How An Attacker Sees Your Website
A View Through The Eye of the Hacker

```
root@kali:~# su
```

Steve Schwartz

AVT Marketing

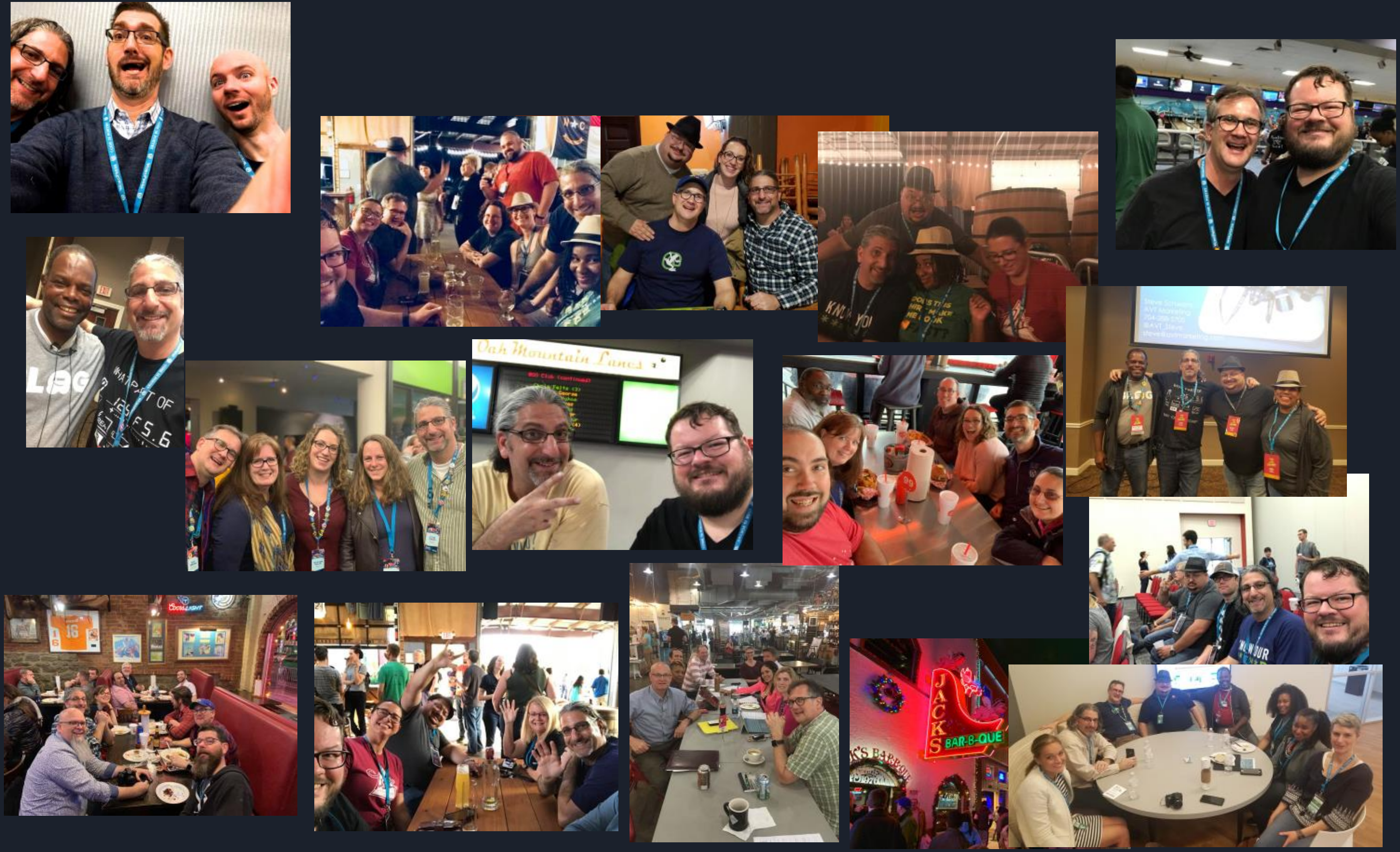
704-288-5705

Steve@AVTmarketing.com

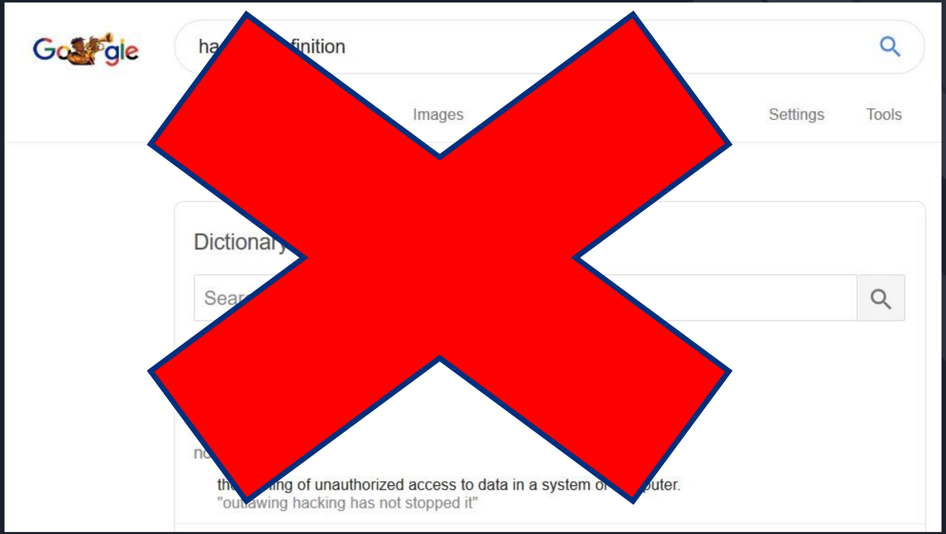
About Me

- 13 years in Corp America in Finance / Tech / Software Implementation
- Started Small Photo / Video Production Company in 2008
- Added Website Design in 2010 / Off Security 2014
- Certified Ethical Hacker (CEH) 2018
- Pursuing Certified Information Systems Security Professional (CISSP)

- Was 80/20 video/web
- Now 80/20 web/video


Oak Mountain Lanes
JACKS
BAR-B-QUE

What is Hacking?



ha finition

Images

Settings

Tools

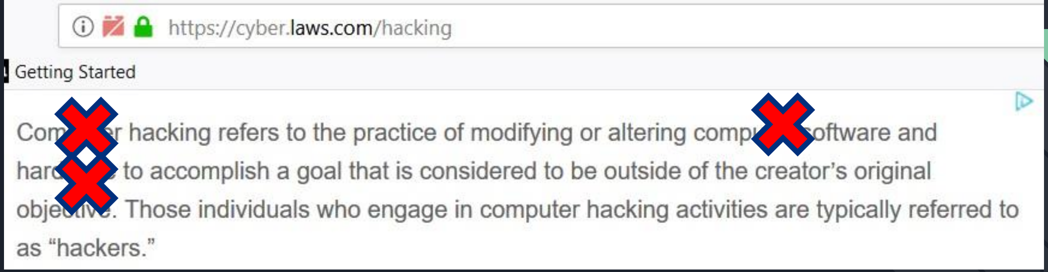
Dictionar

Sear

nc

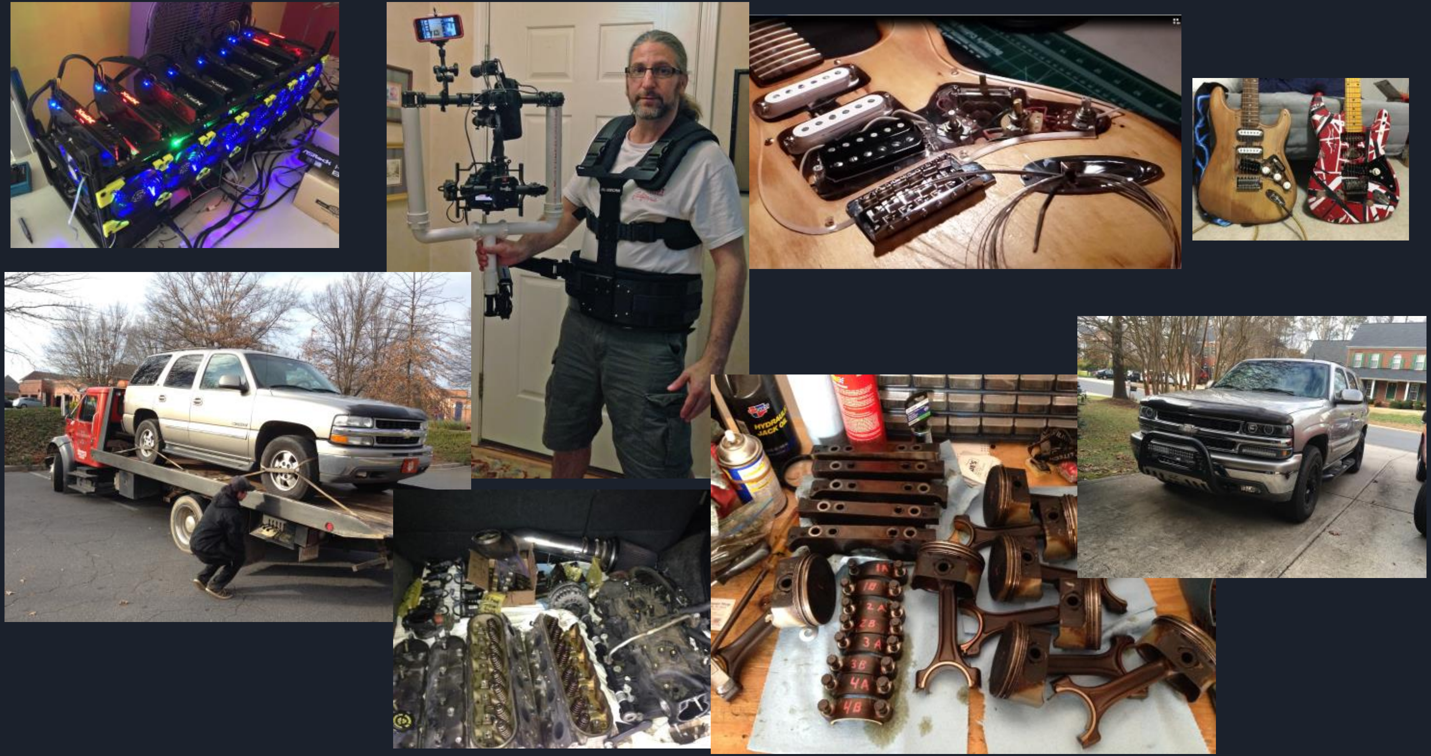
th ing of unauthorized access to data in a system o puter.
"outlawing hacking has not stopped it"

What is Hacking?

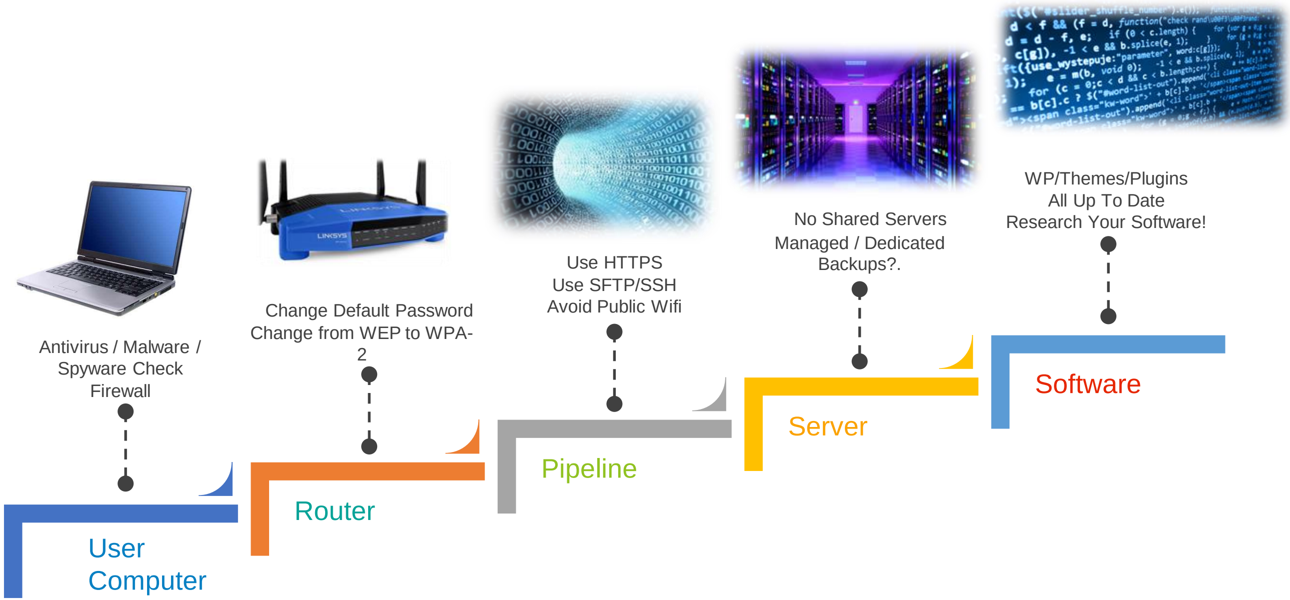


Com r hacking refers to the practice of modifying or altering comp oftware and har e to accomplish a goal that is considered to be outside of the creator's original obje ve. Those individuals who engage in computer hacking activities are typically referred to as "hackers."

It's Not Necessarily a Bad Thing


1A
1B
2A
2B
3A
3B
4A
4B

Educate Your Clients On Security From Their Fingertips to the Server



Antivirus / Malware / Spyware Check Firewall

User Computer

Change Default Password Change from WEP to WPA-2

Router

Use HTTPS
Use SFTP/SSH
Avoid Public Wifi

Pipeline

No Shared Servers
Managed / Dedicated
Backups?.

Server

WP/Themes/Plugins
All Up To Date
Research Your Software!

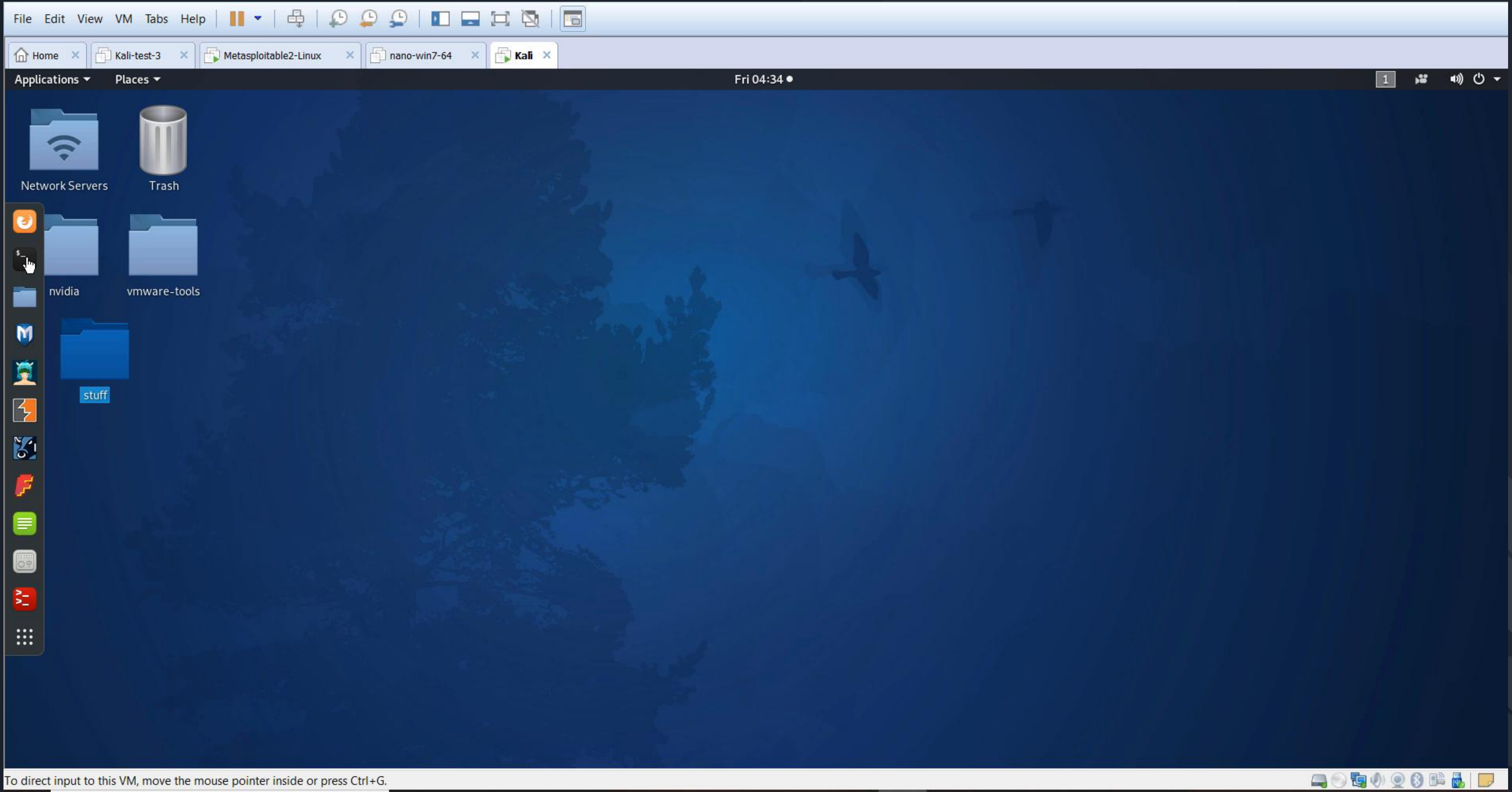
Software

PSA

Router

LINKSYS
LINKSYS
WRT 1900 AC
INTERNET
2.4 GHz
5 GHz
eSATA
USB 1
USB 2

Alfa AWUS036NH

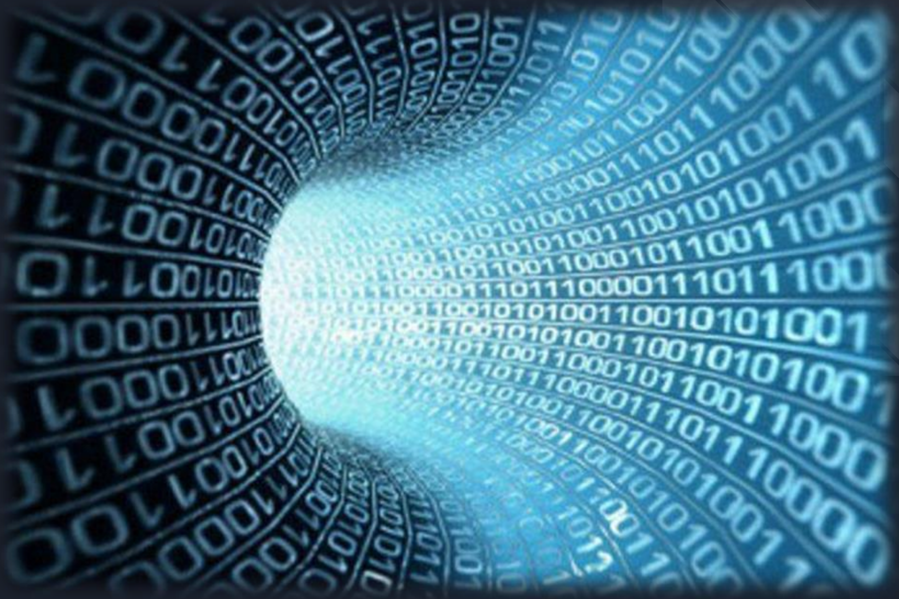


To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Simple Fix :

- **Lock IT Down**

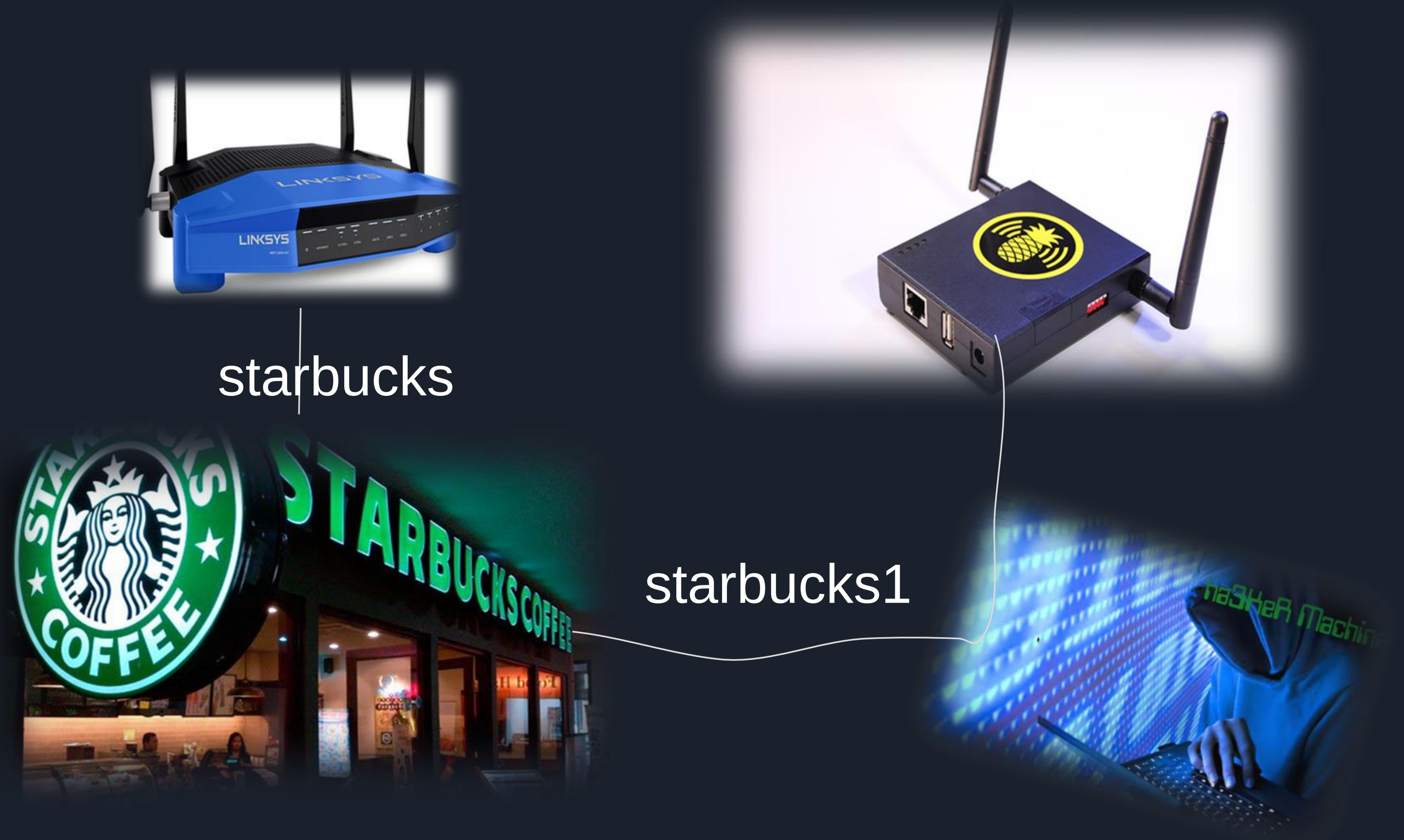
Pipeline



Meet Mary

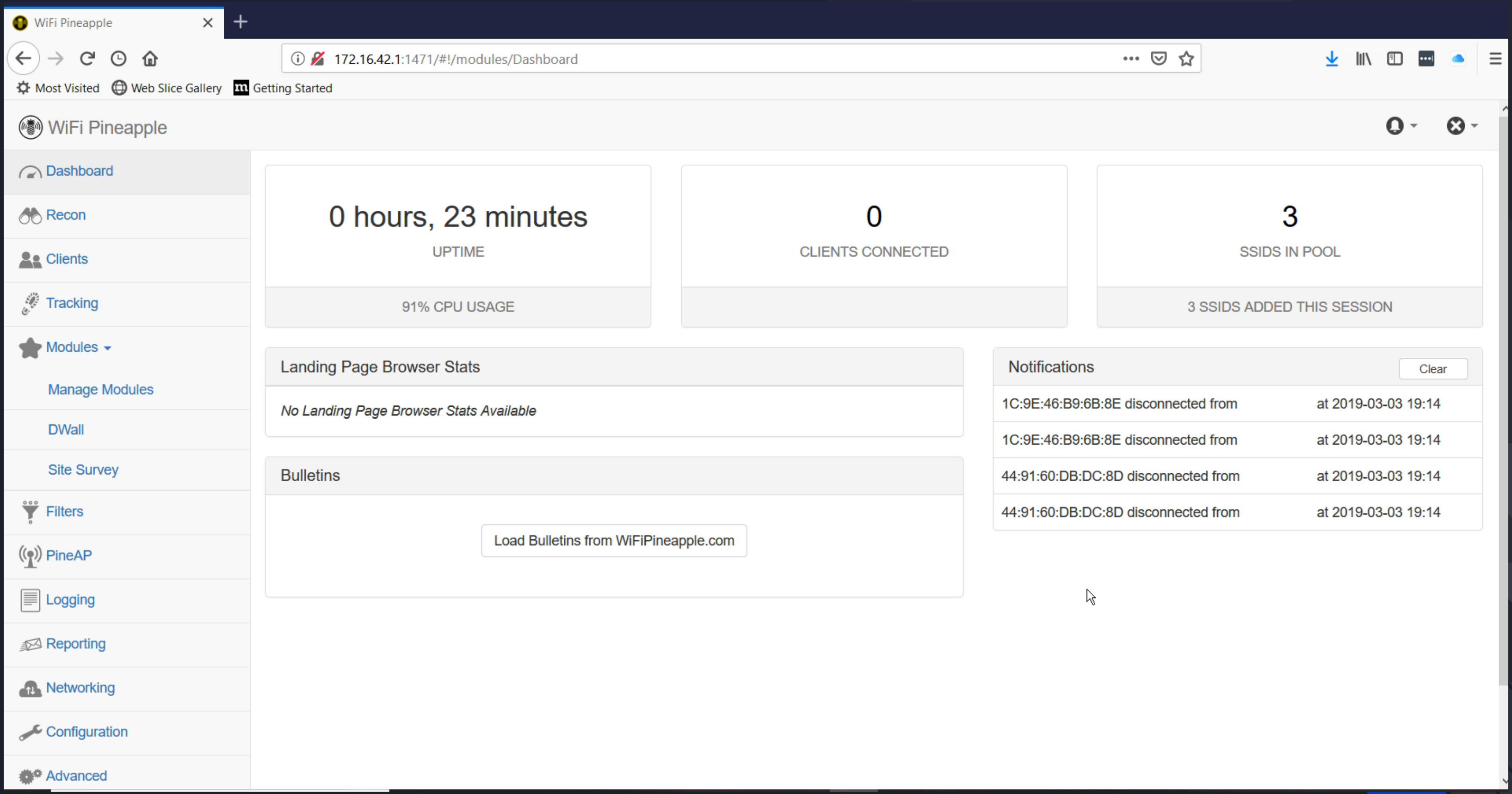
Social
Local
WORDS
B2B
MARKETING
Viral
BRAND
Creative
Mobile
Blogs
Global
Direct
People
SEO
Guerilla
Internet

BLOG



starbucks

starbucks1



0 hours, 23 minutes
UPTIME
91% CPU USAGE

0
CLIENTS CONNECTED

3
SSIDS IN POOL
3 SSIDS ADDED THIS SESSION

Landing Page Browser Stats

No Landing Page Browser Stats Available

Bulletins

Notifications

```
1C:9E:46:B9:6B:8E disconnected from      at 2019-03-03 19:14
1C:9E:46:B9:6B:8E disconnected from      at 2019-03-03 19:14
44:91:60:DB:DC:8D disconnected from      at 2019-03-03 19:14
44:91:60:DB:DC:8D disconnected from      at 2019-03-03 19:14
```

Simple Fix : Make Site SSL = HTTPS!

Force SSL (when possible) -

Just add the following options to your wp-config.php file:

```
define(‘FORCE_SSL_LOGIN’, true);

define(‘FORCE_SSL_ADMIN’, true);
```

Simple Fix : Make Site SSL = HTTPS!

- Use a VPN

Social Engineering

* Hacking the People – Not the Tech

Phishing Emails

Email - Click on the wrong attachment and it’s game over

Phone Calls

Tricked into giving away info, going to a site, taking some action / IRS & Tech Support Scams

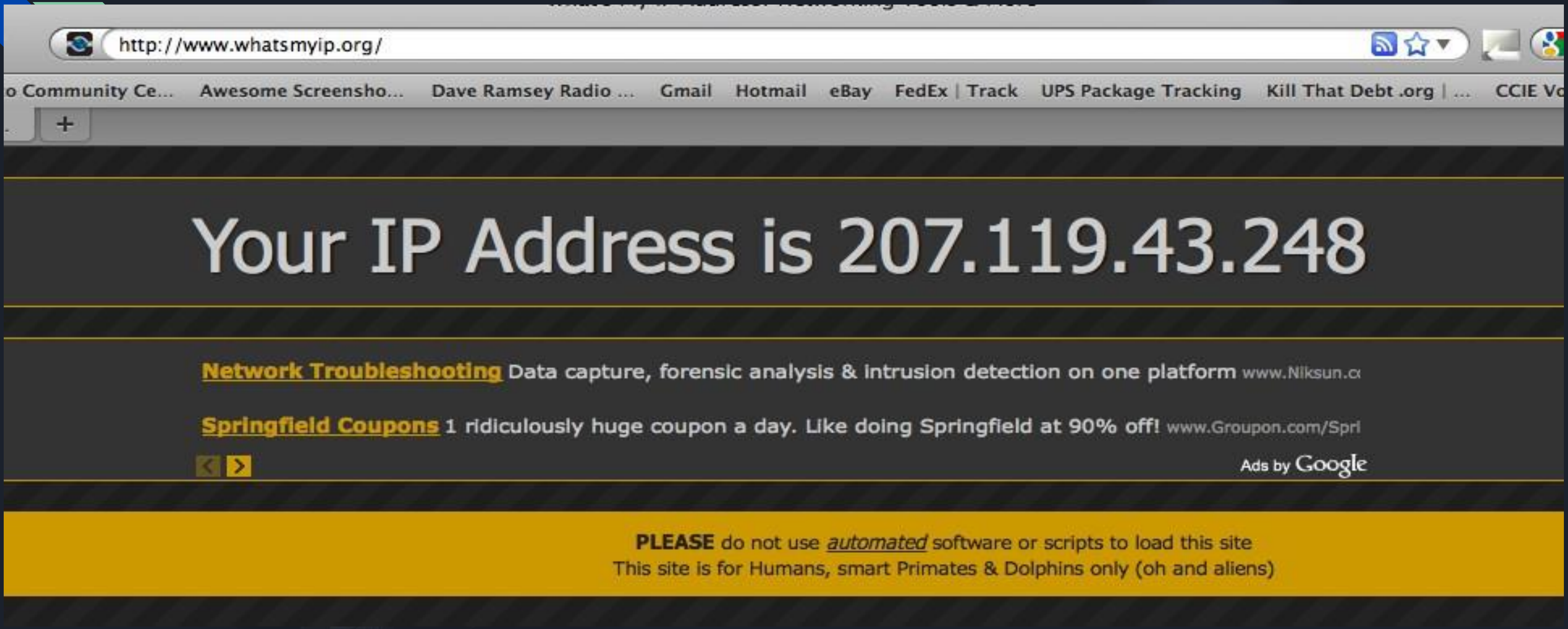
In Person

Hacker pretends to be someone he is not

Other

USB / Freeware offers / Free Games /

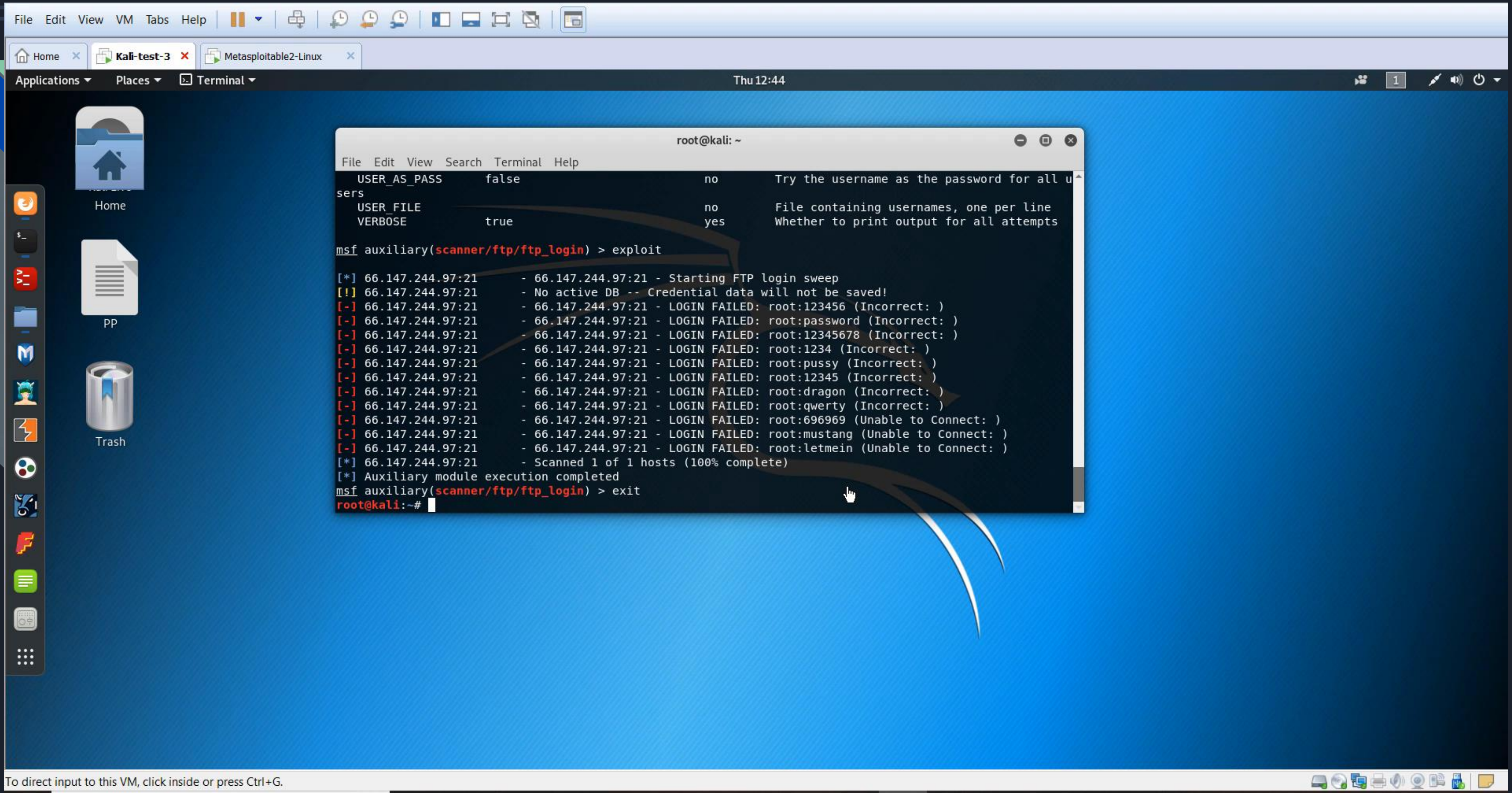
Your Laptop / Desktop



http://www.whatsmyip.org/

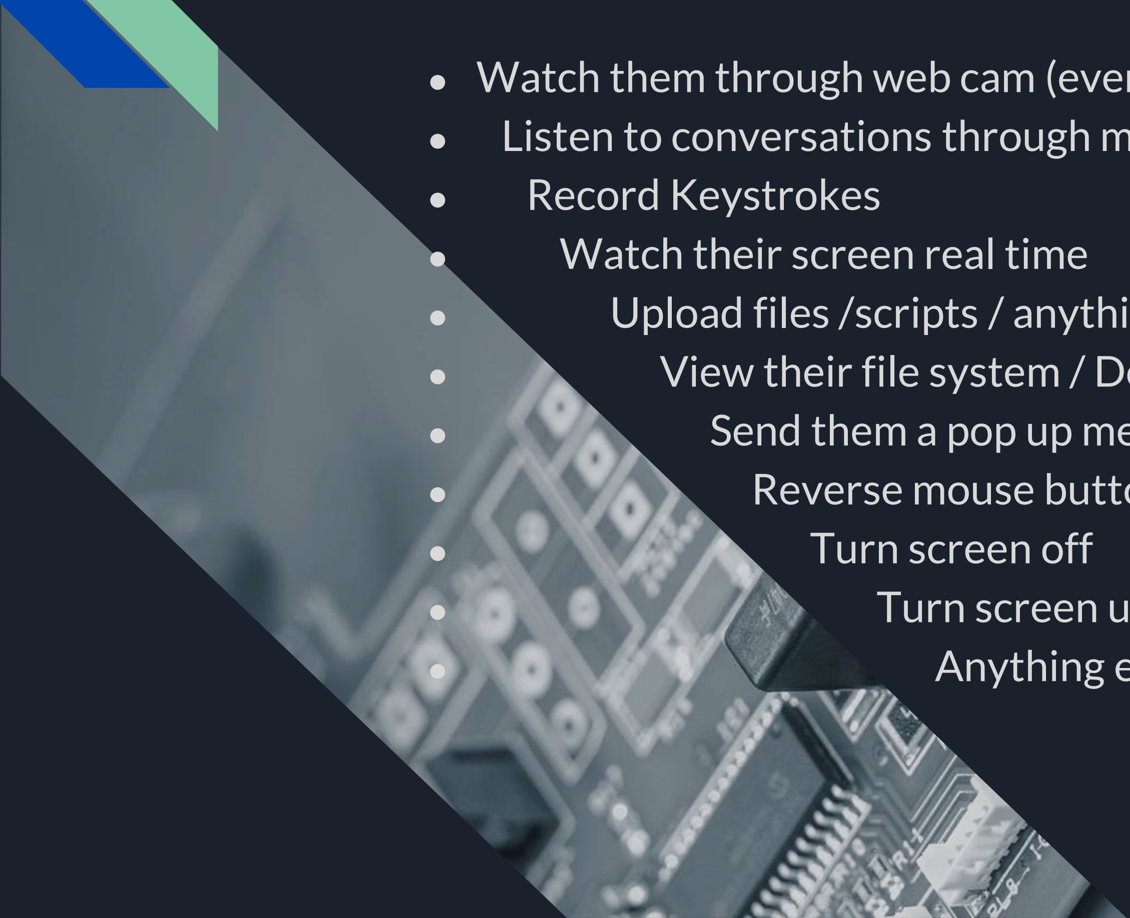
Your IP Address is 207.119.43.248

PLEASE do not use *automated* software or scripts to load this site
This site is for Humans, smart Primates & Dolphins only (oh and aliens)

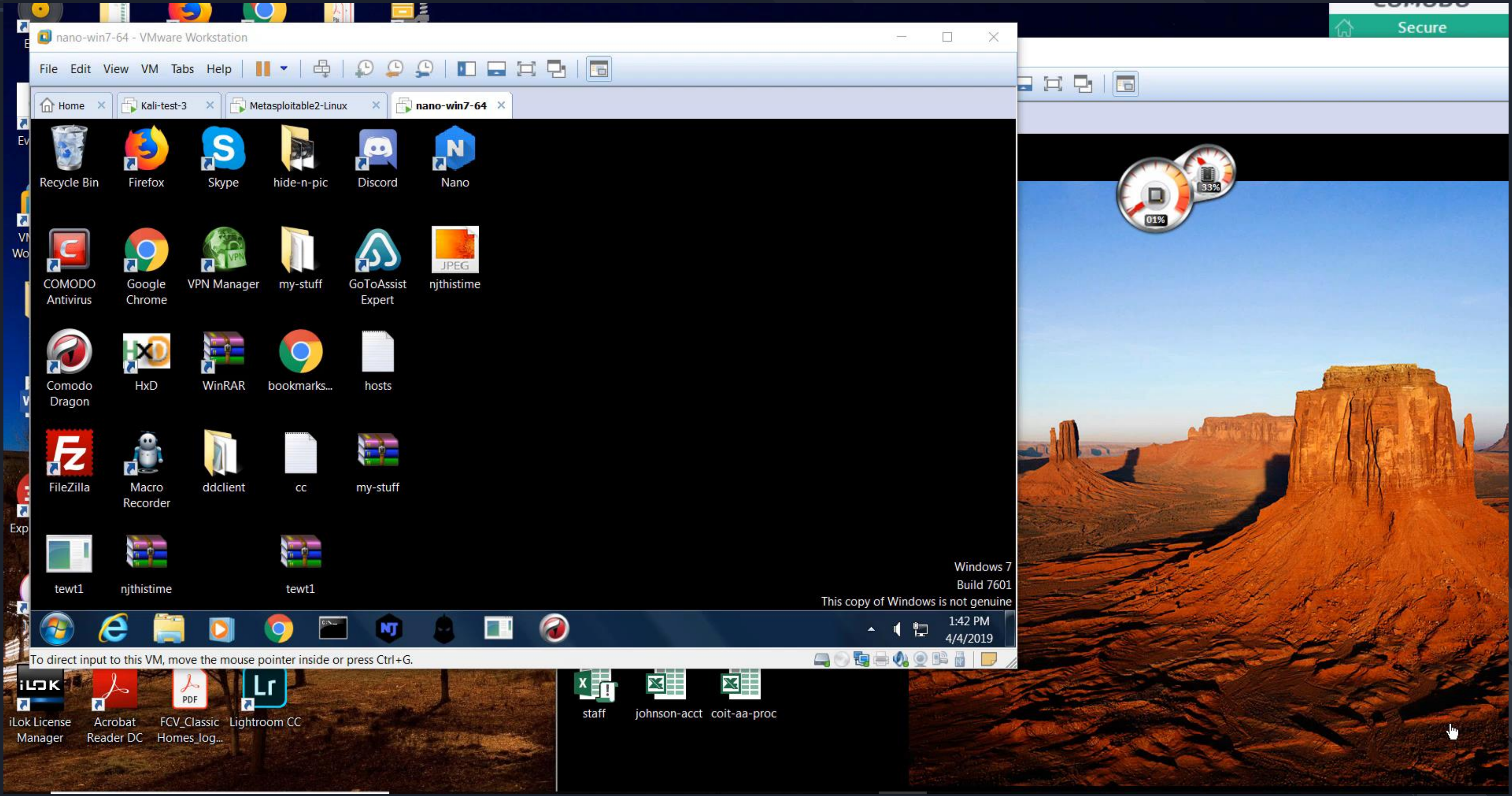


```
   USER_AS_PASS      false                          no        Try the username as the password for all u
sers
   USER_FILE                                        no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts

msf auxiliary(scanner/ftp/ftp_login) > exploit

[*] 66.147.244.97:21      - 66.147.244.97:21 - Starting FTP login sweep
[!] 66.147.244.97:21      - No active DB -- Credential data will not be saved!
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:123456 (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:password (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:12345678 (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:1234 (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:pussy (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:12345 (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:dragon (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:qwerty (Incorrect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:696969 (Unable to Connect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:mustang (Unable to Connect: )
[-] 66.147.244.97:21      - 66.147.244.97:21 - LOGIN FAILED: root:letmein (Unable to Connect: )
[*] 66.147.244.97:21      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/ftp_login) > exit
root@kali:~# 
```

What we can do next…..

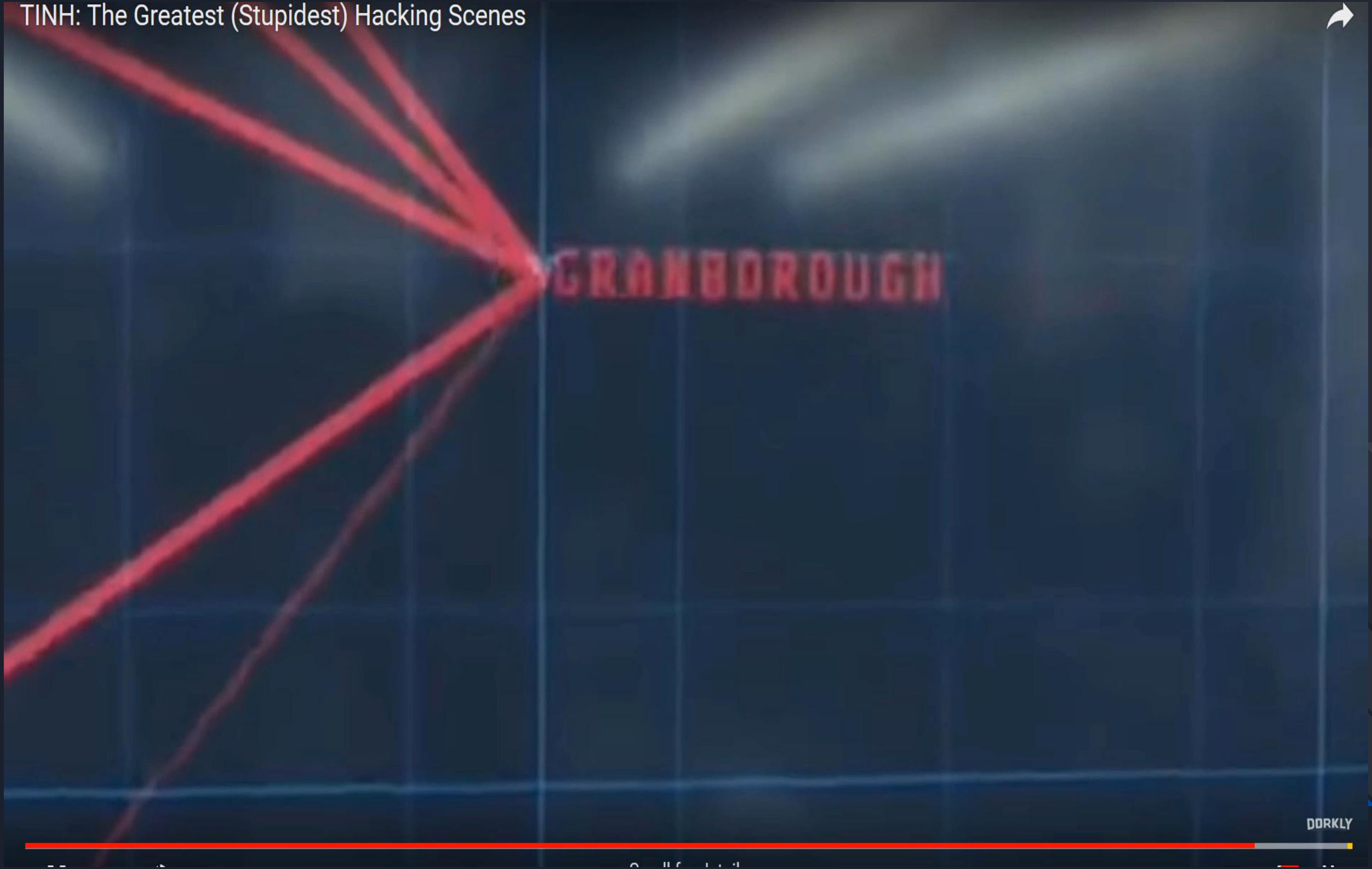


- Watch them through web cam (even turn the light off)
- Listen to conversations through microphone
- Record Keystrokes
- Watch their screen real time
- Upload files /scripts / anything
- View their file system / Download Everything
- Send them a pop up message on their screen (Demand Ransom)
- Reverse mouse buttons
- Turn screen off
- Turn screen upside down
- Anything else you can imagine



Windows 7
Build 7601
This copy of Windows is not genuine

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

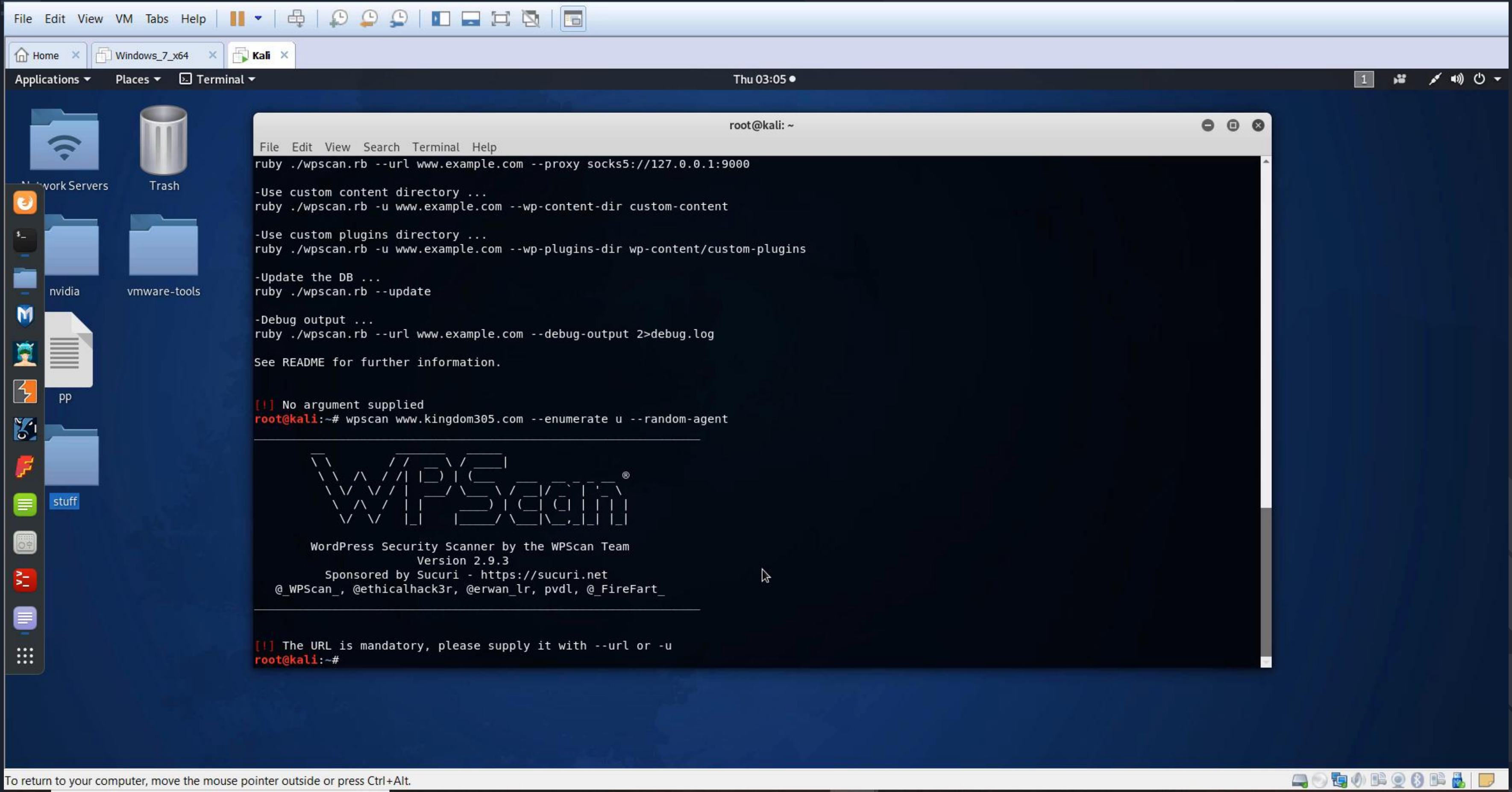


TINH: The Greatest (Stupidest) Hacking Scenes

Server

Server Software

Application



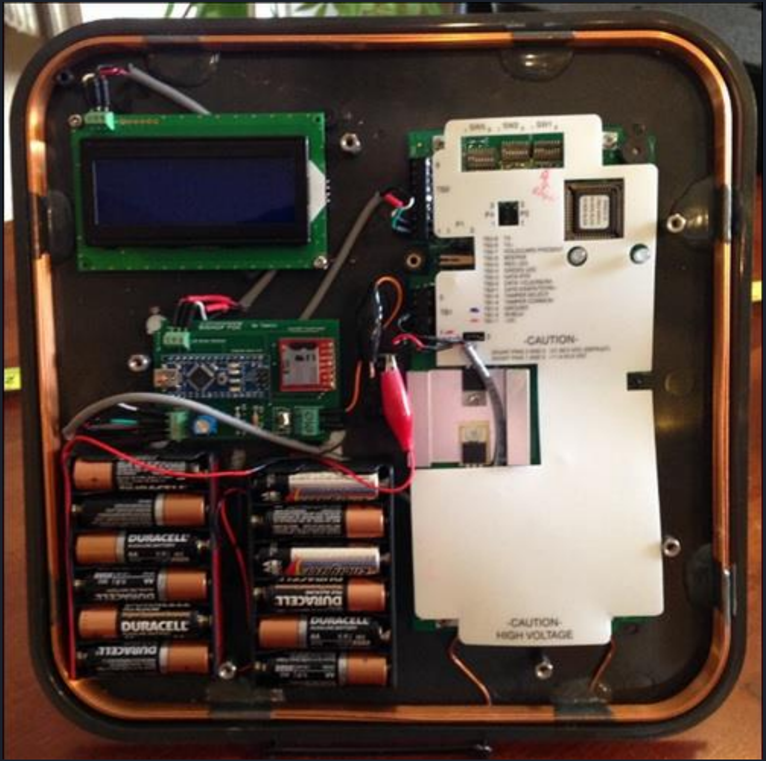
File Edit View VM Tabs Help
Home
Windows_7_x64
Kali
Applications
Places
Terminal
Thu 03:05
Network Servers
Trash
nvidia
vmware-tools
pp
stuff
root@kali: ~
File Edit View Search Terminal Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
ruby ./wpscan.rb --url www.example.com --proxy socks5://127.0.0.1:9000

-Use custom content directory ...
ruby ./wpscan.rb -u www.example.com --wp-content-dir custom-content

-Use custom plugins directory ...
ruby ./wpscan.rb -u www.example.com --wp-plugins-dir wp-content/custom-plugins

-Update the DB ...
ruby ./wpscan.rb --update

-Debug output ...
ruby ./wpscan.rb --url www.example.com --debug-output 2>debug.log

See README for further information.


[!] No argument supplied
root@kali:~# wpscan www.kingdom305.com --enumerate u --random-agent
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________


[!] The URL is mandatory, please supply it with --url or -u
root@kali:~#
```

Physical Security

TYPE : M1 S50
FREQ : 13.56M
TYPE : HID
FREQ : 125K
Proxmark3 Easy
ELECHOUSE
LF_ANT 500uH±1%
Portable ANT V2.0
Center Freq:125K
ELECHOUSE

HSY
$


-CAUTION-
-CAUTION-
HIGH VOLTAGE
DURACELL

00110011010100

How An Attacker Sees Your Website
A View Through The Eye of the Hacker

Want A Free Scan?

CyberSafetyGuy.com

Steve Schwartz

AVT Marketing

Steve@AVTmarketing.com

704-288-5705