Report\_Week\_01

Họ và tên: Trần Hân Nhi

MSSV: 2011770131 Lớp: 20DATA1

**Ex\_01:**

* **Thông tin tên miền “Hutech.edu.vn”**

Phạm vị địa chỉ IP 103.63.112.0 - 103.63.115.255

Thông tin liên hệ về các vấn đề vi phạm đến dãy địa chỉ IP 103.63.112.0 - 103.63.115.255: hm-changed@vnnic.vn

Tên mạng: CMCHCM-VN

Chi tiết thông tin: CMC Telecom Branch (Thành phố Hà Nội)

Chi nhánh: Lầu 2, Toà Rạng Đông, 81 Cách Mạng Tháng 8, Phường Bến Thành, quận 1, thành phố Hồ Chí Minh

Thông tin về người quản trị

Tên: Nguyen Duc Phong

Địa chỉ: CMCHCM-VN

Quốc gia: Việt Nam

Số điện thoại: +84-0918467458

e-mail: phong.nd@cmctelecom.vn

Mã số của người quản trị: NDP6-AP

Tên: Nguyen Nhu Thanh

Địa chỉ: CMCHCM-VN

Quốc gia: Việt Nam

Số điện thoại: +84-0982741198

e-mail: thanh.nn@cmctelecom.vn

Mã số của người quản trị: NNT26-AP

Thông tin nhóm Ứng phó sự cố

irt: IRT-VNNIC-AP

Địa chỉ: Hà Nội, Việt Nam

Số điện thoại: +84-24-35564944

Số fax: +84-24-37821462

e-mail: hm-changed@vnnic.vn

e-mail báo cáo vi phạm: hm-changed@vnnic.vn

Người quản trị và kỹ thuật: NTTT1-AP

Thông tin định tuyến: 103.63.115.0/24

Chi tiết: CMCTELECOM-VN

Được bảo trì bởi : MAINT-VN-VNNIC (Trung tâm Internet Việt Nam - Vietnam Internet Network Information Center)

* **Thông tin tên miền “Huflit.edu.vn”**

Phạm vi địa chỉ IP: 103.160.90.0 - 103.160.91.255

Thông tin liên hệ về các vấn đề vi phạm đến dãy địa chỉ IP 103.160.90.0 - 103.160.91.255: hm-changed@vnnic.vn

Tên mạng: VIKINGGLOBAL-VN

Chi tiết thông tin: VIKING GLOBAL TECHNOLOGY JOINT STOCK COMPANY

Địa chỉ: Tầng 29, tòa Đông, 29, 01 Lotte Center Hà Nội, số 54 Liễu Gia, Phường Cống Vị, Quận Ba Đình, Hà Nội

Quốc gia: Việt Nam

Thông tin nhóm Ứng phó sự cố

irt: IRT-VNNIC-AP

Địa chỉ: Hà Nội, Việt Nam

Số điện thoại: +84-24-35564944

Số fax: +84-24-37821462

e-mail: hm-changed@vnnic.vn

e-mail báo cáo vi phạm: hm-changed@vnnic.vn

Người quản trị và kỹ thuật: NTTT1-AP

Thông tin người quản trị

Tên: Pham Hong Tam

Địa chỉ: VIKINGGLOBAL-VN

Quốc gia: Việt Nam

Số điện thoại: +84-2473007300

e-mail: tamph@fpt.com.vn

Mã số của người quản trị: PHT34-AP

Thông tin định tuyến: 103.160.91.0/24

Được bảo trì bởi : MAINT-VN-VNNIC (Trung tâm Internet Việt Nam - Vietnam Internet Network Information Center)

**Ex\_02:**

**Thông tin bản ghi DNS tên miền “Hutech.edu.vn”**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| name | class | type | data | time to live | |
| hutech.edu.vn | IN | NS | ns2.pavietnam.vn | 3600s | (01:00:00) |
| hutech.edu.vn | IN | NS | nsbak.pavietnam.net | 3600s | (01:00:00) |
| hutech.edu.vn | IN | NS | ns1.pavietnam.vn | 3600s | (01:00:00) |
| hutech.edu.vn | IN | TXT | v=spf1 include:\_spf.google.com ~all | 300s | (00:05:00) |
| hutech.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 20 | | exchange: | alt4.aspmx.l.google.com | | 360s | (00:06:00) |
| hutech.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 30 | | exchange: | aspmx2.googlemail.com | | 360s | (00:06:00) |
| hutech.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 20 | | exchange: | alt3.aspmx.l.google.com | | 360s | (00:06:00) |
| hutech.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 30 | | exchange: | aspmx3.googlemail.com | | 360s | (00:06:00) |
| hutech.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 20 | | exchange: | alt2.aspmx.l.google.com | | 360s | (00:06:00) |
| hutech.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 10 | | exchange: | aspmx.l.google.com | | 360s | (00:06:00) |
| hutech.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 20 | | exchange: | alt1.aspmx.l.google.com | | 360s | (00:06:00) |
| hutech.edu.vn | IN | A | 103.63.115.9 | 3600s | (01:00:00) | |
| hutech.edu.vn | IN | SOA | |  |  | | --- | --- | | server: | ns1.pavietnam.vn | | email: | hostmaster@hutech.edu.vn | | serial: | 2023081959 | | refresh: | 14400 | | retry: | 3600 | | expire: | 1209600 | | minimum ttl: | 86400 | | 3600s | (01:00:00) |
| 9.115.63.103.in-addr.arpa | IN | PTR | static.cmcti.vn | 86400s | (1.00:00:00) |
| 115.63.103.in-addr.arpa | IN | SOA | |  |  | | --- | --- | | server: | hni.ns1.cmcti.vn | | email: | hostmaster@cmcti.vn | | serial: | 2021090809 | | refresh: | 28800 | | retry: | 7200 | | expire: | 1209600 | | minimum ttl: | 86400 | | 86400s | (1.00:00:00) |
| 115.63.103.in-addr.arpa | IN | NS | hcm.ns1.cmcti.vn | 86400 | (1.00:00:00) |
| 115.63.103.in-addr.arpa | IN | NS | hni.ns1.cmcti.vn | 86400s | (1.00:00:00) |

***Giải thích thông tin***

* Hutech.edu.vn được khai báo và quản lý trên các máy chủ:

nsbak.pavietnam.net

ns1.pavietnam.vn

ns2.pavietnam.vn

* Các mail server và độ ưu tiên của "Hutech.edu.vn":

alt4.aspmx.l.google.com - 20

aspmx2.googlemail.com - 30

alt3.aspmx.l.google.com - 20

aspmx3.googlemail.com - 30

alt2.aspmx.l.google.com - 20

aspmx.l.google.com – 10

alt1.aspmx.l.google.com – 20

Email sẽ thử gửi tới mail server “ aspmx.l.google.com ” đầu tiên có độ ưu tiên thấp nhất (10), nếu gửi thấy bại hoặc máy chủ không khả dụng, các mail server có độ ưu tiên là 20 sẽ được gửi thử tiếp theo. Nếu tất cả đều không khả dụng, 2 mail server có độ ưu tiên 30 sẽ thử cuối cùng.

* Phân giải tên miền “Hutech.edu.vn” thành địa chỉ IP 103.63.115.9
* Thông tin quản lý tên miền “hutech.edu.vn” trên DNS Server:

Máy chủ chính: ns1.pavietnam.vn

email: hostmaster@hutech.edu.vn

Số serial: 2023081959

Thời gian làm mới: 14400.

Thời gian thử lại: 3600.

Thời gian hết hạn: 1209600

Thời gian tối thiểu: 86400

* Phân giải đảo ngược địa chỉ IP 9.115.63.103.in-addr.arpa sang tên miền static.cmcti.vn
* Thông tin quản lý tên miền “115.63.103.in-addr.arpa” trên DNS Server:

Máy chủ chính: hni.ns1.cmcti.vn

email: hostmaster@cmcti.vn

Số serial: 2021090809

Thời gian làm mới: 28800

Thời gian thử lại: 7200

Thời gian hết hạn: 1209600

Thời gian tối thiểu: 86400

* 115.63.103.in-addr.arpa được khai báo và quản lý trên các máy chủ:

hcm.ns1.cmcti.vn

hni.ns1.cmcti.vn

**Thông tin bản ghi DNS tên miền “Huflit.edu.vn”**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| name | class | type | data | time to live | |
| huflit.edu.vn | IN | NS | ns1.pavietnam.vn | 360s | (00:06:00) | |
| huflit.edu.vn | IN | NS | nsbak.pavietnam.net | 360s | (00:06:00) | |
| huflit.edu.vn | IN | NS | ns2.pavietnam.vn | 360s | (00:06:00) | |
| huflit.edu.vn | IN | TXT | google-site-verification=XXbIUCCaEWCbtjKbgFL07AfrTH63oACGuXJZZMWACSg | 300s | (00:05:00) | |
| huflit.edu.vn | IN | MX | |  |  | | --- | --- | | preference: | 0 | | exchange: | huflit-edu-vn.mail.protection.outlook.com | | 360s | (00:06:00) | |
| huflit.edu.vn | IN | A | 103.160.91.216 | 360s | (00:06:00) | |
| huflit.edu.vn | IN | SOA | |  |  | | --- | --- | | server: | ns1.pavietnam.vn | | email: | hostmaster@huflit.edu.vn | | serial: | 2023090851 | | refresh: | 14400 | | retry: | 3600 | | expire: | 1209600 | | minimum ttl: | 86400 | | 3600s | (01:00:00) | |

***Giải thích thông tin***

* Huflit.edu.vn được khai báo và quản lý trên các máy chủ:

ns1.pavietnam.vn

nsbak.pavietnam.net

ns2.pavietnam.vn

* Mail server của “Huflit.edu.vn”: huflit-edu-vn.mail.protection.outlook.com với độ ưu tiên là 0.
* “Huflit.edu.vn” được phân giải thành địa chỉ IP 103.160.91.216
* Thông tin quản lý tên miền “huflit.edu.vn” trên DNS Server:

Máy chủ chính: ns1.pavietnam.vn

email: hostmaster@huflit.edu.vn

Số serial: 2023090851

Thời gian làm mới: 14400

Thời gian thử lại: 3600

Thời gian hết hạn: 1209600

Thời gian tối thiểu: 86400

**Ex\_03:**

**Quá trình gửi gói tin đi từ máy tính tới “Hutech.edu.vn”**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| hop | rtt | rtt | rtt |  | ip address | fully qualified domain name |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 1 |  | 169.254.158.58 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | 1 | 1 | 1 |  | 169.48.118.158 | ae103.ppr02.dal13.networklayer.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3 | 1 | 1 | 0 |  | 169.48.118.130 | 82.76.30a9.ip4.static.sl-reverse.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4 | 2 | \* | \* |  | 169.45.18.36 | ae16.cbs01.dr01.dal04.networklayer.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5 | \* | \* | \* |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6 | 32 | 32 | 32 |  | 169.53.16.240 | f0.10.35a9.ip4.static.sl-reverse.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7 | 32 | 34 | 32 |  | 80.77.2.81 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8 | 138 | 138 | 138 |  | 62.216.140.78 | ae1.pjr04.lax002.flagtetl.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9 | 134 | 134 | 134 |  | 62.216.129.206 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10 | 135 | 135 | 135 |  | 62.216.128.65 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 11 | 190 | 190 | 190 |  | 80.77.2.158 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 12 | 205 | 205 | 205 |  | 203.205.56.109 | static.cmcti.vn |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 13 | 205 | 205 | 205 |  | 203.205.56.45 | static.cmcti.vn |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 14 | 204 | 204 | 204 |  | 103.63.115.9 | static.cmcti.vn |

Gói tin đi qua 14 route, từ máy tính cá nhân đến địa chỉ IP 103.63.115.9 (Hutech.edu.vn) mất 1,278 giây. Số bước nhảy là 13. Có những chỗ trống "\*" thể hiện gói tin không nhận được phản hồi.

**Quá trình gửi gói tin đi từ máy tính tới “Shopee.vn”**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| hop | rtt | rtt | rtt |  | ip address | fully qualified domain name |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 0 |  | 169.254.158.58 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | 2 | 2 | 1 |  | 169.48.118.162 | ae103.ppr04.dal13.networklayer.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3 | 1 | 0 | 0 |  | 169.48.118.134 | 86.76.30a9.ip4.static.sl-reverse.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4 | \* | \* | \* |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5 | \* | \* | \* |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6 | 30 | 30 | 31 |  | 169.53.16.238 | ee.10.35a9.ip4.static.sl-reverse.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7 | 31 | 31 | 31 |  | 206.72.210.65 | telstra.as4637.any2ix.coresite.com |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8 | 34 | 33 | 33 |  | 202.84.253.85 | i-93.1wlt-core02.telstraglobal.net |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9 | 170 | 169 | 169 |  | 202.84.253.85 | i-93.1wlt-core02.telstraglobal.net |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10 | \* | \* | \* |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 11 | 178 | 179 | 178 |  | 202.84.156.54 | i-97.hkgg01.telstraglobal.net |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 12 | 178 | 178 | 178 |  | 202.127.78.174 | unknown.telstraglobal.net |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 13 | 217 | 215 | 215 |  | 27.68.244.26 | localhost |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 14 | 225 | 231 | 231 |  | 27.68.232.2 | localhost |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 15 | 221 | \* | \* |  | 27.68.255.61 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 16 | 224 | 224 | 224 |  | 27.68.229.2 | localhost |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 17 | 214 | 213 | 212 |  | 203.113.156.196 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 18 | 225 | 225 | 224 |  | 103.1.208.26 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 19 | 222 | 220 | 220 |  | 171.244.2.14 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 20 | \* | \* | \* |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 21 | \* | \* | \* |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 22 | 224 | 224 | 224 |  | 103.117.240.34 |

Gói tin đi qua 21 route, từ máy tính cá nhân đến địa chỉ IP 103.117.240.34 (Hutech.edu.vn) mất 2,726 giây. Số bước nhảy là 21.

**Ex\_04:**

Daotao.hutech.edu.vn







Các thông tin thu thập được từ trang web “Daotao.hutech.edu.vn”

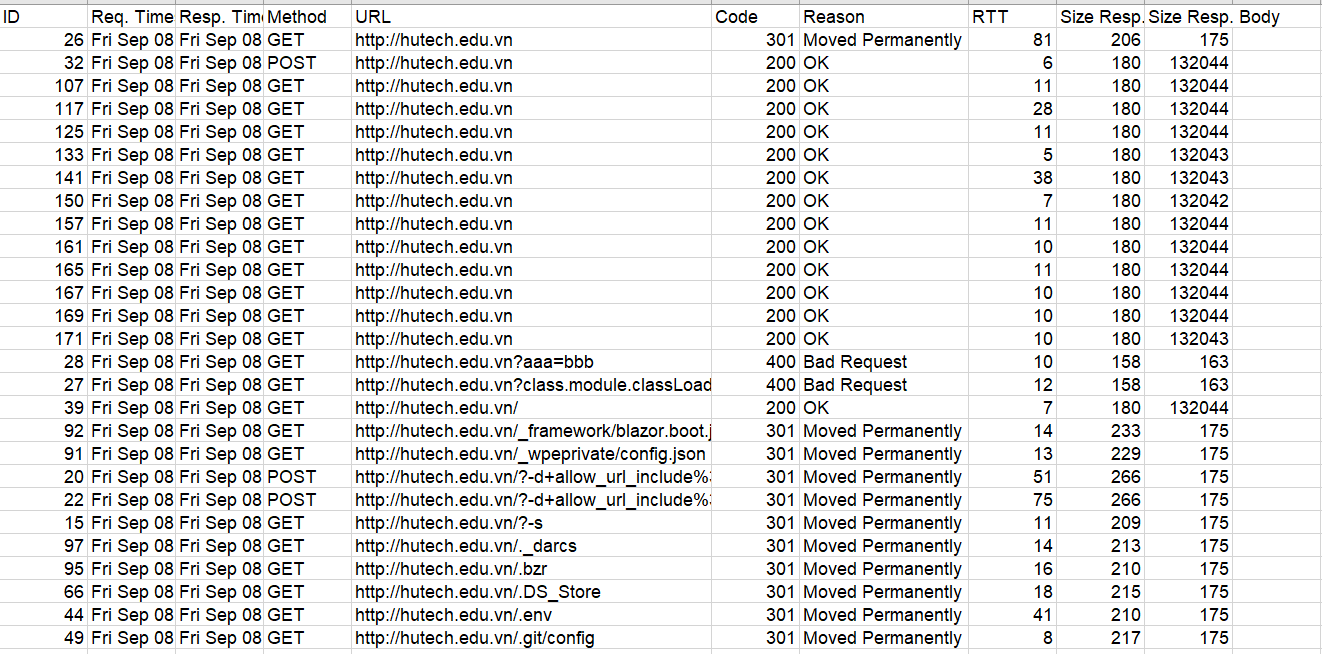
* Trang web là sản phẩm của Công ty TNHH Một thành viên Phần Mềm Anh Quân
* Số điện thoại:

(08) 381 13579

(08) 629 67016

* Số Fax: (08) 629 67016
* Email : [info@edusoft.net.vn](mailto:info@edusoft.net.vn)

**Ex\_05:**



**Thông tin nhận được :**

Phương thức yêu cầu:

Phương thức GET: 46 lần

Phương thức POST: 3 lần

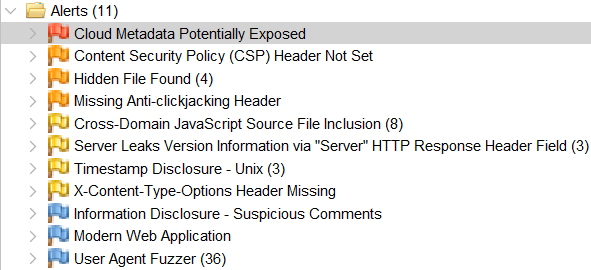
Mã trạng thái HTTP của phản hồi từ máy chủ.

- 200 (OK): 27 lần

- 301 (Moved Permanently): 52 lần - Yêu cầu chuyển hướng

- 400 (Bad Request): 2 lần - Máy chủ không thể hiểu hoặc xử lý yêu cầu

Các vấn đề bảo mật cùng với các mức độ rủi ro, giải pháp:



* Cloud Metadata Potentially Exposed - Cao

Thông tin về cơ sở hạ tầng máy chủ hoặc dịch vụ có thể đã được tiết lộ, đặc biệt là các dịch vụ đám mây như AWS, Azure, hoặc Google Cloud. Việc tiết lộ thông tin về môi trường điện toán đám mây có thể ảnh hưởng đến an ninh thông tin.

* Content Security Policy (CSP) Header Not Set - Trung bình

CSP header chưa được thiết lập, điều này có thể làm tăng nguy cơ XSS attack. CSP là một biện pháp bảo mật web để ngăn chặn tấn công Cross-Site Scripting (XSS) và các tấn công khác. Thiếu CSP header có thể tạo lỗ hổng bảo mật và cần được quản lý. Nên cài đặt CSP để bảo vệ ứng dụng

* Hidden File Found - Trung bình

Môt tập tin ẩn (hidden file) đã được phát hiện. Có thể tiềm ẩn rủi ro bảo mật, tùy thuộc vào nội dung của tập tin đó, đặc biệt nếu chúng chứa thông tin nhạy cảm. Cần kiểm tra xem tập tin ẩn này có thông tin quan trọng không và xác định liệu nó nên được tiếp tục giữ ẩn hay không.

* Missing Anti-clickjacking Header - Trung bình

Header chống clickjacking có thể đã không được thiết lập. Clickjacking là một hình thức tấn công trang web. Thiếu anti-clickjacking header có thể làm cho trang web của dễ bị tấn công, một trang web có thể bị nhúng vào một khung ẩn để lừa người dùng và nó cần được quản lý. Cài đặt các header giúp bảo vệ khỏi tấn công clickjacking.

* Cross-Domain JavaScript Source File Inclusion - Thấp

Vấn đề bảo mật liên quan đến việc bao gồm (inclusion) các tập tin nguồn JavaScript từ các nguồn tài nguyên khác nhau. Nếu việc bao gồm các tập tin nguồn JavaScript từ các domain khác nhau không được thực hiện đúng cách hoặc bị bỏ qua, có thể tạo ra lỗ hổng bảo mật trên trang web, cho phép tin tặc tiềm năng thực hiện các cuộc tấn công bảo mật.

* Server Leaks Version Information via "Server" HTTP Response Header Field - Thấp

Thông báo này chỉ ra rằng thông tin phiên bản của máy chủ đã được tiết lộ thông qua trường "Server" trong header HTTP response. Mức độ nguy cơ thấp, nhưng nên xem xét ẩn thông tin này để ngăn chặn việc tấn công dựa trên lỗ hổng cụ thể.

* Timestamp Disclosure - Unix- Thấp

Mức độ nguy cơ thấp, tuy nhiên, nên kiểm tra xem liệu thông tin về thời gian này có thể được sử dụng để tấn công không. (2023-09-07 15:06:34)

* X-Content-Type-Options Header Missing - Thấp

Thông báo này cho biết rằng header "X-Content-Type-Options" chưa được thiết lập. Header này giúp ngăn chặn tấn công kiểu MIME (MIME sniffing). Mức độ nguy cơ thấp, nhưng nên cài đặt header này để bảo vệ trình duyệt khỏi các loại tấn công liên quan đến kiểu MIME

**Ex\_06:**

* Acunetix quét trang “keep.google.com” thông báo mức độ đe doạ 3. Trình quét phát hiện nhiều lỗ hổng nghiệm trọng trong ứng dụng đe doạ đáng kể đến bảo mật của ứng dụng, có thể cho phép attacker xâm nhập vào cơ sở dữ liệu.
* Ngoài những lỗ hổng ra, trình quét còn có những thông tin liên quan đến trang web như:

Server : ESF

Máy chủ được phát hiện :

https://google.com

https://bdn.dev

https://origin-test.bdn.dev

https://google.ca

https://google.cl

https://google.co.in

https://google.co.jp

https://google.co.uk

https://google.com.ar

https://google.com.au

https://google.com.br

https://google.com.co

https://google.com.mx

https://google.com.tr

https://google.com.vn

https://google.de

https://google.es

https://google.fr

https://google.hu

https://google.it

https://google.nl

https://google.pl

https://google.pt

https://googleadapis.com

https://googleapis.cn

https://googlevideo.com

https://gstatic.cn

https://gstatic-cn.com

https://googlecnapps.cn

https://googleapps-cn.com

https://gkecnapps.cn

https://googledownloads.cn

https://recaptcha.net.cn

https://recaptcha-cn.net

https://widevine.cn

https://ampproject.org.cn

https://ampproject.net.cn

https://google-analytics-cn.com

https://googleadservices-cn.com

https://googlevads-cn.com

https://googleapis-cn.com

https://googleoptimize-cn.com

https://doubleclick-cn.net

https://fls.doubleclick-cn.net

https://g.doubleclick-cn.net

https://doubleclick.cn

https://fls.doubleclick.cn

https://g.doubleclick.cn

https://dartsearch-cn.net

https://googletraveladservices-cn.com

https://googletagservices-cn.com

https://googletagmanager-cn.com

https://googlesyndication-cn.com

https://safeframe.googlesyndication-cn.com

https://app-measurement-cn.com

https://gvt1-cn.com

https://gvt2-cn.com

https://2mdn-cn.net

https://googleflights-cn.net

https://admob-cn.com

https://googlesandbox-cn.com

https://safenup.googlesandbox-cn.com

https://gstatic.com

https://gvt1.com

https://gcpcdn.gvt1.com

https://gvt2.com

https://gcp.gvt2.com

https://youtube-nocookie.com

https://ytimg.com

https://android.com

https://flash.android.com

https://g.cn

https://g.co

https://goo.gl

https://www.goo.gl

https://google-analytics.com

https://googlecommerce.com

https://ggpht.cn

https://urchin.com

https://youtu.be

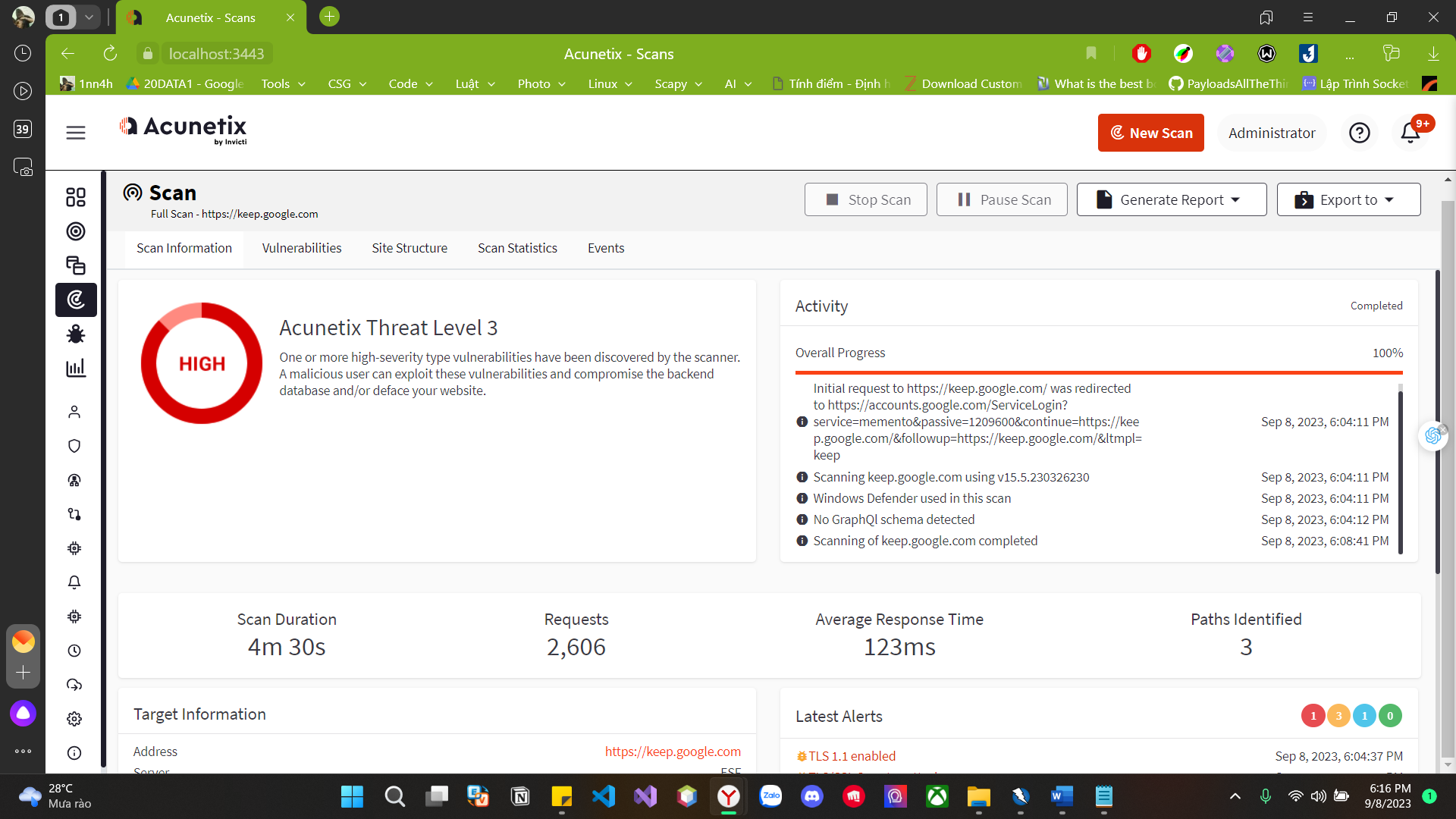
https://youtubeeducation.com

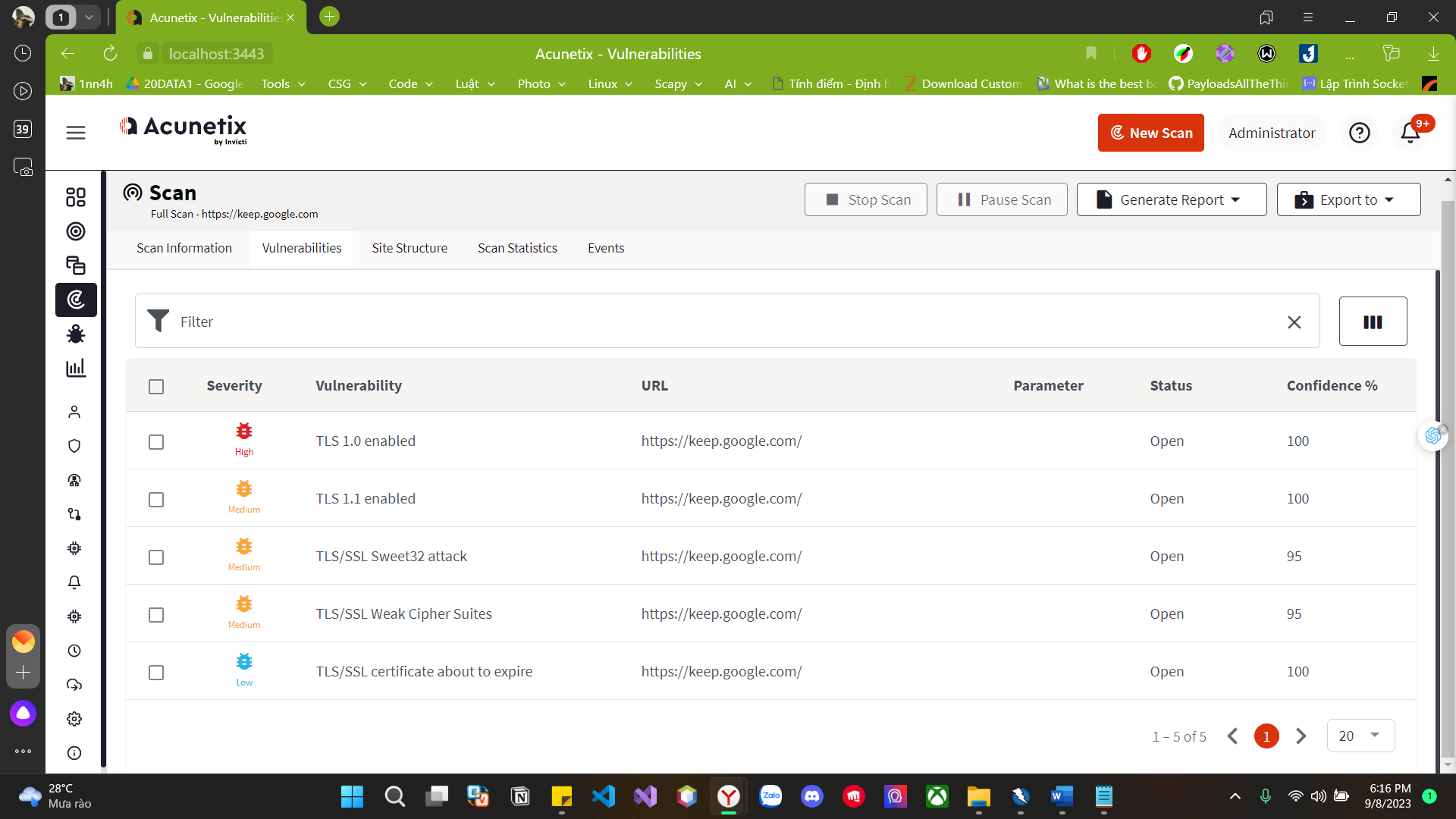
https://youtubekids.com

https://yt.be

Cảnh báo mới nhất với các mức độ rủi ro:

* TLS 1.0 enabled – Cao. Việc sử dụng TLS 1.0 có thể làm tăng nguy cơ cho việc tấn công mạng và tiết lộ thông tin.
* TLS 1.1 enabled – Trung bình. Mặc dù nó tốt hơn TLS 1.0, nhưng nó cũng đã bị khuyến nghị thay thế bằng các phiên bản TLS mới hơn như TLS 1.2 hoặc TLS 1.3.
* TLS/SSL Sweet32 attack – Trung bình. Đây là một tấn công có thể giải mã thông tin bí mật khi sử dụng một số thuật toán mã hóa và ciphersuite yếu trong TLS và SSL.
* TLS/SSL Weak Cipher Suites – Trung bình. Việc sử dụng cipher suites yếu có thể làm giảm bảo mật của kết nối TLS/SSL và làm tăng nguy cơ cho các cuộc tấn công (man-in-the-middle).
* TLS/SSL certificate about to expire – Thấp. Giấy chứng nhận SSL có hiệu lực ngắn hạn đòi hỏi phải thay đổi hoặc gia hạn chúng đúng thời hạn. Nếu giấy chứng nhận hết hạn, trang web có thể không được trình duyệt công nhận là an toàn và người dùng có thể gặp khó khăn khi truy cập.





* Report theo tiêu chuẩn ISO/IEC 27001:



Các thông tin ảnh hưởng đến ISMS:

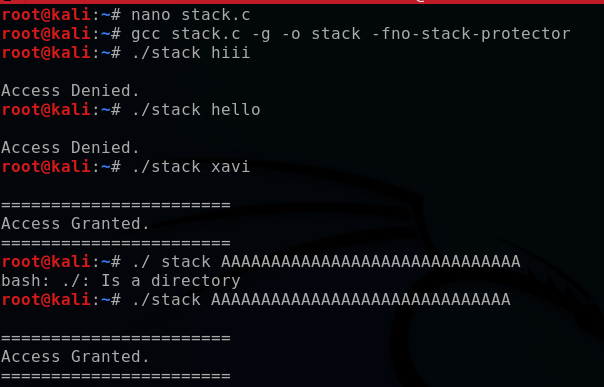
TLS 1.0 và TLS 1.1 enabled: Việc sử dụng các phiên bản TLS cũ và không an toàn có thể làm suy yếu tính bảo mật của hệ thống. ISO 27001 yêu cầu đánh giá và quản lý rủi ro liên quan đến an ninh thông tin, vì vậy việc sử dụng TLS không an toàn có thể được xem xét là một rủi ro cần đánh giá và giảm thiểu.

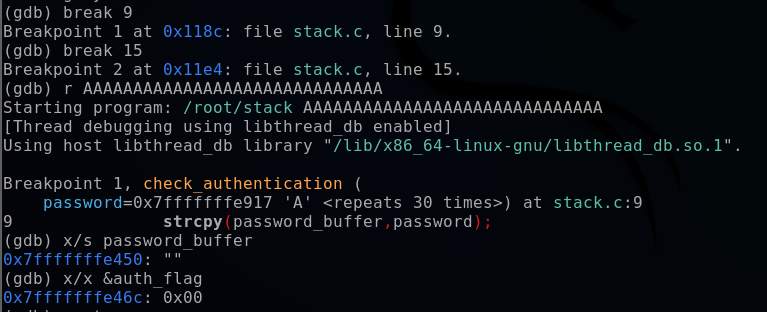
TLS/SSL Sweet32 attack và TLS/SSL Weak Cipher Suites: Các vấn đề liên quan đến ciphersuite yếu và các tấn công như Sweet32 có thể làm giảm tính bảo mật của hệ thống. ISO 27001 đòi hỏi việc xác định và giảm thiểu các rủi ro bảo mật, và việc giảm thiểu các cipher suites yếu là một phần quan trọng của việc này.

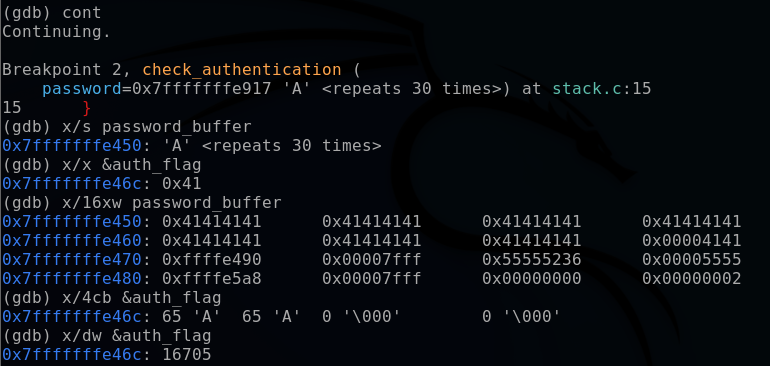
TLS/SSL certificate about to expire: ISO 27001 yêu cầu duy trì tính khả dụng và an toàn của thông tin. Nếu giấy chứng nhận SSL hết hạn và trang web không thể truy cập, điều này có thể ảnh hưởng đến tính khả dụng của hệ thống và thông tin liên quan đến an ninh.

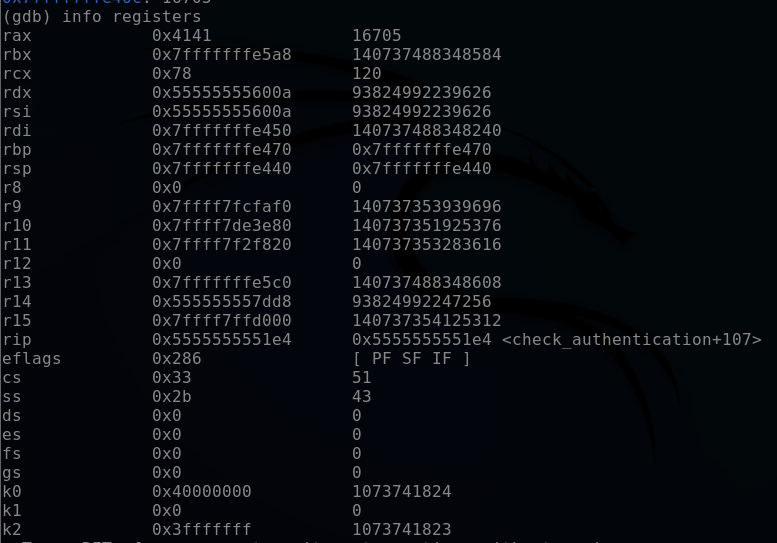
**Ex\_07:**

* Bài tập Buffer Overflow

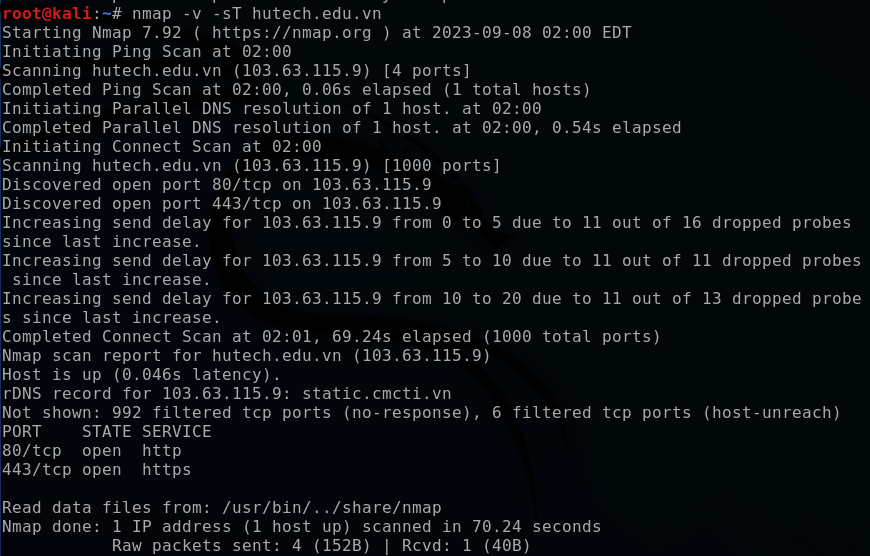








Dùng nmap kiểm tra



Có 2 cổng đang mở là : 80 (HTTP) – giao thức web, 443(HTTPS) – giao thức web bảo mật. Đây đều là những cổng thông thường được sử dụng phổ biến trên internet.

992 cổng không phản hồi, có thể do tường lửa hoặc máy chủ không gửi phản hồi cho các yêu cầu thăm dò dù có hoặc động hay không.

6 cổng máy chủ không thể tiếp cận được có thể do máy chủ đích không thể truy cập hoặc hoạt động tại thời điểm thăm dò.