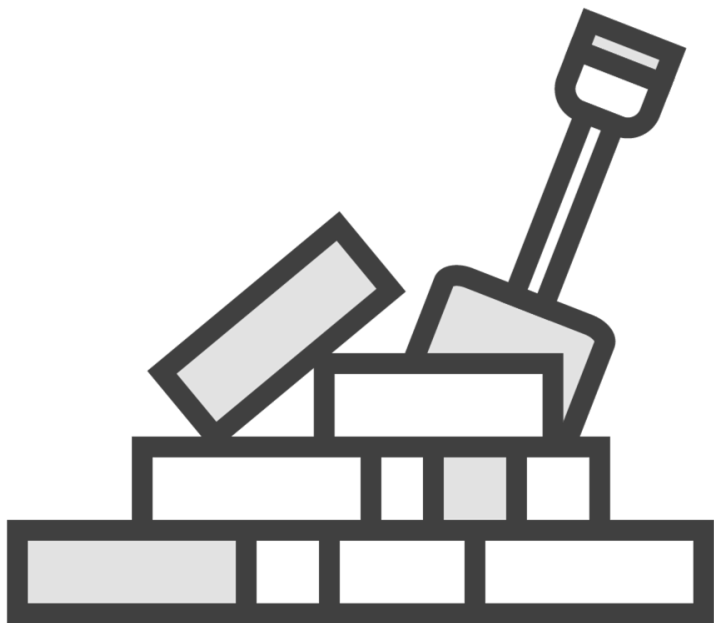
Inspect module scanners



Investigate Module Output



Metasploit Architecture



Filesystems and libraries

Modules

Metasploit object model

Mixins and plugins



Module Types

auxiliary

encoders

exploits

nops

payloads

post



Primary



Auxiliary



Exploits

Additional

Payloads consist of code that runs remotely, while encoders ensure that payloads make it to their destination intact. Nops keep the payload sizes consistent across exploit attempts.



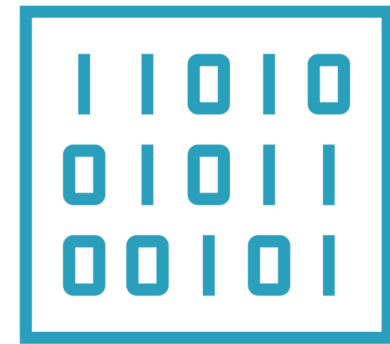
Payloads

Singles, stagers and stages



Encoders

Ruby, php, x86 and x64

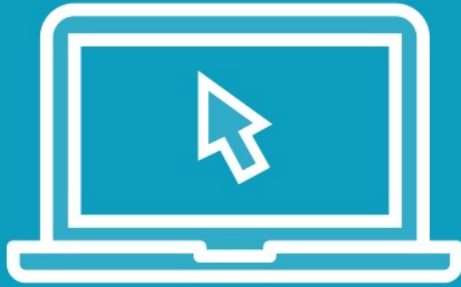


Nops

Arm, sparc, x86 and x64



Demo



Module exploration



Clarify Exploit Content



Main Components

Name

Rank

Targets

Options

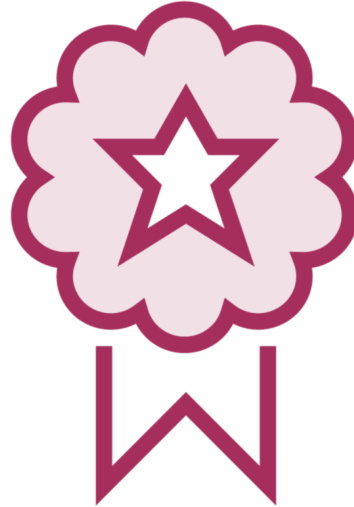
Description



Exploit Rank



Good

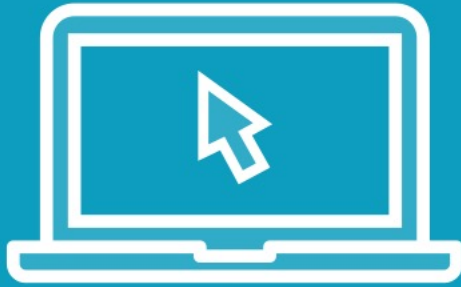


Great



Excellent

Demo



Exploit content



Inspect Module Scanners



Scanners



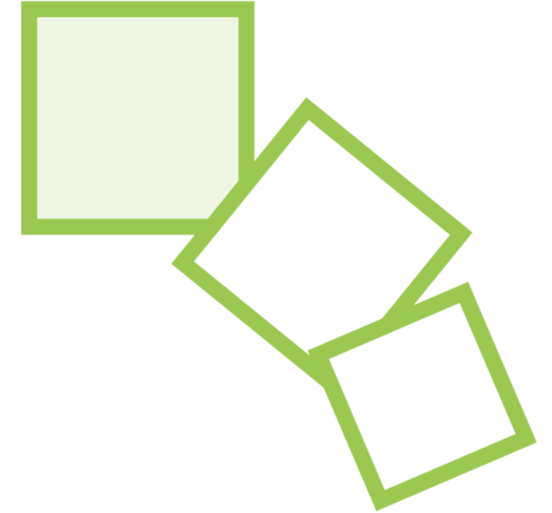
Ports



Services



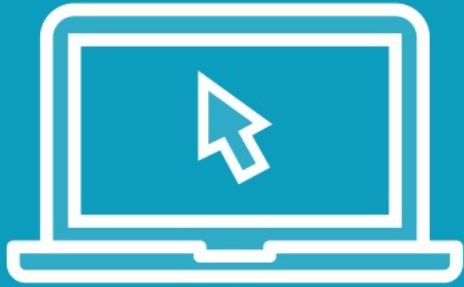
Protocol



Custom



Demo



Module scanners



Summary



Investigated module output

Clarified exploit content

Inspected module scanners

