

Mapping and Analyzing exposed devices

By Brutal Panda

TOC

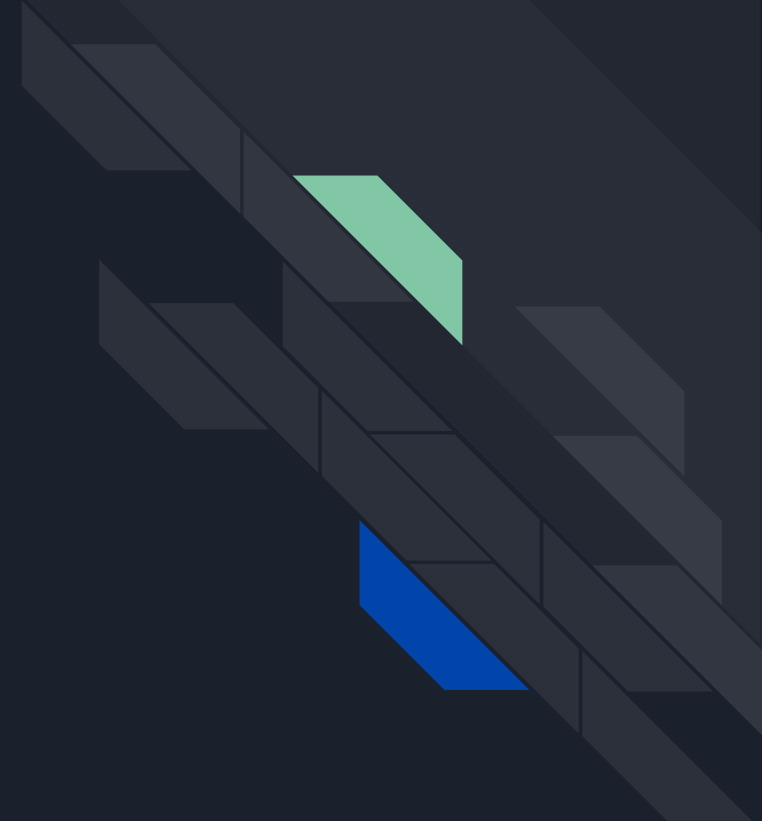
Introduction awareness and
why
What is out there

Methodology

Technologies and their pro

Vulnerabilities

History and Advancement





Intro

As Security Researchers we are curious about everything happening around us starting from devices we use daily to new technology booming around us any tech gadget that .

Why?

Mapping and analyzing exposed devices is a critical part of cybersecurity research because it allows researchers to identify and understand the attack surface of the internet. This information can be used to develop new security controls and techniques, and to prioritize remediation efforts.

(OSINT , Malware , Threat Intel & Hunt)

Methodology

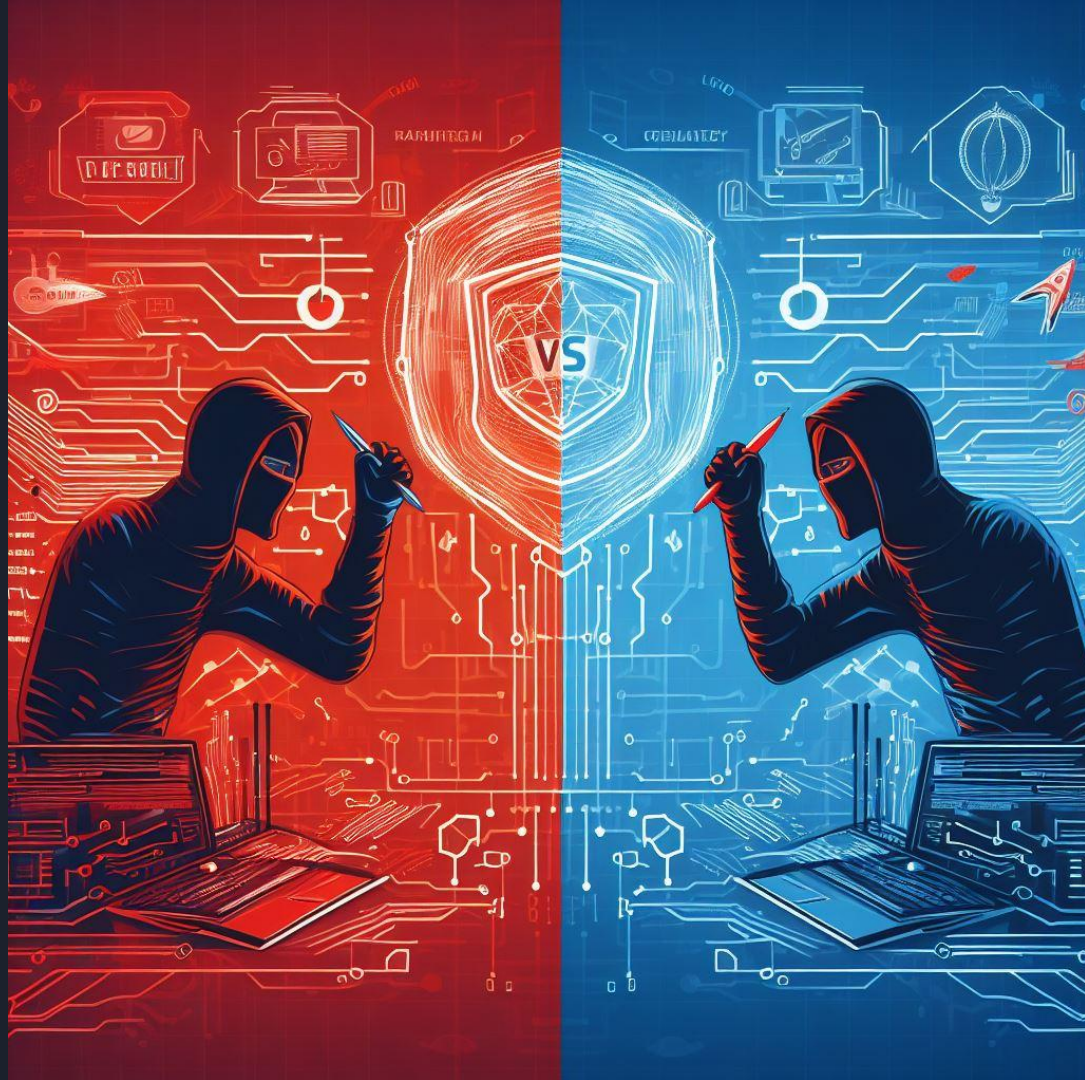
Internet Based (TCP/IP)


- Shodan io
- Censys.com
- FOFA.info

Other devices

- Wigle





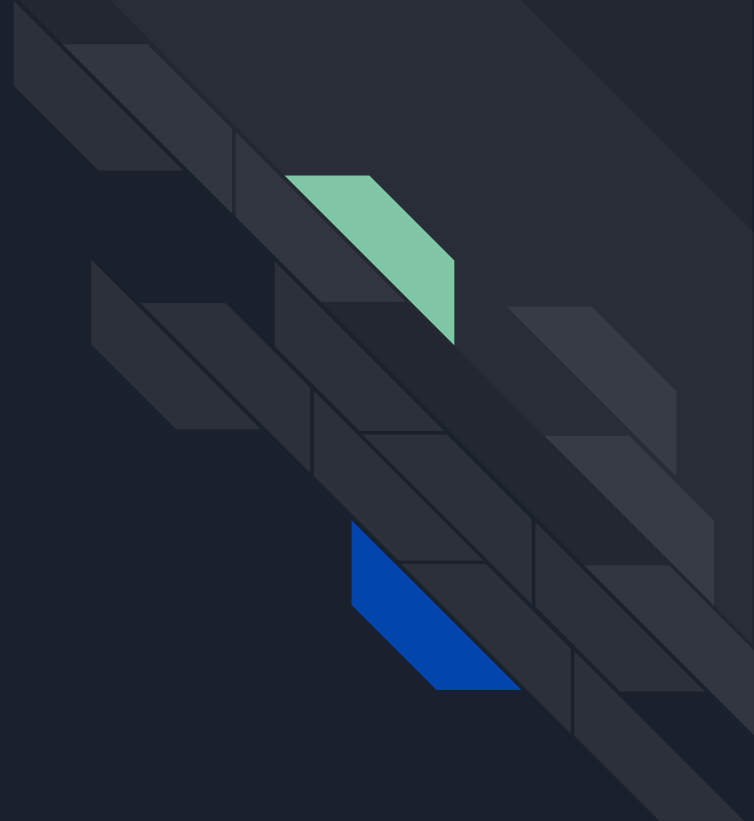
- 
- Shodan
 - Censys

Red Team

- Searching domain names
- Searching vulnerability
- OSINT

Malicious Actors

- Cyber Attack Campaigns
- C2 servers hosting



As a red teamer, you can passively scan for open ports and vulnerabilities on a target host and its subdomains without interacting with the host itself.

Tagscloudself-signed

General Information

Cloud Provider

Country

City

Organization

ISP

ASN

Web Technologies

JavaScript LibrariesjQuery3.5.1

UI FrameworksBootstrap4.5.0

Open Ports

225380443208350058443

22 / TCP

SSH 2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.8

SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.8
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQgBwBvaStzQuXSwJpDPv5Iw+Av7eZ7evmwmKpLihjPcc
Fgc32KAP71h0+455+u0E37w+HQLGCSHv/Lf6uax/cHIZVFHmu4yL/5raF5g3d0ZVox3063
H8uY8v+15cz2LmVWmcqQ3Ll04t8y11Q/L/2xYFGe05Zr3elE93Cuk0W2yM4gmpk01
ruwV6306dgATalkon8TqHtq1WwXEE1H06ZyFQ71a/OuWv73ycK53wVed0p0n09H1e2ge
ep3JYDvtyg0Mde65ShgK2uL/XPLf62y3atFOPQK/G0Xpnt11Iw4V9uchvny2658Ww28c4I
K4L7U/gY8WqQ1x37q7988htwUa261EX4Jy8k3H0MGv18FwethX331p4h/EYR7F6vz4
76K3Thw4258ypj3+e3E8uZhvnduqld8w15gtdsp108W0871BwJVKd3g30m+quil9-rDv95n
YoZ90685ec
Fingerprint: 2a:08:47:28:95:64:0d:10:4e:00:bb:3f:a9:53:4e:00
Key Algorithme:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-25690

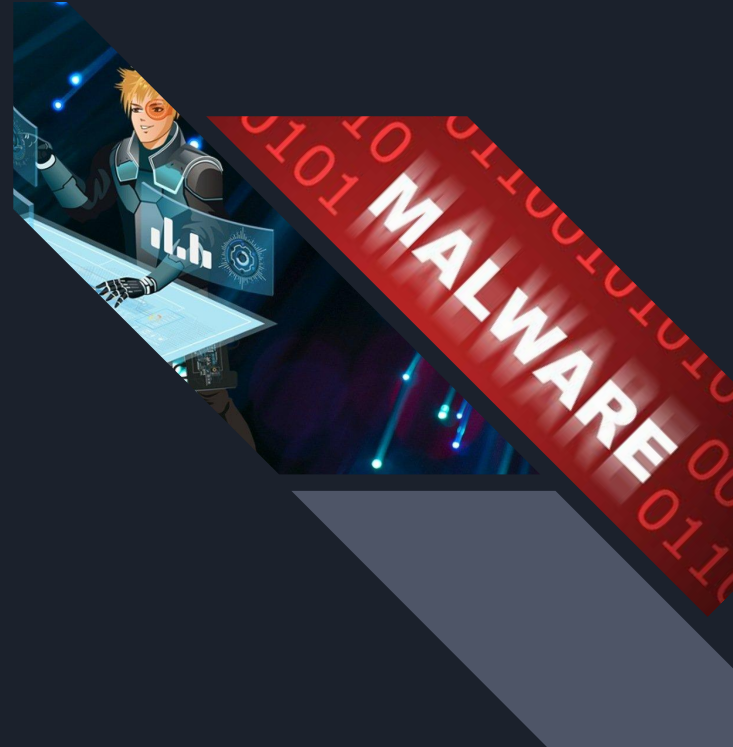
Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/L/" "http://example.com:8080/elsewhere?\${1}; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

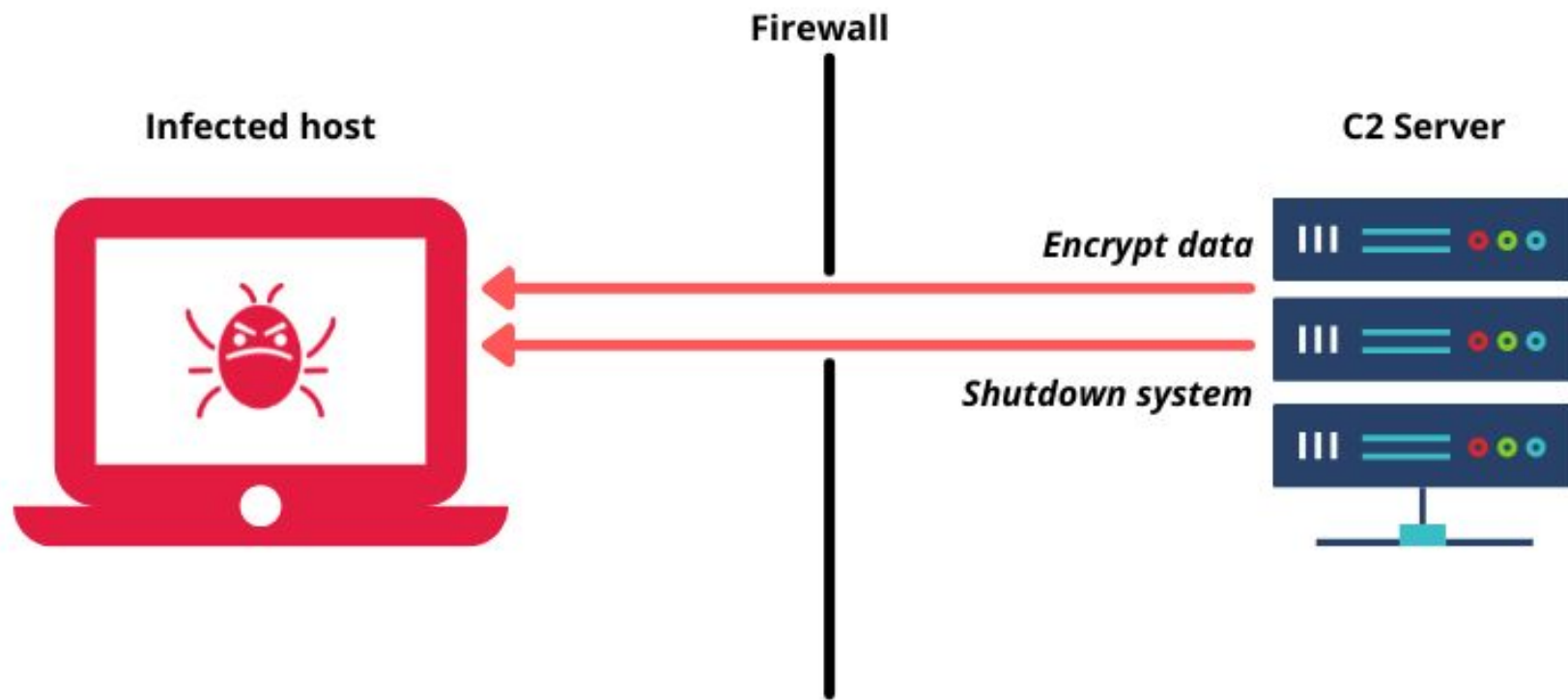
CVE-2022-37436

Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

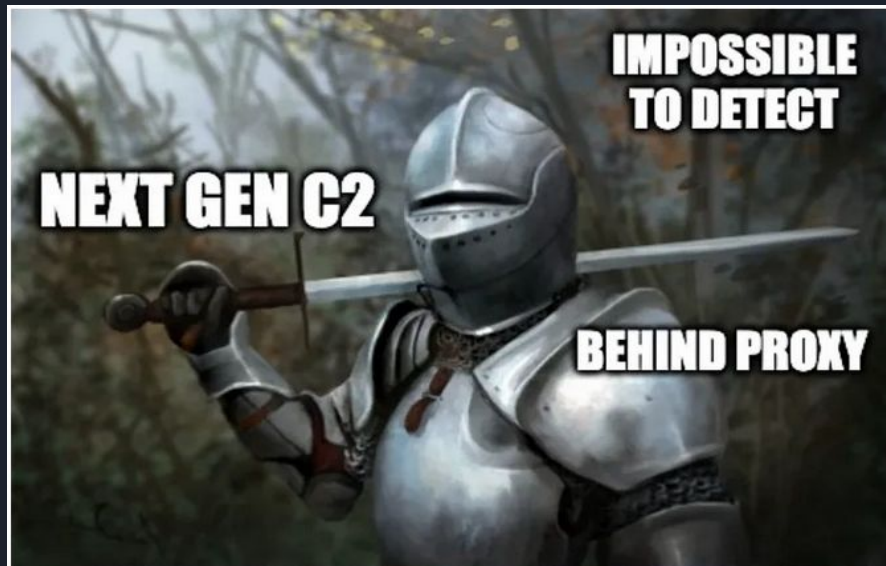
Hunting C2 servers

C2 is a command-and-control server that allows malware to communicate and receive commands. We can use tools like Shodan to hunt down malware.








- 
- Threat Hunting
 - Threat Intel
 - Hunting APT (Advanced Threat groups)



We can use shodan to hunt C2 servers such as cobalt strike framework through different mechanisms we can see one method as following for more u can read [this](#). You can see how powerful shodan can used for threat hunting process.

 SHODAN

ExploreDownloadsPricing 


ssl.cert.serial:146473198

Account

TOTAL RESULTS

319


TOP COUNTRIES





China	182
Hong Kong	33
United States	31
Russian Federation	12
Netherlands	11
More...	


TOP PORTS

443	227
8443	39
4433	14
...	...


 View Report


 Download Results

 Historical Trend


 View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

216.238.116.187 

216-238-116-187.constant.com
The Constant Company, LLC
 Brazil, Osasco


cloudself-signed


 SSL Certificate

Issued By:
|- Common Name:
|- Organization:
Issued To:
|- Common Name:
|- Organization:
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2


HTTP/1.1 404 Not Found
Date: Mon, 13 Nov 2023 18:27:03 GMT
Server: Apache-Coyote/1.1
Content-Type: text/plain
Cache-Control: max-age=2
X-Content-Type-Options: nosniff
X-Powered-By: Brightspot
Vary: Accept-Encoding
Connection: close
Content-Length: 0

2023-11-13T18:27:01.391145

101.33.231.180 

Tencent Cloud Computing
(Beijing) Co., Ltd
 China, Shenzhen

cloudself-signed

 SSL Certificate

Issued By:
|- Common Name:
|- Organization:
Issued To:
|- Common Name:
|- Organization:
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 404 Not Found
Date: Mon, 13 Nov 2023 17:59:07 GMT
Content-Type: text/plain
Content-Length: 0
Cobalt Strike Beacon:
x86:
beacon_type: HTTPS
beacon_strategy: full_payload -1

2023-11-13T17:59:08.617549



Wigle

- Android
- Bluetooth
- Cars (BUS)
- War driving

An attacker can use Wigle to impersonate a Wi-Fi network in order to trick a user into connecting to it and launching an evil twin attack or similar attacks.

WIGLE.NET™

All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES	CELL T...
477,956	1,179,327,619	16,152,945,661	264,313	2,000,573,549	21,74

RF Hacker Sanctuary DEF CON 31 World Wide Wardrive

Thu, 13 Jul 2023 21:48:04 GMT

registration for the WWWDD is open - see <https://wigle.net/contest/DC31> if you're already a user.

[read more...](#)

-arkasha

Billion Mapped WiFi Networks

Sun, 19 Feb 2023 15:18:03 GMT

Congrats to user 'ymbio' who posted the *ONE BILLIONTH* geo-located WIFI network! This project continues to delight, thanks to all the users!

-bobzilla

Thanks a Billion!

Tue, 07 Feb 2023 21:27:26 GMT

Last week, WIGLE reached 1 billion WiFi Networks recorded. This is mind-boggling number, and we couldn't have done it without the community - in particular, Lucifenko, who submitted the 1-billionth network.

[read more...](#)

-arkasha

Want to help support WigLE?

You can [allow WigLE to use your data for commercial purposes](#). You can also select "[no, please don't use my data for commercial purposes](#)," and w

+

-

WIGLE.NET

WIGLE.NET

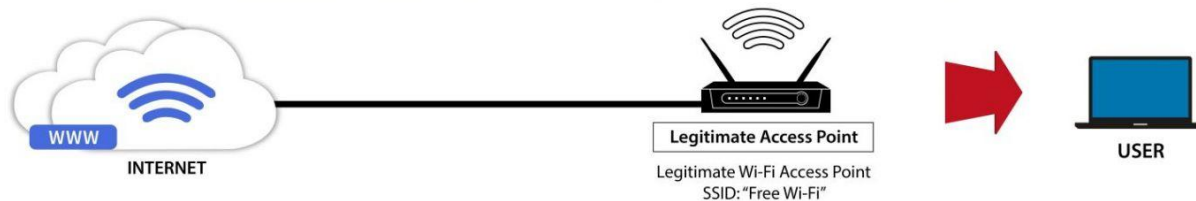
WIGLE.NET

Zoom to

Nearest Network (lat: 37.78, lon: -122.426)

SSID: OlegChevy
BSSID: BC:82:5D:57:2E:88
First Time: 2019-04-09T12:00:00.000Z
Last Time: 2019-04-09T15:00:00.000Z
Channel: 1
Encryption: wpa2
Quality of Signal: 0
Address: 967;971;973 Golden Gate Avenue, San Francisco, CA, US, 94102

Typical Wi-Fi Connection:



What Happens in an Evil Twin Attack:

