

Report_Week_01

Họ và tên: Trần Hân Nhi

MSSV: 2011770131 Lớp: 20DATA1

Ex_01:

- Thông tin tên miền “Hutech.edu.vn”

Phạm vi 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	360s (00:06:00)

			exchange:	aspmx3.googlemail.com	
hutech.edu.vn	IN	MX	preference:	20	360s (00:06:00)
			exchange:	alt2.aspmx.l.google.com	
hutech.edu.vn	IN	MX	preference:	10	360s (00:06:00)
			exchange:	aspmx.l.google.com	
hutech.edu.vn	IN	MX	preference:	20	360s (00:06:00)
			exchange:	alt1.aspmx.l.google.com	
hutech.edu.vn	IN	A		103.63.115.9	3600s (01:00:00)
hutech.edu.vn	IN	SOA	server:	ns1.pavietnam.vn	3600s (01:00:00)
			email:	hostmaster@hutech.edu.v n	
			serial:	2023081959	
			refresh:	14400	
			retry:	3600	
			expire:	1209600	
			minimu m ttl:	86400	
9.115.63.103.i n-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	86400s (1.00:00:00)
			email:	hostmaster@cmcti.vn	
			serial:	2021090809	
			refresh:	28800	
			retry:	7200	
			expire:	1209600	
			minimum ttl:	86400	
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		360s (00:06:00)
			exchange: huflit-edu-vn.mail.protection.outlook.com		
huflit.edu.vn	IN	A	103.160.91.216		360s (00:06:00)
huflit.edu.vn	IN	SOA	server: ns1.pavietnam.vn		3600s (01:00:00)
			email: hostmaster@huflit.edu.vn		
			serial: 2023090851		
			refresh: 14400		
			retry: 3600		
			expire: 1209600		
			minimum ttl: 86400		

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.hkkg01.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

Email	Name	URL	Title	Host
info@edusoft.net.vn	info	http://daotao.hutech.edu.vn/Default.aspx?page=thongtinsp	C?ng Th?ng Tin ?ào T?o-Tru?ng ??i H?c C?ng Ngh? TP.HCM-KTCN	http://daotao.hutech.edu.vn

Phone	Source	Tag	URL	Title	Host
0838113579	(08) 381 13579	Tel	http://daotao.hutech.edu.vn/Default.aspx?page=thongtinsp	C?ng Th?ng Tin ?ào T?o-Tru?ng ??i H?c C?ng Ngh? TP.HCM-KTCN	http://daotao.hutech.edu.vn
0962967016	(08) 6296 7016		http://daotao.hutech.edu.vn/Default.aspx?page=thongtinsp	C?ng Th?ng Tin ?ào T?o-Tru?ng ??i H?c C?ng Ngh? TP.HCM-KTCN	http://daotao.hutech.edu.vn

Fax	Source	Tag	URL	Title	Host	Keywords de
0838113579	(08) 381 13579		http://daotao.hutech.edu.vn/Default.aspx?page=thongtinsp	C?ng Th?ng Tin ?ào T?o-Tru?ng ??i H?c C?ng Ngh? TP.HCM-KTCN	http://daotao.hutech.edu.vn	0
0962967016	(08) 6296 7016	Fax	http://daotao.hutech.edu.vn/Default.aspx?page=thongtinsp	C?ng Th?ng Tin ?ào T?o-Tru?ng ??i H?c C?ng Ngh? TP.HCM-KTCN	http://daotao.hutech.edu.vn	0

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

Ex_05:

ID	Req. Time	Resp. Time	Method	URL	Code	Reason	RTT	Size Resp.	Size Resp.	Body
26	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	301	Moved Permanently	81	206	175	
32	Fri Sep 08	Fri Sep 08	POST	http://hutech.edu.vn	200	OK	6	180	132044	
107	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	11	180	132044	
117	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	28	180	132044	
125	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	11	180	132044	
133	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	5	180	132043	
141	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	38	180	132043	
150	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	7	180	132042	
157	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	11	180	132044	
161	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	10	180	132044	
165	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	11	180	132044	
167	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	10	180	132044	
169	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	10	180	132044	
171	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn	200	OK	10	180	132043	
28	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn?aaa=bbb	400	Bad Request	10	158	163	
27	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn?class.module.classLoad	400	Bad Request	12	158	163	
39	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/	200	OK	7	180	132044	
92	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/_framework/blazor.boot.j	301	Moved Permanently	14	233	175	
91	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/_wpeprivate/config.json	301	Moved Permanently	13	229	175	
20	Fri Sep 08	Fri Sep 08	POST	http://hutech.edu.vn/?-d+allow_url_include%	301	Moved Permanently	51	266	175	
22	Fri Sep 08	Fri Sep 08	POST	http://hutech.edu.vn/?-d+allow_url_include%	301	Moved Permanently	75	266	175	
15	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/?-s	301	Moved Permanently	11	209	175	
97	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/_darcs	301	Moved Permanently	14	213	175	
95	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/_bzz	301	Moved Permanently	16	210	175	
66	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/.DS_Store	301	Moved Permanently	18	215	175	
44	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/.env	301	Moved Permanently	41	210	175	
49	Fri Sep 08	Fri Sep 08	GET	http://hutech.edu.vn/.git/config	301	Moved Permanently	8	217	175	

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:

Alerts (11)
Cloud Metadata Potentially Exposed
Content Security Policy (CSP) Header Not Set
Hidden File Found (4)
Missing Anti-clickjacking Header
Cross-Domain JavaScript Source File Inclusion (8)
Server Leaks Version Information via "Server" HTTP Response Header Field (3)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing
Information Disclosure - Suspicious Comments
Modern Web Application
User Agent Fuzzer (36)

- 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

Một 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 dọa 3. Trình quét phát hiện nhiều lỗ hổng nghiêm trọng trong ứng dụng đe dọa 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>

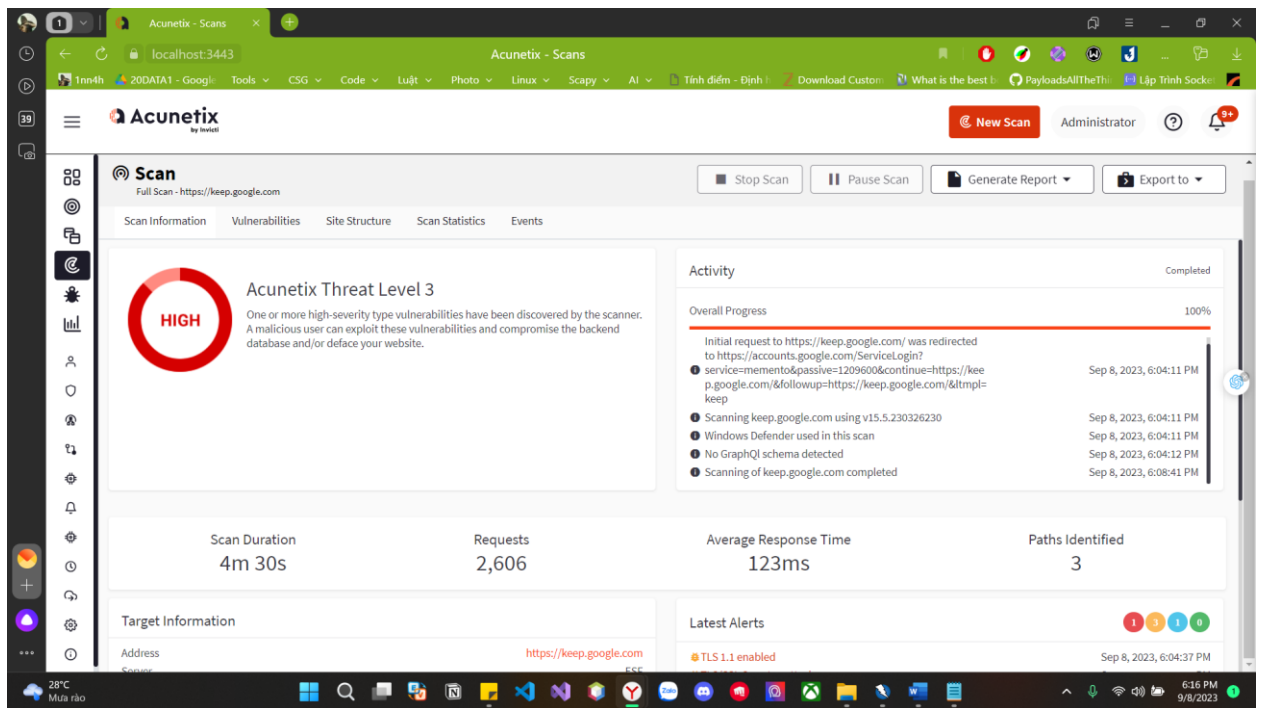
<https://google.com.tr>
<https://google.com.vn>
<https://google.de>
<https://google.es>
<https://google.fr>
<https://google.hu>
<https://google.it>
<https://google.nl>
<https://google.pl>
<https://google.pt>
<https://googleadapis.com>
<https://googleapis.cn>
<https://googlevideo.com>
<https://gstatic.cn>
<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://yting.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 chứng 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.



The screenshot displays the Acunetix Vulnerabilities interface for a full scan of https://keep.google.com. The table lists the following vulnerabilities:

Severity	Vulnerability	URL	Parameter	Status	Confidence %
High	TLS 1.0 enabled	https://keep.google.com/		Open	100
Medium	TLS 1.1 enabled	https://keep.google.com/		Open	100
Medium	TLS/SSL Sweet32 attack	https://keep.google.com/		Open	95
Medium	TLS/SSL Weak Cipher Suites	https://keep.google.com/		Open	95
Low	TLS/SSL certificate about to expire	https://keep.google.com/		Open	100

- Report theo tiêu chuẩn ISO/IEC 27001:



20230908_ISO_27001_https_keep_google_com.pdf

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.

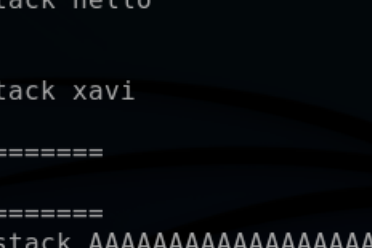
TLS/SSL Sweet32 attack và TLS/SSL Weak Cipher Suites: Các vấn đề liên quan đến ciphersuite yếu và các tấn công như Sweet32 có thể làm giảm tính bảo mật của hệ thống. ISO 27001 đòi hỏi việc xác định và giảm thiểu các rủi ro bảo mật, và việc giảm thiểu các cipher suites yếu là một phần quan trọng của việc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

```
root@kali:~# nano stack.c  
root@kali:~# gcc stack.c -g -o stack -fno-stack-protector  
root@kali:~# ./stack hiii  
  
Access Denied.  
root@kali:~# ./stack hello  
  
Access Denied.  
root@kali:~# ./stack xavi  
  
=====  
Access Granted.  
=====
```



```
root@kali:~# ./ stack AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
bash: ./: Is a directory  
root@kali:~# ./stack AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
  
=====  
Access Granted.  
=====
```



```

(gdb) break 9
Breakpoint 1 at 0x118c: file stack.c, line 9.
(gdb) break 15
Breakpoint 2 at 0x11e4: file stack.c, line 15.
(gdb) r AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Starting program: /root/stack AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, check_authentication (
    password=0x7fffffff917 'A' <repeats 30 times>) at stack.c:9
9      strcpy(password_buffer,password);
(gdb) x/s password_buffer
0x7fffffff917: ""
(gdb) x/x &auth_flag
0x7fffffff918: 0x00

```

```

(gdb) cont
Continuing.

Breakpoint 2, check_authentication (
    password=0x7fffffff917 'A' <repeats 30 times>) at stack.c:15
15 }
(gdb) x/s password_buffer
0x7fffffff917: 'A' <repeats 30 times>
(gdb) x/x &auth_flag
0x7fffffff918: 0x41
(gdb) x/16xw password_buffer
0x7fffffff917: 0x41414141 0x41414141 0x41414141 0x41414141
0x7fffffff918: 0x41414141 0x41414141 0x41414141 0x00004141
0x7fffffff919: 0xffffe490 0x00007fff 0x55555236 0x00005555
0x7fffffff91a: 0xffffe5a8 0x00007fff 0x00000000 0x00000002
(gdb) x/4cb &auth_flag
0x7fffffff918: 65 'A' 65 'A' 0 '\000' 0 '\000'
(gdb) x/dw &auth_flag
0x7fffffff918: 16705

```

```

(gdb) info registers
rax                0x4141                16705
rbx                0x7fffffff5a8          140737488348584
rcx                0x78                  120
rdx                0x55555555600a         93824992239626
rsi                0x55555555600a         93824992239626
rdi                0x7fffffff450         140737488348240
rbp                0x7fffffff470         0x7fffffff470
rsp                0x7fffffff440         0x7fffffff440
r8                 0x0                   0
r9                 0x7ffff7fcfaf0        140737353939696
r10                0x7ffff7de3e80        140737351925376
r11                0x7ffff7f2f820        140737353283616
r12                0x0                   0
r13                0x7fffffff5c0         140737488348608
r14                0x555555557dd8        93824992247256
r15                0x7ffff7ffd000        140737354125312
rip                0x5555555551e4        0x5555555551e4 <check_authentication+107>
eflags             0x286                [ PF SF IF ]
cs                 0x33                51
ss                 0x2b                43
ds                 0x0                  0
es                 0x0                  0
fs                 0x0                  0
gs                 0x0                  0
k0                 0x40000000           1073741824
k1                 0x0                  0
k2                 0x3fffffff           1073741823

```

Dùng nmap kiểm tra

```

root@kali:~# nmap -v -sT hutech.edu.vn
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-08 02:00 EDT
Initiating Ping Scan at 02:00
Scanning hutech.edu.vn (103.63.115.9) [4 ports]
Completed Ping Scan at 02:00, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:00
Completed Parallel DNS resolution of 1 host. at 02:00, 0.54s elapsed
Initiating Connect Scan at 02:00
Scanning hutech.edu.vn (103.63.115.9) [1000 ports]
Discovered open port 80/tcp on 103.63.115.9
Discovered open port 443/tcp on 103.63.115.9
Increasing send delay for 103.63.115.9 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Increasing send delay for 103.63.115.9 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 103.63.115.9 from 10 to 20 due to 11 out of 13 dropped probes since last increase.
Completed Connect Scan at 02:01, 69.24s elapsed (1000 total ports)
Nmap scan report for hutech.edu.vn (103.63.115.9)
Host is up (0.046s latency).
rDNS record for 103.63.115.9: static.cmcti.vn
Not shown: 992 filtered tcp ports (no-response), 6 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 70.24 seconds
Raw packets sent: 4 (152B) | Rcvd: 1 (40B)

```

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.