

Attacking Targets with Metasploit

CLIENT-SIDE ATTACKS



Kevin Cardwell

PRESIDENT, CYBER2ALBS LLC

www.cyber2labs.com



Overview



Tricking the client

Prevent detection

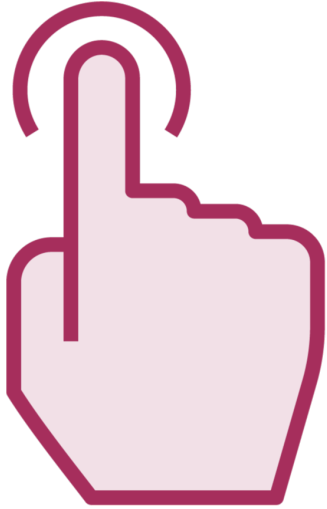
Identify types of client exploits



Tricking the Client



User Help Required



Clicking



Opening



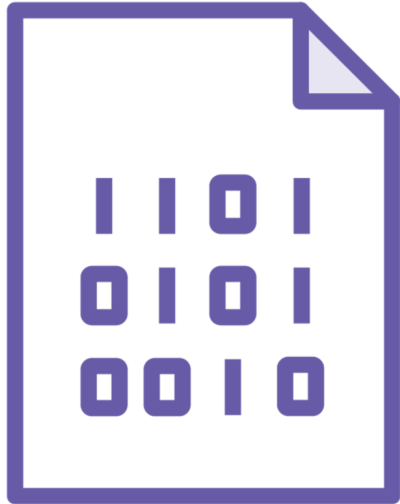
Running

Phishing

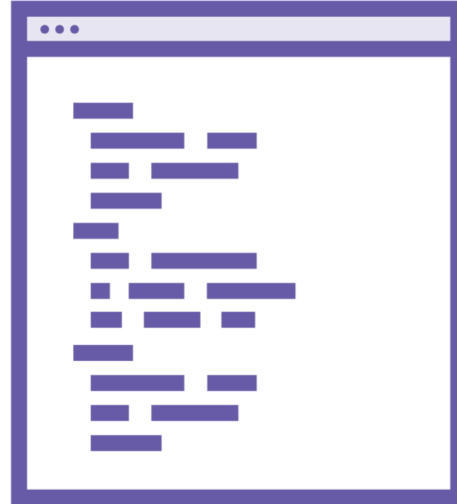


The preferred method to get client interaction is via an email!

Building Payloads



Binary



Scripts



Trojan



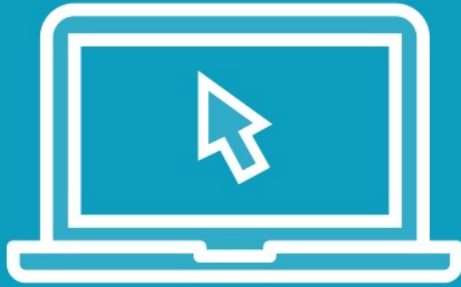
Tool



The msfvenom tool can be used for generating payloads to be used in many locations and offers a variety of output options, from perl to C to raw.



Demo



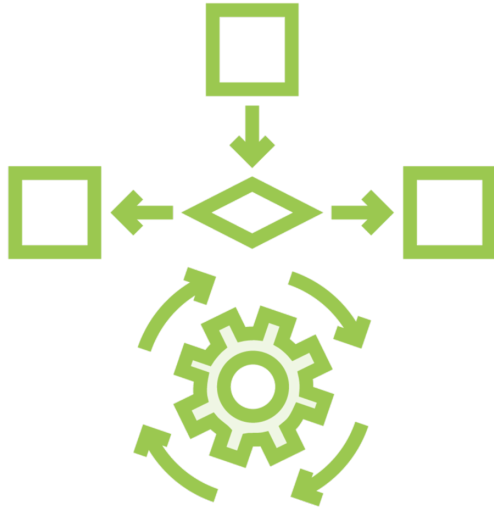
Building Payloads



Avoiding Detection



Evasion

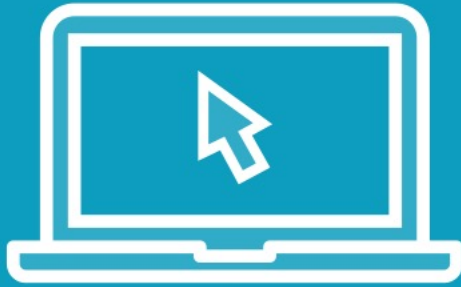


Encoding



Encryption

Demo



Evasion



Identify Client Exploits





Initial access is required

Installed applications are a source for attack

Depends on configuration of the endpoint



Requirements for Success

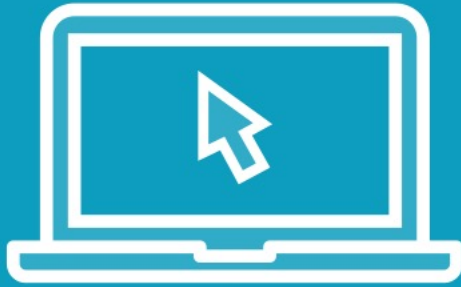


Kernel



Patches

Demo



Local attacks



Summary



Tricked the client

Prevented detection

Identified types of client exploits

