Intro To Cyber | Project 1: Net Crafts

Muhammad Termidzi Bin Azmi (S27)

CFC190324

Samson Xiao

31 March 2024

Table of contents

Introduction

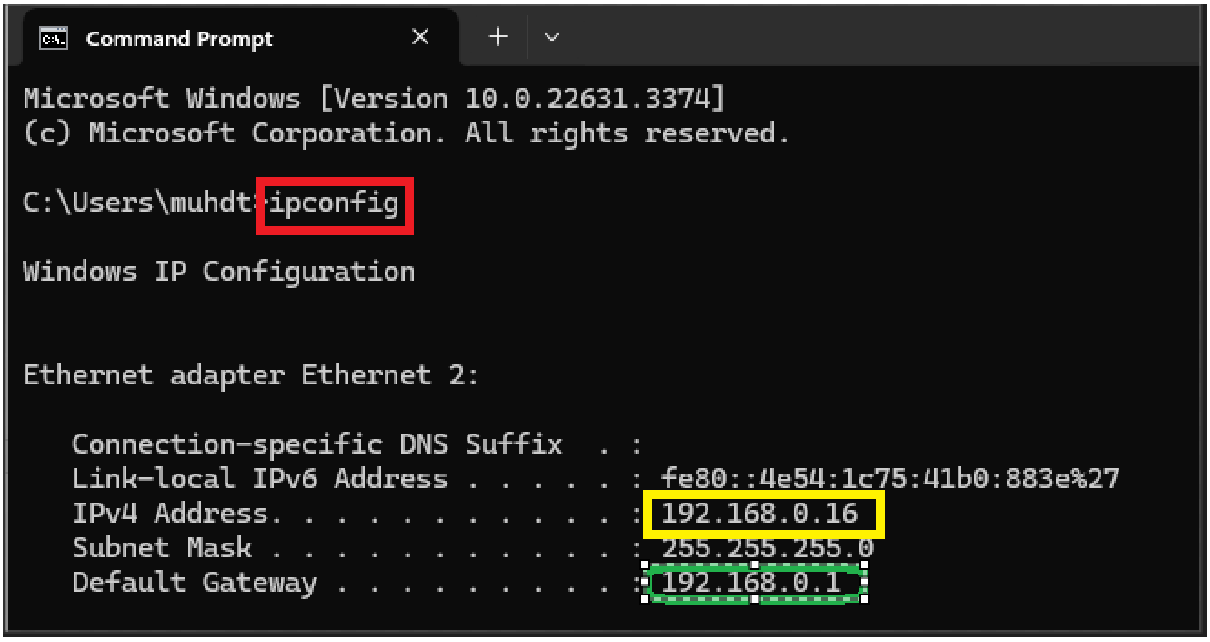
Operation Net Crafts is a two-phased reconnaissance mission. Phase 1, "Network Mapping," commands a detailed survey of the internal network terrain, identifying all devices, their communication protocols, and strategic infrastructure points. Phase 2, "External Intel Gathering," deploys digital surveillance via Shodan and WHOIS, examining the network's public presence and analyzing traffic for operational security. Execute with precision to secure a comprehensive battlefield overview.

This report aims to create a detailed analysis of the home network to gain insights into the components and network architecture. It also documents the procedures, tools utilized and the outcome.

Execution & Methodologies

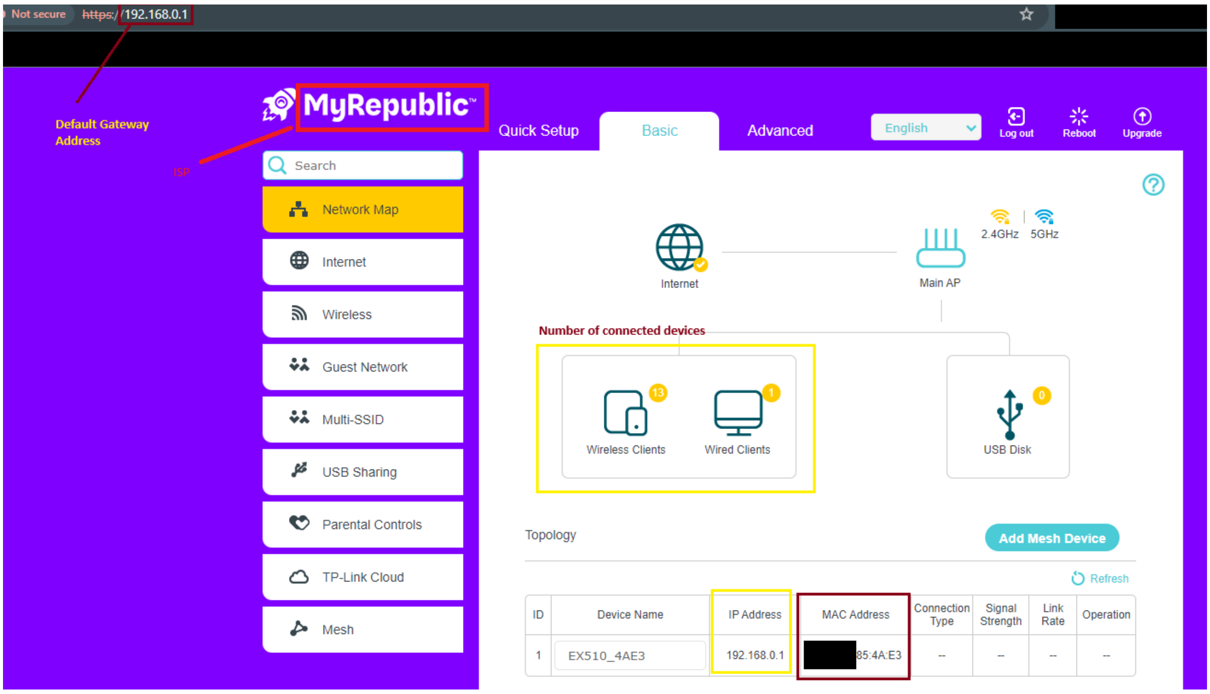
Phase 1: Network Mapping

1. Using Command Prompt
   - Type in “ipconfig” into the command prompt to see the routers internal IP Address (Default Gateway) and the local machine IP address (Ipv4 Address).



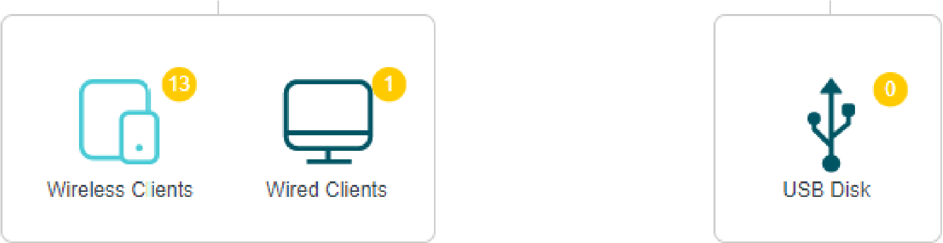
```
Microsoft Windows [Version 10.0.22631.3374]
(c) Microsoft Corporation. All rights reserved.

C:\Users\muhdt>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4e54:1c75:41b0:883e%27
   IPv4 Address. . . . . . . . . . . : 192.168.0.16
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

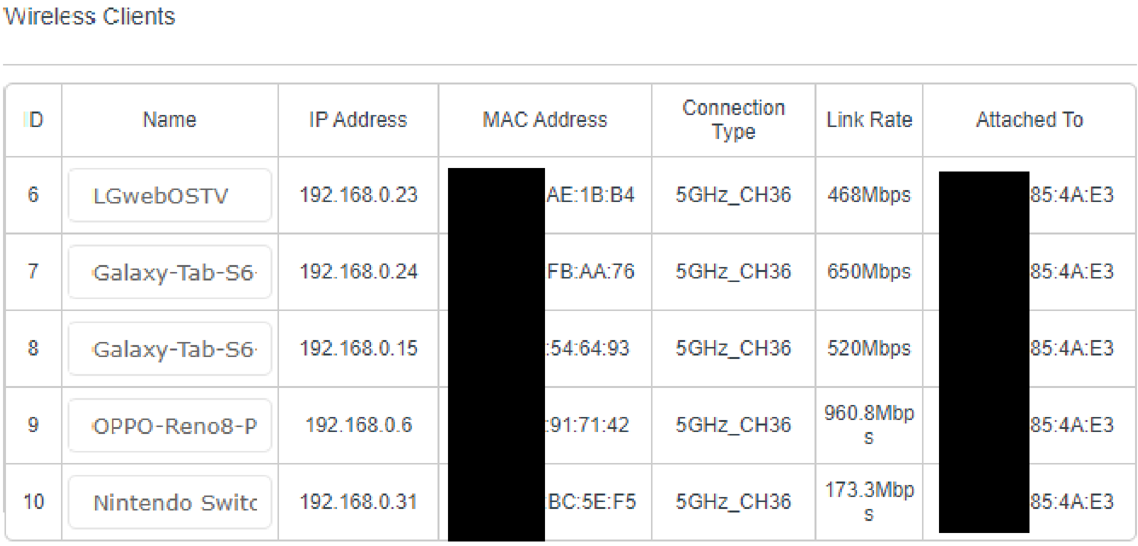
2. Login into the router
   - Type in 192.168.0.1 (Default Gateway) in a browser.
   - Here we are able to see the number of devices connected to the router with active connection
   - We are also able to identify the MAC Address



ID	Device Name	IP Address	MAC Address	Connection Type	Signal Strength	Link Rate	Operation
1	EX510_4AE3	192.168.0.1	[redacted]85:4A:E3	--	--	--	--

- Clicking on the Wireless / Wired Clients, we can identify the connected devices' IP and MAC addresses.



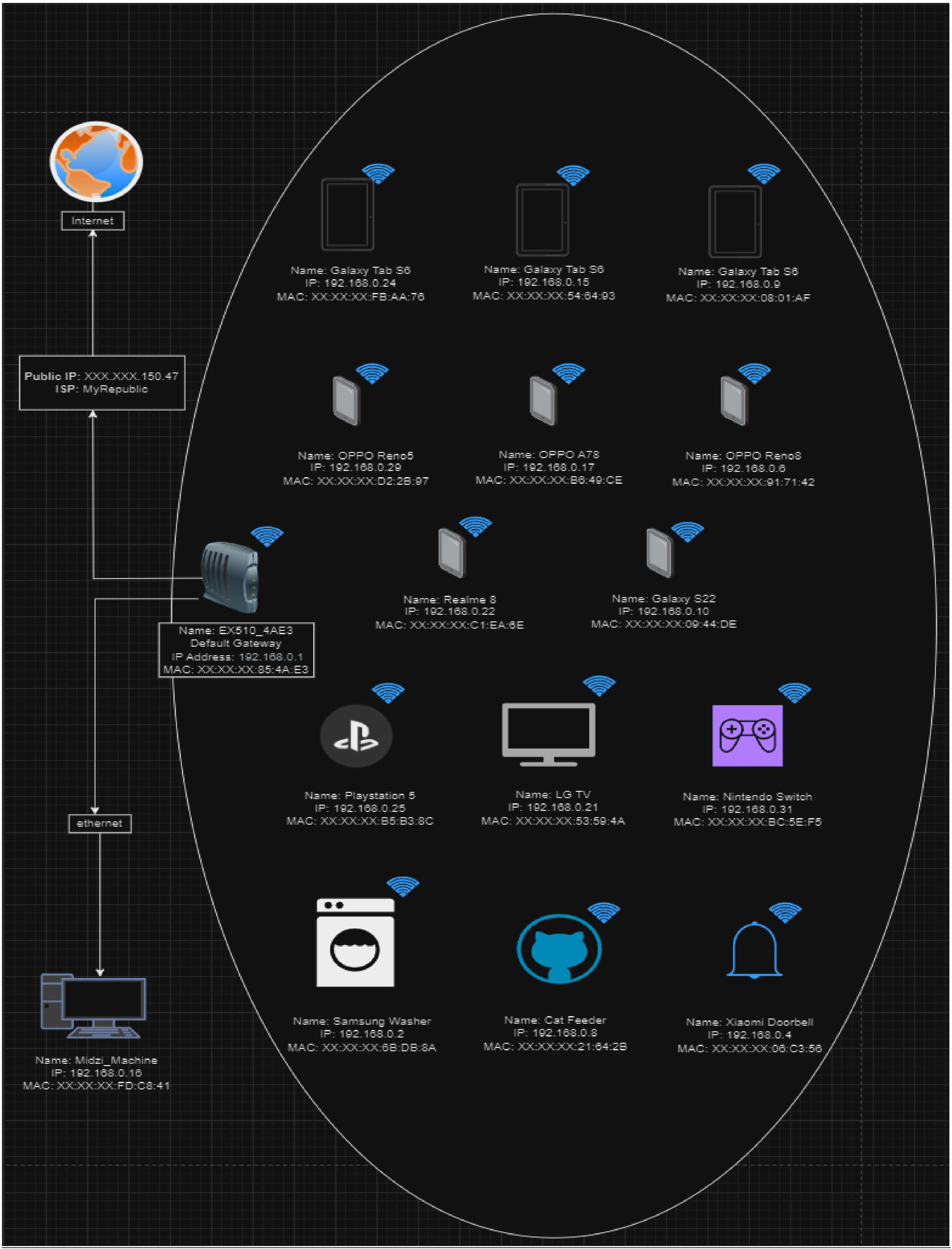


Wireless Clients

ID	Name	IP Address	MAC Address	Connection Type	Link Rate	Attached To
6	LGwebOSTV	192.168.0.23	[redacted]AE:1B:B4	5GHz_CH36	468Mbps	[redacted]85:4A:E3
7	Galaxy-Tab-S6	192.168.0.24	[redacted]FB:AA:76	5GHz_CH36	650Mbps	[redacted]85:4A:E3
8	Galaxy-Tab-S6	192.168.0.15	[redacted]:54:64:93	5GHz_CH36	520Mbps	[redacted]85:4A:E3
9	OPPO-Reno8-P	192.168.0.6	[redacted]:91:71:42	5GHz_CH36	960.8Mbps	[redacted]85:4A:E3
10	Nintendo Switc	192.168.0.31	[redacted]BC:5E:F5	5GHz_CH36	173.3Mbps	[redacted]85:4A:E3

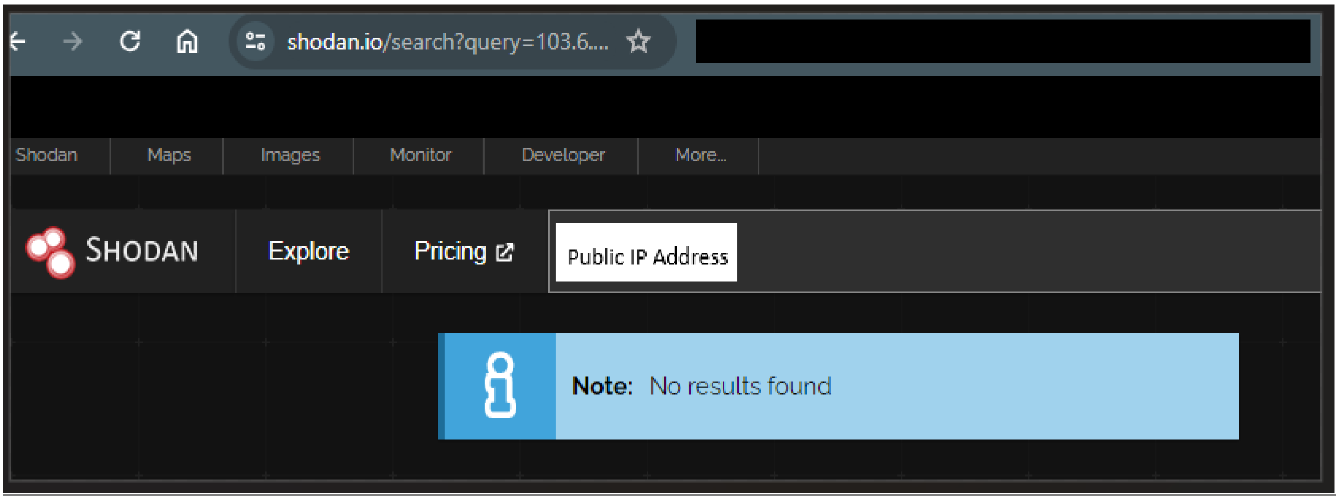
3. Use macaddress.io to determine the device that is connected to the home network.
4. Use draw.io tool to map.
5. Use whatismyapaddress.com to determine external IP address of the router.
6. Visual physical inspection: To confirm that the device that is connected to the network is the reflected one and to be familiarized with it.

Network Mapping Results:



Phase 2: External Intel Gathering

1. Run wireshark to capture packets.
2. Log in to shodon.io and enter external IP address.

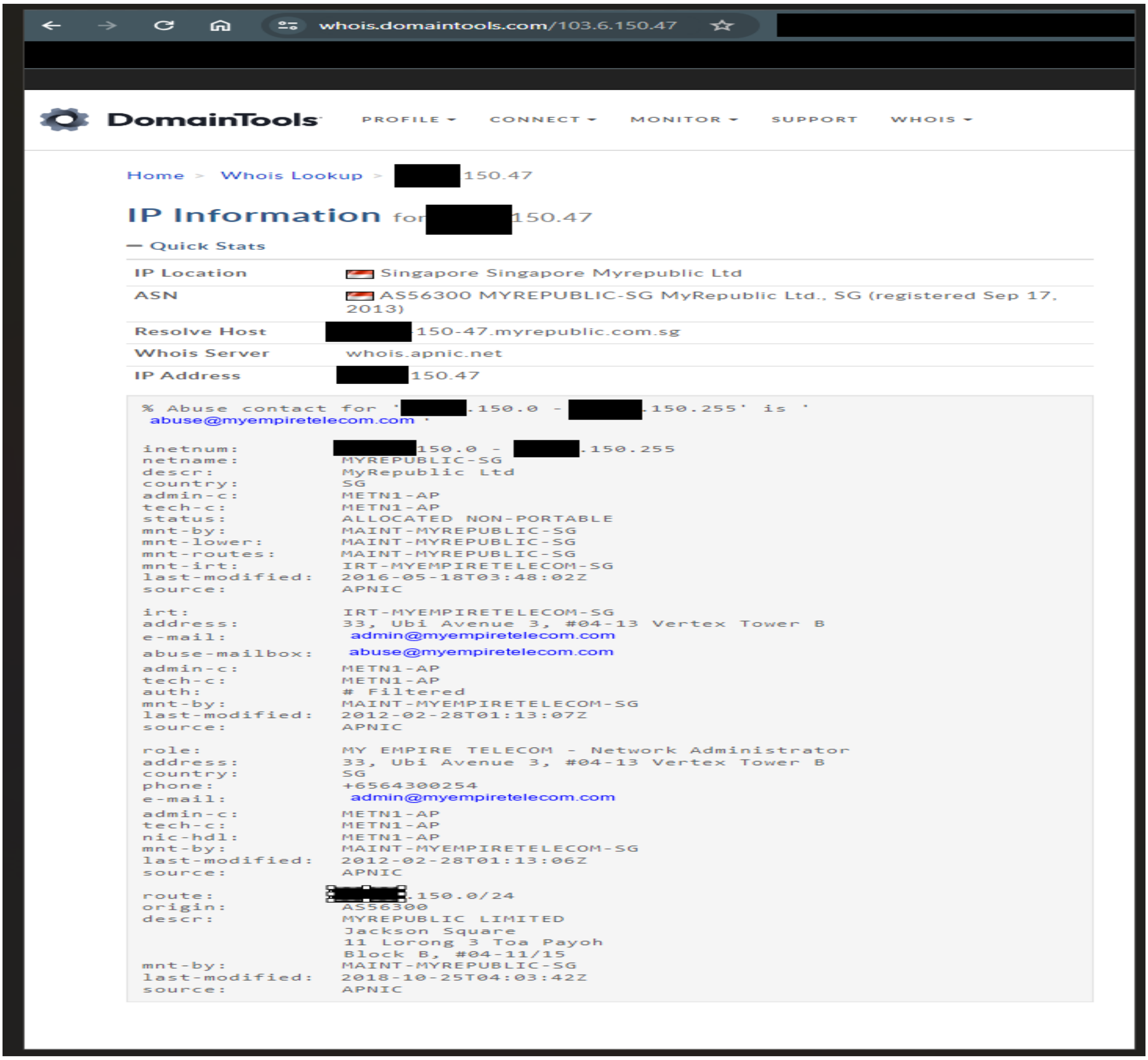


[redacted]

Public IP Address

Note: No results found

3. Log in to whois.domaintools.com and enter external IP address.



[redacted]

Home > Whois Lookup > [redacted]150.47

IP Information for [redacted]150.47

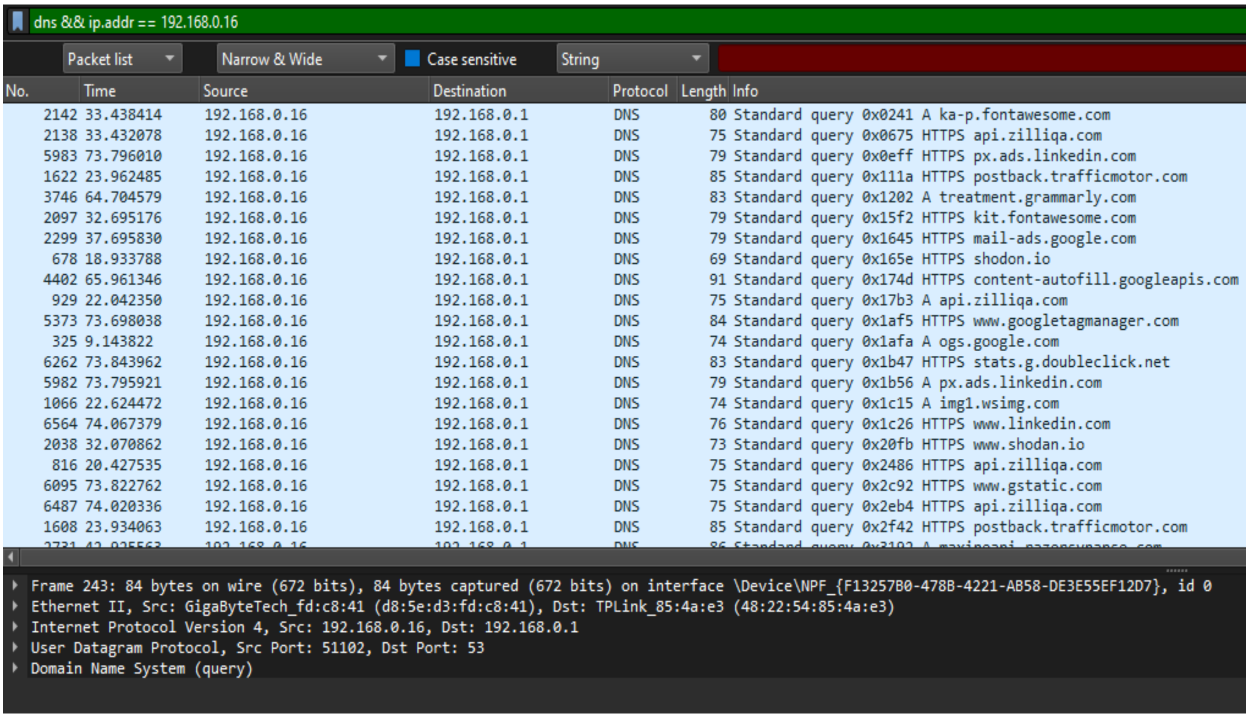
— Quick Stats

IP Location	Singapore Singapore Myrepublic Ltd
ASN	AS56300 MYREPUBLIC-SG MyRepublic Ltd., SG (registered Sep 17, 2013)
Resolve Host	[redacted]150-47.myrepublic.com.sg
Whois Server	whois.apnic.net
IP Address	[redacted]150.47

```
% Abuse contact for '[redacted].150.0 - [redacted].150.255' is '
 abuse@myempiretelecom.com '

inetnum:        [redacted]150.0 - [redacted].150.255
netname:        MYREPUBLIC-SG
descr:          MyRepublic Ltd
country:        SG
admin-c:        METN1-AP
tech-c:         METN1-AP
status:         ALLOCATED NON-PORTABLE
mnt-by:         MAINT-MYREPUBLIC-SG
mnt-lower:      MAINT-MYREPUBLIC-SG
mnt-routes:     MAINT-MYREPUBLIC-SG
mnt-irt:        IRT-MYEMPIRETELECOM-SG
last-modified:  2016-05-18T03:48:02Z
source:         APNIC

irt:            IRT-MYEMPIRETELECOM-SG
address:        33, Ubi Avenue 3, #04-13 Vertex Tower B
e-mail:          admin@myempiretelecom.com
abuse-mailbox:   abuse@myempiretelecom.com
admin-c:        METN1-AP
tech-c:         METN1-AP
auth:           # Filtered
mnt-by:         MAINT-MYEMPIRETELECOM-SG
last-modified:  2012-02-28T01:13:07Z
source:         APNIC

role:           MY EMPIRE TELECOM - Network Administrator
address:        33, Ubi Avenue 3, #04-13 Vertex Tower B
country:        SG
phone:          +6564300254
e-mail:          admin@myempiretelecom.com
admin-c:        METN1-AP
tech-c:         METN1-AP
nic-hdl:        METN1-AP
mnt-by:         MAINT-MYEMPIRETELECOM-SG
last-modified:  2012-02-28T01:13:06Z
source:         APNIC

route:          [redacted].150.0/24
origin:         AS56300
descr:          MYREPUBLIC LIMITED
                Jackson Square
                11 Lorong 3 Toa Payoh
                Block B, #04-11/15
mnt-by:         MAINT-MYREPUBLIC-SG
last-modified:  2018-10-25T04:03:42Z
source:         APNIC
```

4. Captured information via Wireshark with display search for DNS, UDP and HTTP.

DNS



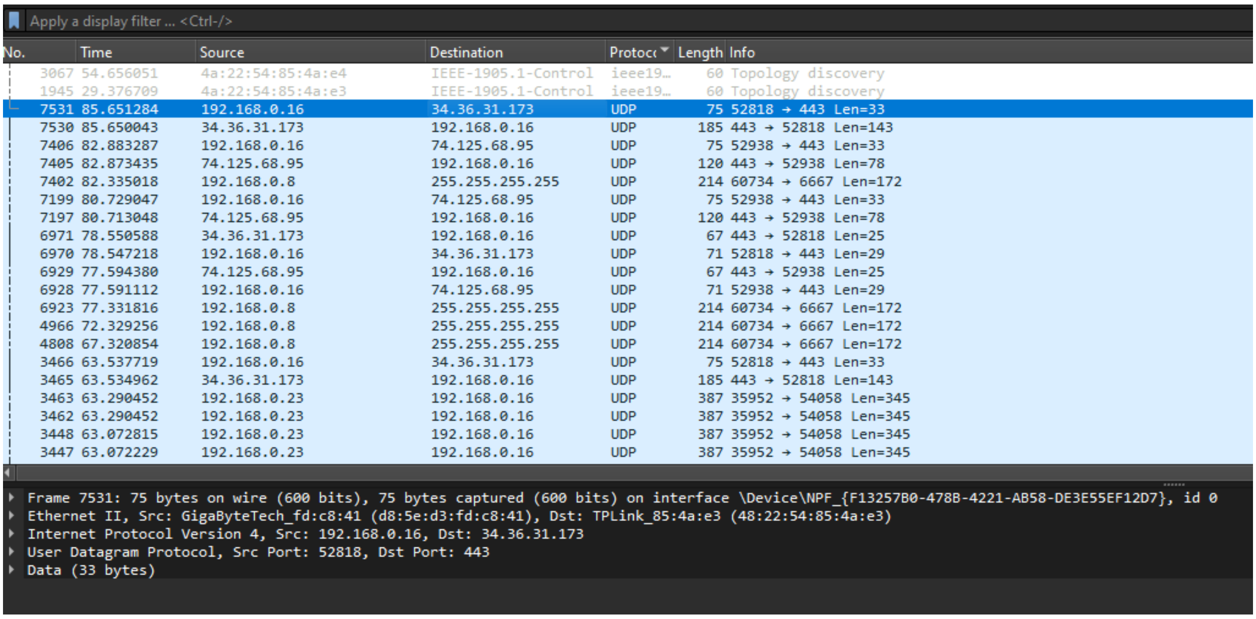
```
dns && ip.addr == 192.168.0.16
Packet list    Narrow & Wide    Case sensitive    String
No.   Time        Source            Destination      Protocol Length Info
 2142 33.438414   192.168.0.16      192.168.0.1      DNS        80 Standard query 0x0241 A ka-p.fontawesome.com
 2138 33.432078   192.168.0.16      192.168.0.1      DNS        75 Standard query 0x0675 HTTPS api.zilliqa.com
 5983 73.796010   192.168.0.16      192.168.0.1      DNS        79 Standard query 0x0eff HTTPS px.ads.linkedin.com
 1622 23.962485   192.168.0.16      192.168.0.1      DNS        85 Standard query 0x111a HTTPS postback.trafficmotor.com
 3746 64.704579   192.168.0.16      192.168.0.1      DNS        83 Standard query 0x1202 A treatment.grammarly.com
 2097 32.695176   192.168.0.16      192.168.0.1      DNS        79 Standard query 0x15f2 HTTPS kit.fontawesome.com
 2299 37.695830   192.168.0.16      192.168.0.1      DNS        79 Standard query 0x1645 HTTPS mail-ads.google.com
  678 18.933788   192.168.0.16      192.168.0.1      DNS        69 Standard query 0x165e HTTPS shodon.io
 4402 65.961346   192.168.0.16      192.168.0.1      DNS        91 Standard query 0x174d HTTPS content-autofill.googleapis.com
  929 22.042350   192.168.0.16      192.168.0.1      DNS        75 Standard query 0x17b3 A api.zilliqa.com
 5373 73.698038   192.168.0.16      192.168.0.1      DNS        84 Standard query 0x1af5 HTTPS www.googletagmanager.com
  325 9.143822    192.168.0.16      192.168.0.1      DNS        74 Standard query 0x1afa A ogs.google.com
 6262 73.843962   192.168.0.16      192.168.0.1      DNS        83 Standard query 0x1b47 HTTPS stats.g.doubleclick.net
 5982 73.795921   192.168.0.16      192.168.0.1      DNS        79 Standard query 0x1b56 A px.ads.linkedin.com
 1066 22.624472   192.168.0.16      192.168.0.1      DNS        74 Standard query 0x1c15 A img1.wsimg.com
 6564 74.067379   192.168.0.16      192.168.0.1      DNS        76 Standard query 0x1c26 HTTPS www.linkedin.com
 2038 32.070862   192.168.0.16      192.168.0.1      DNS        73 Standard query 0x20fb HTTPS www.shodan.io
  816 20.427535   192.168.0.16      192.168.0.1      DNS        75 Standard query 0x2486 HTTPS api.zilliqa.com
 6095 73.822762   192.168.0.16      192.168.0.1      DNS        75 Standard query 0x2c92 HTTPS www.gstatic.com
 6487 74.020336   192.168.0.16      192.168.0.1      DNS        75 Standard query 0x2eb4 HTTPS api.zilliqa.com
 1608 23.934063   192.168.0.16      192.168.0.1      DNS        85 Standard query 0x2f42 HTTPS postback.trafficmotor.com

Frame 243: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{F13257B0-478B-4221-AB58-DE3E55EF12D7}, id 0
Ethernet II, Src: GigaByteTech_fd:c8:41 (d8:5e:d3:fd:c8:41), Dst: TPLink_85:4a:e3 (48:22:54:85:4a:e3)
Internet Protocol Version 4, Src: 192.168.0.16, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 51102, Dst Port: 53
Domain Name System (query)
```

Port Number: 51102

Usage:

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

UDP



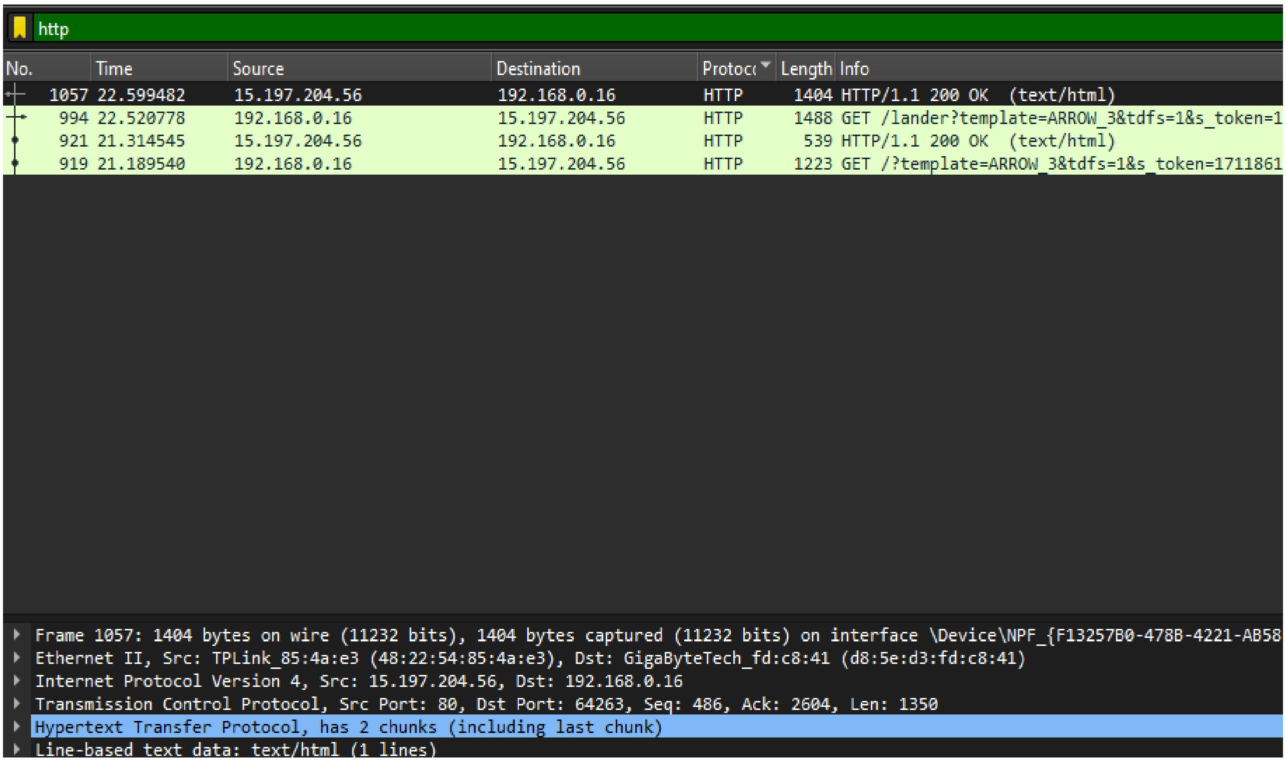
```
Apply a display filter ... <Ctrl-/>
No.   Time        Source              Destination          Protocc Length Info
 3067 54.656051   4a:22:54:85:4a:e4   IEEE-1905.1-Control  ieee19…   60 Topology discovery
 1945 29.376709   4a:22:54:85:4a:e3   IEEE-1905.1-Control  ieee19…   60 Topology discovery
 7531 85.651284   192.168.0.16        34.36.31.173         UDP       75 52818 → 443 Len=33
 7530 85.650043   34.36.31.173        192.168.0.16         UDP      185 443 → 52818 Len=143
 7406 82.883287   192.168.0.16        74.125.68.95         UDP       75 52938 → 443 Len=33
 7405 82.873435   74.125.68.95        192.168.0.16         UDP      120 443 → 52938 Len=78
 7402 82.335018   192.168.0.8         255.255.255.255      UDP      214 60734 → 6667 Len=172
 7199 80.729047   192.168.0.16        74.125.68.95         UDP       75 52938 → 443 Len=33
 7197 80.713048   74.125.68.95        192.168.0.16         UDP      120 443 → 52938 Len=78
 6971 78.550588   34.36.31.173        192.168.0.16         UDP       67 443 → 52818 Len=25
 6970 78.547218   192.168.0.16        34.36.31.173         UDP       71 52818 → 443 Len=29
 6929 77.594380   74.125.68.95        192.168.0.16         UDP       67 443 → 52938 Len=25
 6928 77.591112   192.168.0.16        74.125.68.95         UDP       71 52938 → 443 Len=29
 6923 77.331816   192.168.0.8         255.255.255.255      UDP      214 60734 → 6667 Len=172
 4966 72.329256   192.168.0.8         255.255.255.255      UDP      214 60734 → 6667 Len=172
 4808 67.320854   192.168.0.8         255.255.255.255      UDP      214 60734 → 6667 Len=172
 3466 63.537719   192.168.0.16        34.36.31.173         UDP       75 52818 → 443 Len=33
 3465 63.534962   34.36.31.173        192.168.0.16         UDP      185 443 → 52818 Len=143
 3463 63.290452   192.168.0.23        192.168.0.16         UDP      387 35952 → 54058 Len=345
 3462 63.290452   192.168.0.23        192.168.0.16         UDP      387 35952 → 54058 Len=345
 3448 63.072815   192.168.0.23        192.168.0.16         UDP      387 35952 → 54058 Len=345
 3447 63.072229   192.168.0.23        192.168.0.16         UDP      387 35952 → 54058 Len=345

Frame 7531: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{F13257B0-478B-4221-AB58-DE3E55EF12D7}, id 0
Ethernet II, Src: GigaByteTech_fd:c8:41 (d8:5e:d3:fd:c8:41), Dst: TPLink_85:4a:e3 (48:22:54:85:4a:e3)
Internet Protocol Version 4, Src: 192.168.0.16, Dst: 34.36.31.173
User Datagram Protocol, Src Port: 52818, Dst Port: 443
Data (33 bytes)
```

Port Number: 52818

Usage:

The User Datagram Protocol, or UDP, is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not formally establishing a connection before data is transferred.

HTTP



```
http
No.   Time       Source          Destination     Protocol Length Info
 1057 22.599482  15.197.204.56   192.168.0.16    HTTP     1404 HTTP/1.1 200 OK  (text/html)
  994 22.520778  192.168.0.16    15.197.204.56   HTTP     1488 GET /lander?template=ARROW_3&tdfs=1&s_token=1
  921 21.314545  15.197.204.56   192.168.0.16    HTTP      539 HTTP/1.1 200 OK  (text/html)
  919 21.189540  192.168.0.16    15.197.204.56   HTTP     1223 GET /?template=ARROW_3&tdfs=1&s_token=1711861

Frame 1057: 1404 bytes on wire (11232 bits), 1404 bytes captured (11232 bits) on interface \Device\NPF_{F13257B0-478B-4221-AB58
Ethernet II, Src: TPLink_85:4a:e3 (48:22:54:85:4a:e3), Dst: GigaByteTech_fd:c8:41 (d8:5e:d3:fd:c8:41)
Internet Protocol Version 4, Src: 15.197.204.56, Dst: 192.168.0.16
Transmission Control Protocol, Src Port: 80, Dst Port: 64263, Seq: 486, Ack: 2604, Len: 1350
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
Line-based text data: text/html (1 lines)
```

Port Number: 80

Usage:

The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack.

Discussion

Phase 1: Network Mapping

1. Devices are given IP address in the private range and are dynamically assigned via DHCP.
2. The DHCP server, managed by the router, dynamically assign.
3. There are many ways to gather information for network mapping, either by Command Prompt, or by going into the router IP address.
4. It is not enough to just know where the devices are in the network. Physically checking that these devices exist will help to provide an additional layer of security.

Phase 2: External Intel Gathering

1. Shodan enables anyone to find devices that use default login details.
2. It indexes IoT (Internet of Things) devices.
3. However, Shodan purpose in exposing the vulnerability is not for exploitation purposes.
4. Shodan is a powerful and easy-to-use tool for home users and businesses to help identify vulnerable devices.
5. The network public presenance is not shown on Shodan. This is good as it means no port is being exposed and that our information is protected and not vulnerable.

Conclusion

Network Mapping

Mapping a home network has several benefits. Firstly, it acts as a visual representation of the whole network layout, showing how devices connect and interact. This would make identifying potential issues easier.

Secondly, having a map can significantly reduce the time it takes to troubleshoot when problems arise. It enables users to quickly pinpoint where the issue might be originating from, be it a specific device or connection point.

Finally, by having a map, it can help to identify weaknesses in network security. By having a visual representation of where the devices are connected, we can quickly identify if any unauthorized devices snuck onto the network.

Overall, it is a proactive approach to maintaining a smooth-running, secure, and efficient household network.

Collecting Information

By using tools like Shodan and WHOIS, we checked how visible our network is to the public and analyzed the traffic to make sure we're safe. This step has helped us find and fix weak spots, and it taught us a lot about how to protect our network better.

Recommendations

Recommendations for Enhancing Data Security from being shown on Shodan.io:

1. Secure Booting: Implement secure boot mechanisms to ensure that devices boot using software that is known to be trusted. This prevents malicious software from running on the device.
2. Access Control: Limit access control of applications and devices to authorized personnel only, reducing the risk of accidental or intentional data breaches.
3. Authentication Protocols: Enforce strong authentication before transmitting or receiving data to verify the identity of the communicating entities and ensure data integrity.
4. Firewalls: Install robust firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules.
5. Firmware Updates: Regularly update devices to the latest firmware to patch vulnerabilities and enhance security features.

References

1. What is DNS? | How DNS works
   https://www.cloudflare.com/learning/dns/what-is-dns/#:~:text=The%20Domain%20Name%20System%20(DNS,browsers%20can%20load%20Internet%20resources.

2. What is UDP?
   https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/#:~:text=The%20User%20Datagram%20Protocol%2C%20or,connection%20before%20data%20is%20transferred.

3. What is HTTP?
   https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/#:~:text=The%20Hypertext%20Transfer%20Protocol%20(HTTP,of%20the%20network%20protocol%20stack.

4. How safe is your data with IoT and smart devices?
   https://www.comparitech.com/blog/information-security/iot-data-safety-privacy-hackers/

5. How to find and remove your device from the Shodan IoT search engine?
   https://www.comparitech.com/blog/vpn-privacy/remove-device-shodan/