

Credential Access with Cain & Abel



Jeff Stein

CISSP, GCED, CEH, CHFI, SECURITY+

www.securityinobscurity.com







Creator: Massimiliano Montoro



Tooling for Microsoft operating systems designed for passwords recovery. Capable of cracking numerous types of encrypted passwords using Dictionary, Brute-Force, and Cryptanalysis attacks



Free software for password cracking
using the Windows operating system

Available at the oxid.it site archive on the
Wayback Machine:

[https://web.archive.org/web/20190616083719/http://
www.oxid.it/cain.html](https://web.archive.org/web/20190616083719/http://www.oxid.it/cain.html)

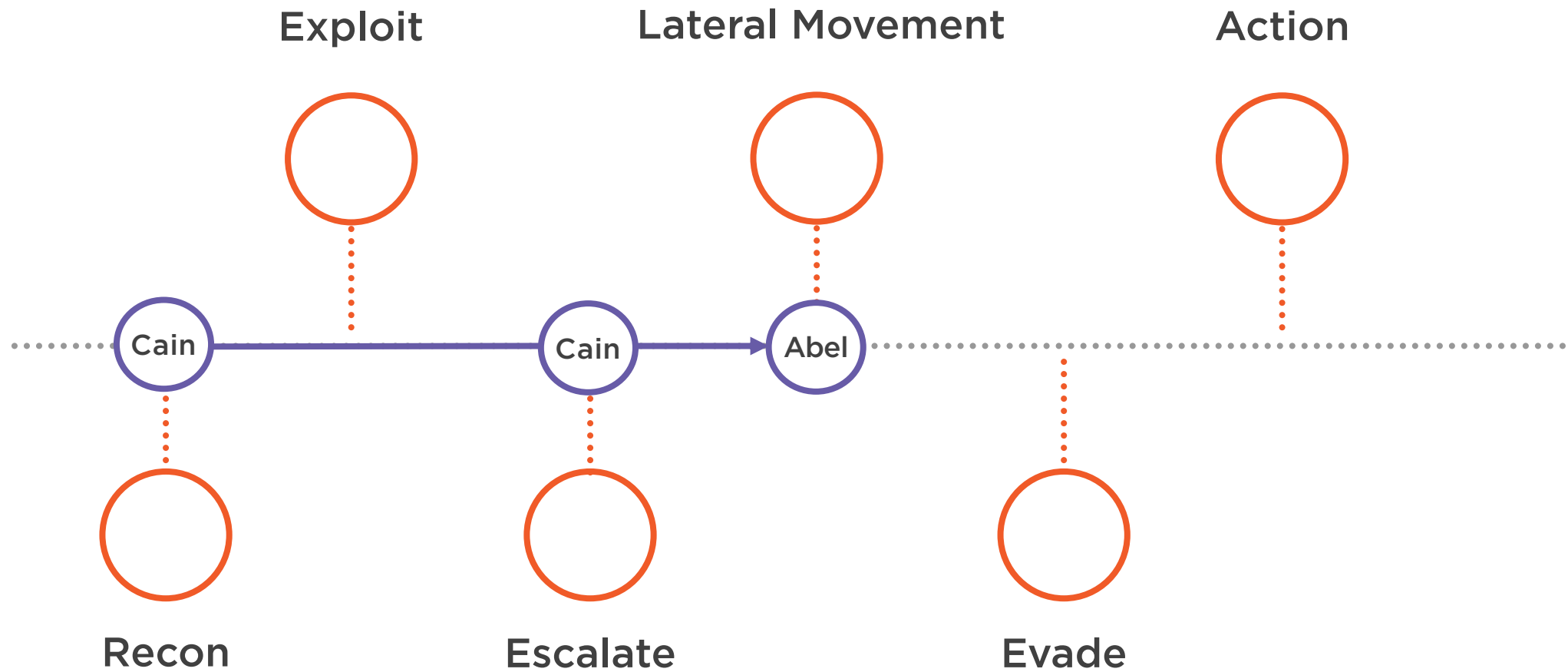
Manipulate network traffic using the
Windows OS

Use harvested credentials to move
through multiple systems in a network
during an attack engagement.

Potential challenges with anti-virus
protection



Kill Chain



MITRE ATT&CK

Tactics

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1014:

Discovery

T1110:

Brute Force

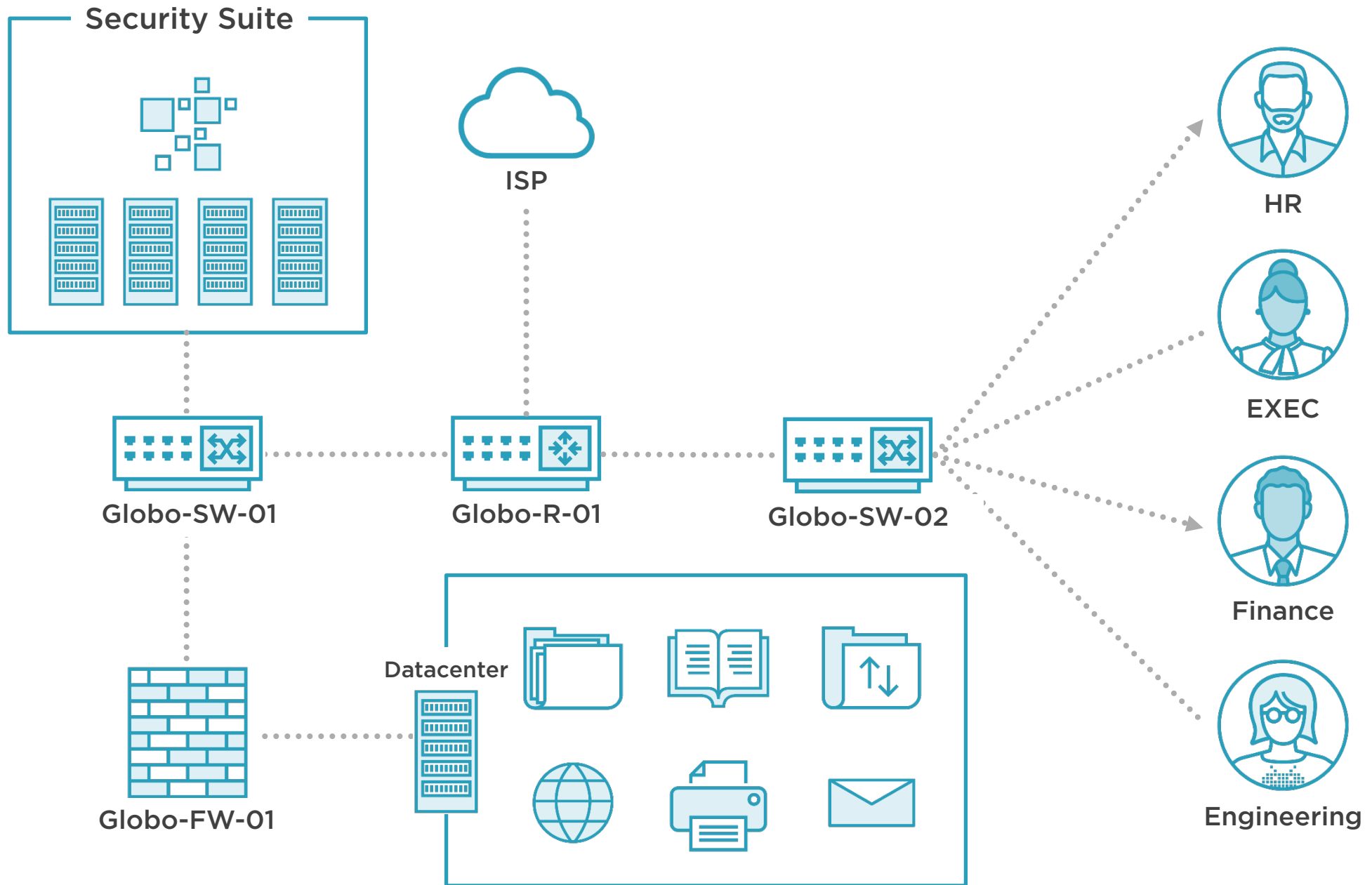
T1110.002

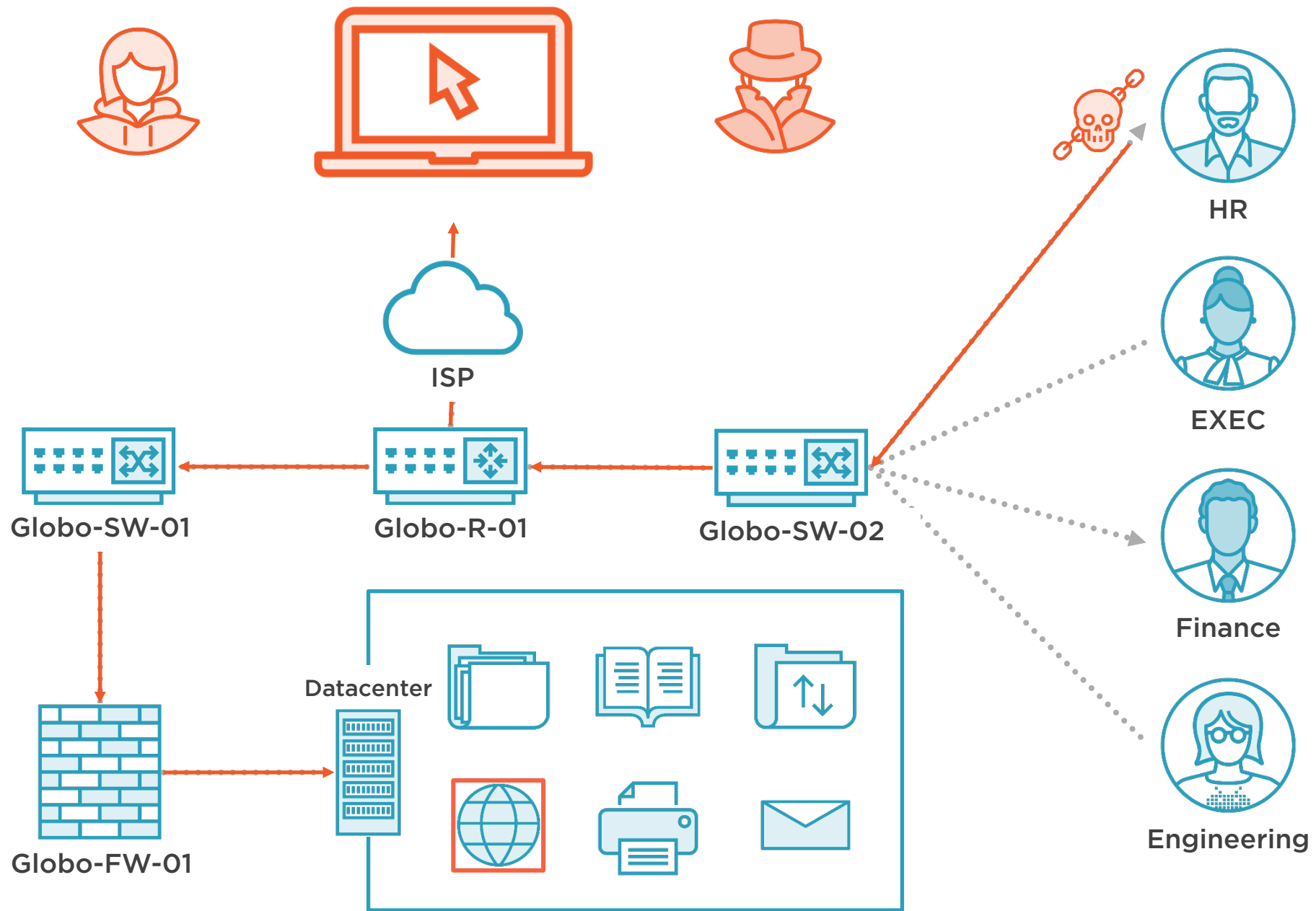
Password Cracking

T1219:

Remote Access Software







Demo



Enable reconnaissance of targeted network

Crack WPA wireless network with Cain

- Perform Dictionary Attack against WPA network hash

Identify systems on network to target



Demo



Perform a man-in-the-middle attack using Cain

- Sniff the network for credentials
- Leverage Cain's ARP Poisoning feature

Used to exploit credentials transmitted across the network

Establish foothold in network to escalate attack



Demo



Move laterally with Abel

- Access and control targeted system
- Leverage Abel remotely to send commands to system

Used to access remote system credentials

Run commands on remote system and expand foothold across the targeted network



Demo



Access system credentials with Cain

- Exploit system to gather valuable credentials
- Perform Cryptanalysis Attack against NTLM hashes

Used to further access credentials on systems and move laterally



More Information

Capabilities

VoIP

https://web.archive.org/web/20180926230958/http://www.oxid.it/ca_um/topics/voip.htm

RSA SecurID Token Calculator

https://web.archive.org/web/20190408060414/http://www.oxid.it/ca_um/topics/rsa_securid_token_calculator.htm

Related Information

Wifi Samples to explore

https://wiki.wireshark.org/SampleCaptures#Wifi_2F_Wireless_LAN_captures_2F_802.11

Password Lists

<https://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.html>

Rainbow Tables

<http://project-rainbowcrack.com/table.htm>

