

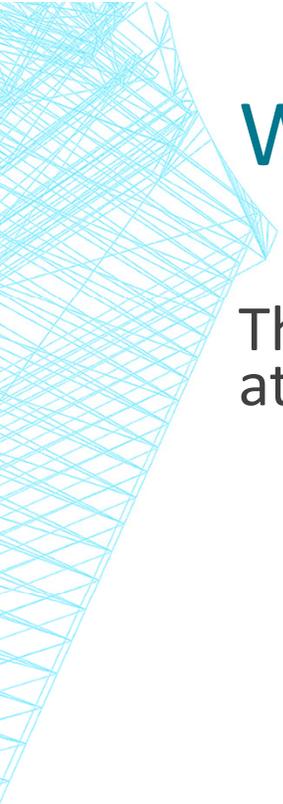
# THE HACKER TOOL

Jay Ferron

CEHi, CDPSE ,CISSP, CHFii, C)PTEi, CISM, CRISC, CVEi, MCITP, MCSE, MCT, MVP, NSA-IAM...

[jferron@interactivesecuritytraining.com](mailto:jferron@interactivesecuritytraining.com)

[blog.mir.net](http://blog.mir.net)



# WHAT WE WILL COVER

This is an overview of some of tools that are used by hackers to attack using various means that include:

- Social Engineering
- Network Penetration
- Vulnerabilities scanners
- Wi-Fi
- Physical Security
- Attached Devices
- Phones

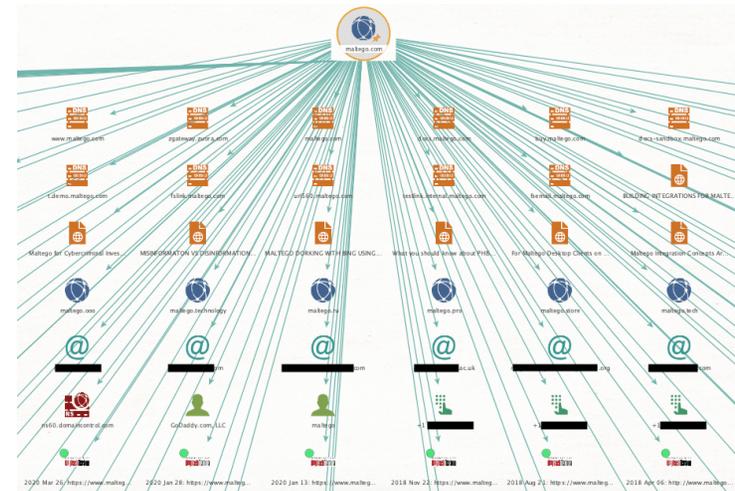
# SOCIAL ENGINEERING

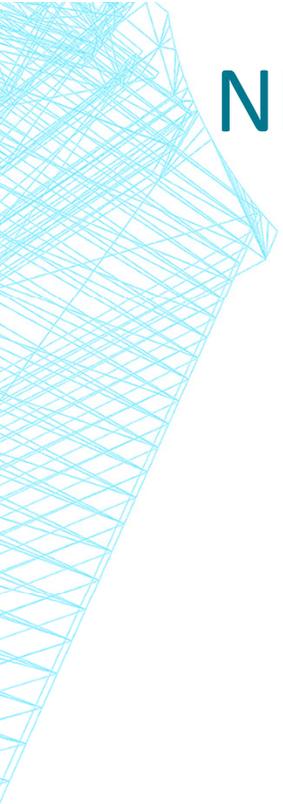
Maltego -OSINT (open-source intelligence) investigation tool

If you can get a user to click it's Over !!!

## Demo

Social Engineering Tool Kit (SET)- SET has various custom attack vectors that enable you to set up a believable attack in no time.





# NETWORK PENETRATION

Learning about the network

Network scanner

NMAP

**Demo**

Masscan

DNS Tools -

Dig

Nslookup

Attacking the Network

Metasploit - a tool for developing and executing exploit code against a remote target machine.

# Vulnerabilities Scanners

Nessus

Qualys

OpenVas- Greenbone

Core-Impact

Greenbone Security Assistant

Refresh every 30 S... | Logged in as Admin eric | Logout Thu Nov 1 16:10:05 2018 PDT

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: host=192.168.0.22  
first:1 rows=50 apply\_overrides=0 min\_qod=70 sort=name

Results (119 of 757)

Results by Severity Class (Total: 119)

Medium: 5  
Low: 109  
Log: 5

Results vulnerability word cloud

Results by CVSS (Total: 119)

Vulnerability	Severity	QoD	Host	Location	Created
Check for SMB accessible registry	0.0 (Log)	97%	192.168.0.22	general/tcp	Tue Oct 30 07:04:45 2018
Check for SMB accessible registry	0.0 (Log)	97%	192.168.0.22	general/tcp	Tue Oct 30 07:26:26 2018
Check for SMB accessible registry	0.0 (Log)	97%	192.168.0.22	general/tcp	Tue Oct 30 07:33:33 2018
Check for SMB accessible registry	0.0 (Log)	97%	192.168.0.22	general/tcp	Tue Oct 30 07:46:10 2018
Check for SMB accessible registry	0.0 (Log)	97%	192.168.0.22	general/tcp	Tue Oct 30 07:56:17 2018
CPE Inventory	0.0 (Log)	80%	192.168.0.22	general/CPE-T	Tue Oct 30 07:04:52 2018
CPE Inventory	0.0 (Log)	80%	192.168.0.22	general/CPE-T	Tue Oct 30 07:28:32 2018
CPE Inventory	0.0 (Log)	80%	192.168.0.22	general/CPE-T	Tue Oct 30 07:35:39 2018
CPE Inventory	0.0 (Log)	80%	192.168.0.22	general/CPE-T	Tue Oct 30 07:48:18 2018
CPE Inventory	0.0 (Log)	80%	192.168.0.22	general/CPE-T	Tue Oct 30 07:58:23 2018
CPE Inventory	0.0 (Log)	80%	192.168.0.22	general/CPE-T	Tue Oct 30 09:21:42 2018

# Wi-Fi - WEP/WPA/WPA2

## Tools

Aircrack-ng- full suite of tools for sniffing, and cracking WEP/WPA/WPA2

## DEMO

Airgeddon – menu driven suite of tools



Vulnerable to offline **dictionary attacks**: a captured handshake can be used to brute-force the password



**No forward secrecy**: can decrypt previously captured traffic after learning the password



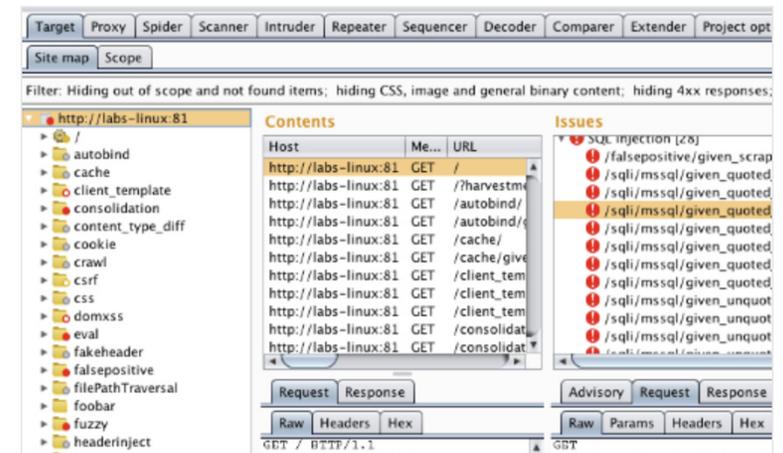
**Unprotected management frames**: can spoof beacons, deauthentication frames, & other non-data frames



WIFI PINEAPPLE

# WEB SITES

Burpsuite - Burp Suite is an integrated platform for performing security testing of web applications



WPScan - WordPress security scanner

Skipfish- is an active web application security reconnaissance tool.

# PHYSICAL SECURITY

If It can be touch it, you loose...

Cameras – All shapes and sizes

Screen Grab - This covert inline screen grabber sits between HDMI devices - like a computer and monitor, or console and television to quietly capture screenshots



Keyboard Loggers Up to 16gb of storage both wire and wireless



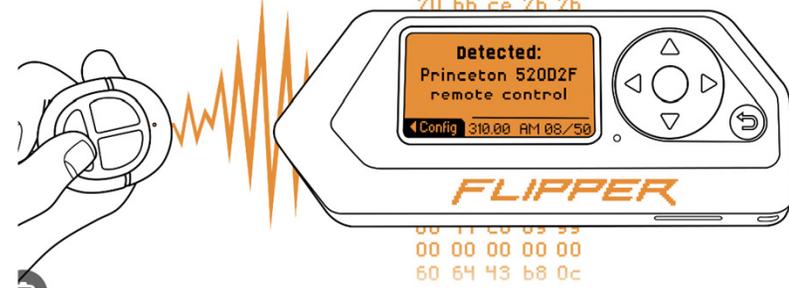
# PHYSICAL SECURITY

Card Readers

Icopy-x - Rapidly and easily clone RFID tags



Flipper Zero – RFID, NFC, Garage doors & barriers, Smart sockets & bulbs, IoT sensors & doorbells, and Infrared Transmitter



# ATTACHED DEVICES

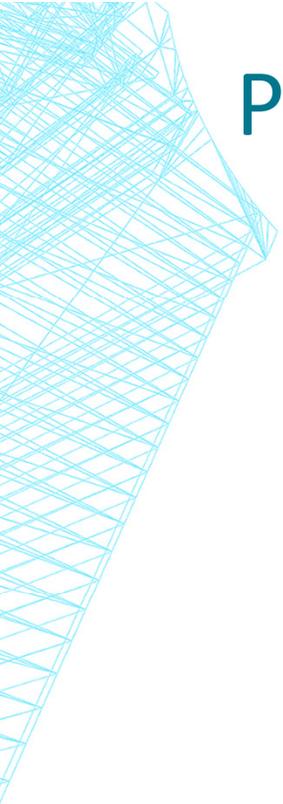
Rubber Duck type products -computers trust humans. Humans use keyboards. Hence the universal spec — HID, or Human Interface Device. A keyboard presents itself as a HID, and in turn it's inherently trusted as human by the computer.

## DEMO

<https://ducktoolkit.com/userscripts>

LAN Taps -(Terminal Access Point) is a passive device to monitoring the traffic over a Lan connections

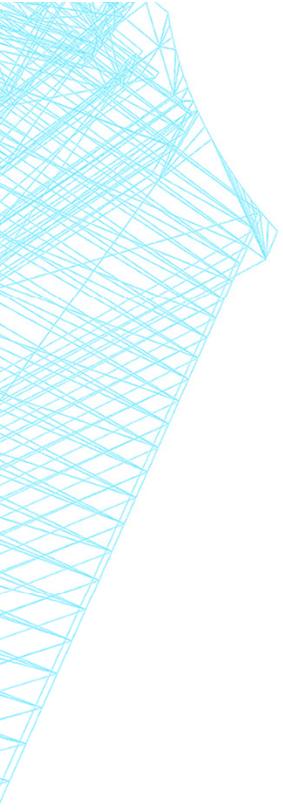




# PHONES

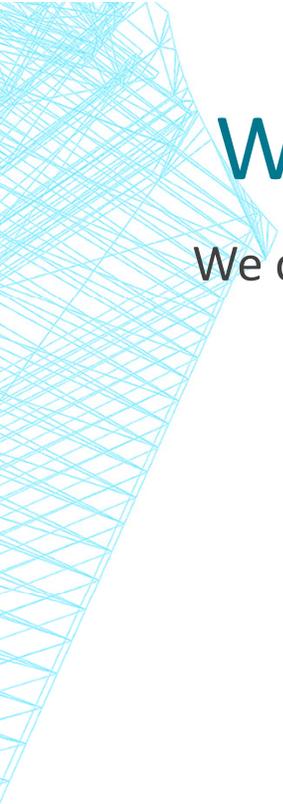
O.MG / USB Ninja Cables  
Looks and functions just like a regular USB cable (both power and data) Emulating keyboard and mouse actions, payloads can be completely customized.

O.MG Cable Tier	Basic	Elite
Keystroke Injection (DuckyScript™)	✓	✓
Mouse Injection	✓	✓
Payload Slots	8	50-200*
Payload Speed	120 keys/sec	890 keys/sec*
Self-Destruct	✓	✓
Geo-Fencing	✓	✓
WiFi Triggers	✓	✓
FullSpeed USB Hardware Keylogger		✓
HIDX StealthLink		✓*
Networked C2		✓*
Extended WiFi range		✓
Stealth-Optimized Power Draw		✓



# QR CODES





# WE HAVE ONLY TOUCHED THE SURFACE

We could spend days and month on this topic.

## Questions

Jay Ferron

[jferron@interactivesecuritytraining.com](mailto:jferron@interactivesecuritytraining.com)

[blog.mir.net](http://blog.mir.net)