WelcomeSecurity
Enabling value through IT security

Exploiting Systems

Behind the scenes

Thomas Ljungberg Kristensen, thomas@welcomesecurity.net

Aug. 2016

Shadow Brokers claim to have hacked the Equation Group, a group linked to the NSA’s Tailored Access Group, and began auctioning off stolen hacking tools online

March 2017

Microsoft is informed of the vulnerabilities and patches them

14 Apr. 2017

Shadow Brokers release the EternalBlue and DoublePulsar exploits

12 May 2017

WannaCry ransomware attack begins using the EternalBlue exploit, infecting over 300,000 computers in 150 countries.

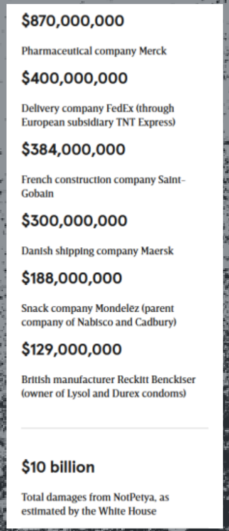
The consequence could have been even worse if Marcus Hutchins had not found it’s Kill Switch

North Korea is expected to be behind the attack

27 June 2017

NotPetya cyberattack occurs using the same EternalBlue exploit, infecting thousands of computers across the globe, including the shipping giant Maersk

The Russian government (Sandworm hacking group within the GRU Russian military intelligence organization) is expected to by behind the attack which started as an attack on the software update mechanism of M.E.Doc — a Ukrainian tax preparation program



$870,000,000	Pharmaceutical company Merck
$400,000,000	Delivery company FedEx (through European subsidiary TNT Express)
$384,000,000	French construction company Saint-Gobain
$300,000,000	Danish shipping company Maersk
$188,000,000	Snack company Mondelēz (parent company of Nabisco and Cadbury)
$129,000,000	British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)
$10 billion	Total damages from NotPetya, as estimated by the White House

https://en.wikipedia.org/wiki/The_Shadow_Brokers
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
https://en.wikipedia.org/wiki/Petya_(malware_family)
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

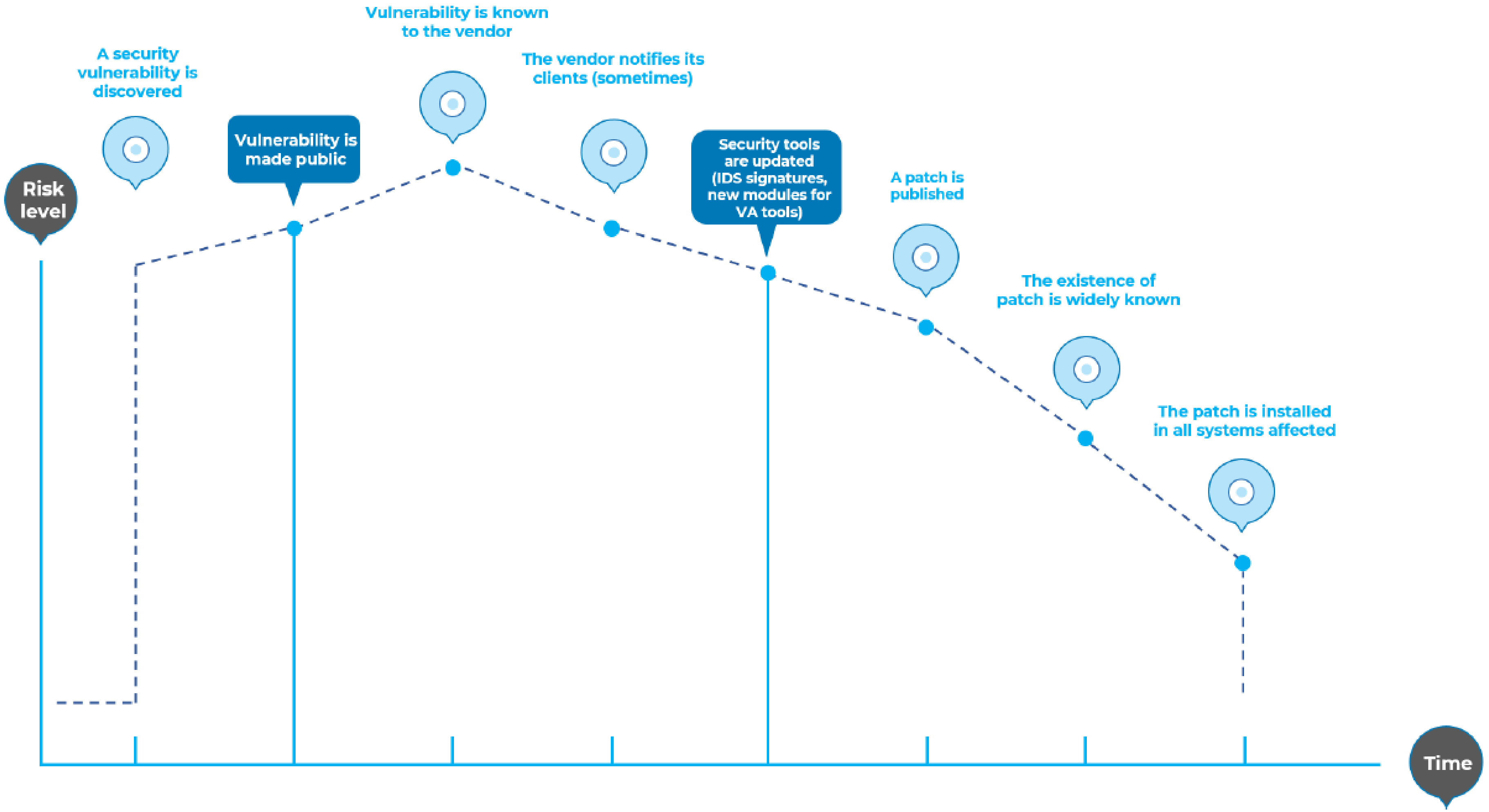

Risk level
A security vulnerability is discovered
Vulnerability is made public
Vulnerability is known to the vendor
The vendor notifies its clients (sometimes)
Security tools are updated (IDS signatures, new modules for VA tools)
A patch is published
The existence of patch is widely known
The patch is installed in all systems affected
Time

Figure 2-2: Window of Vulnerability

https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

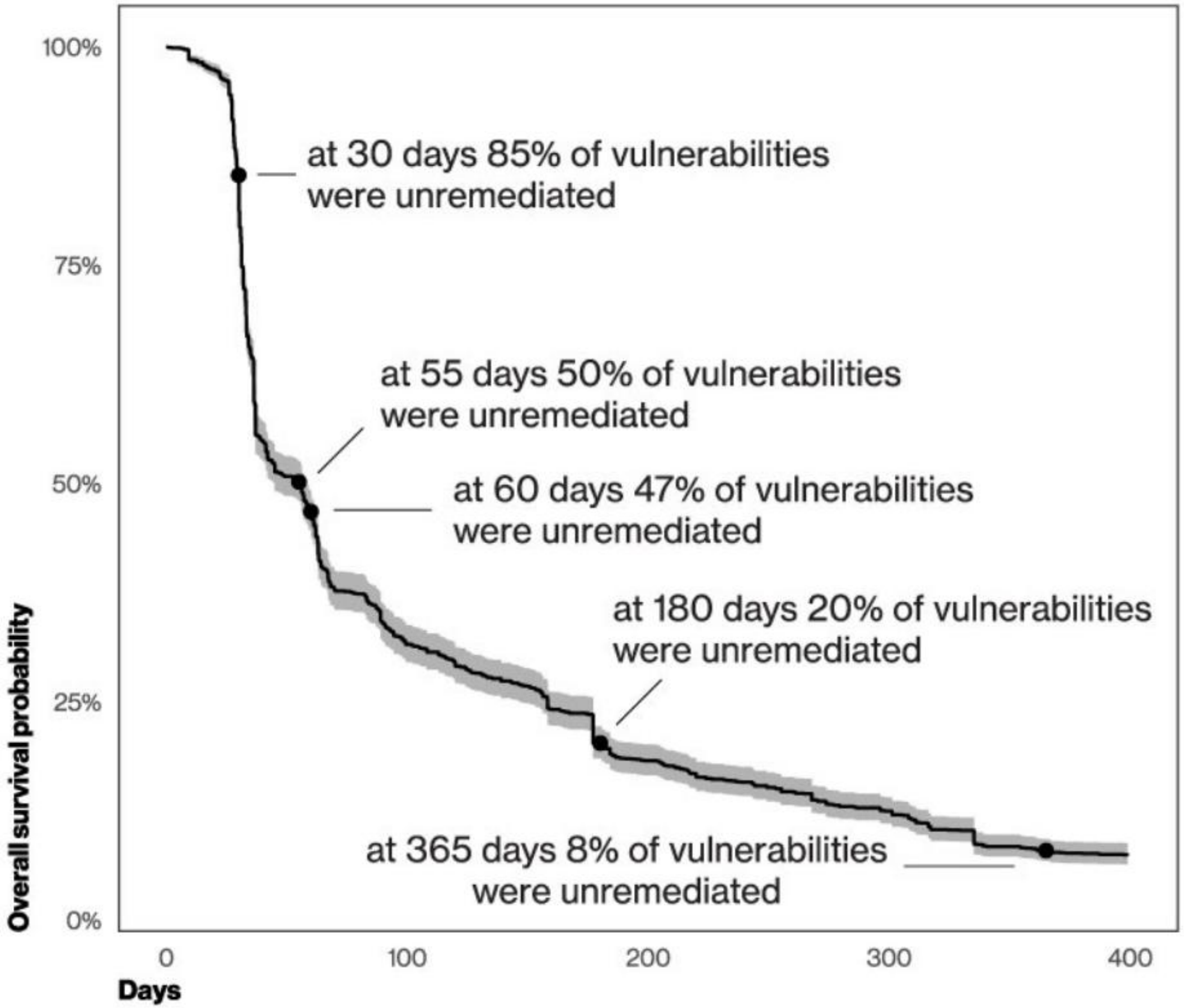
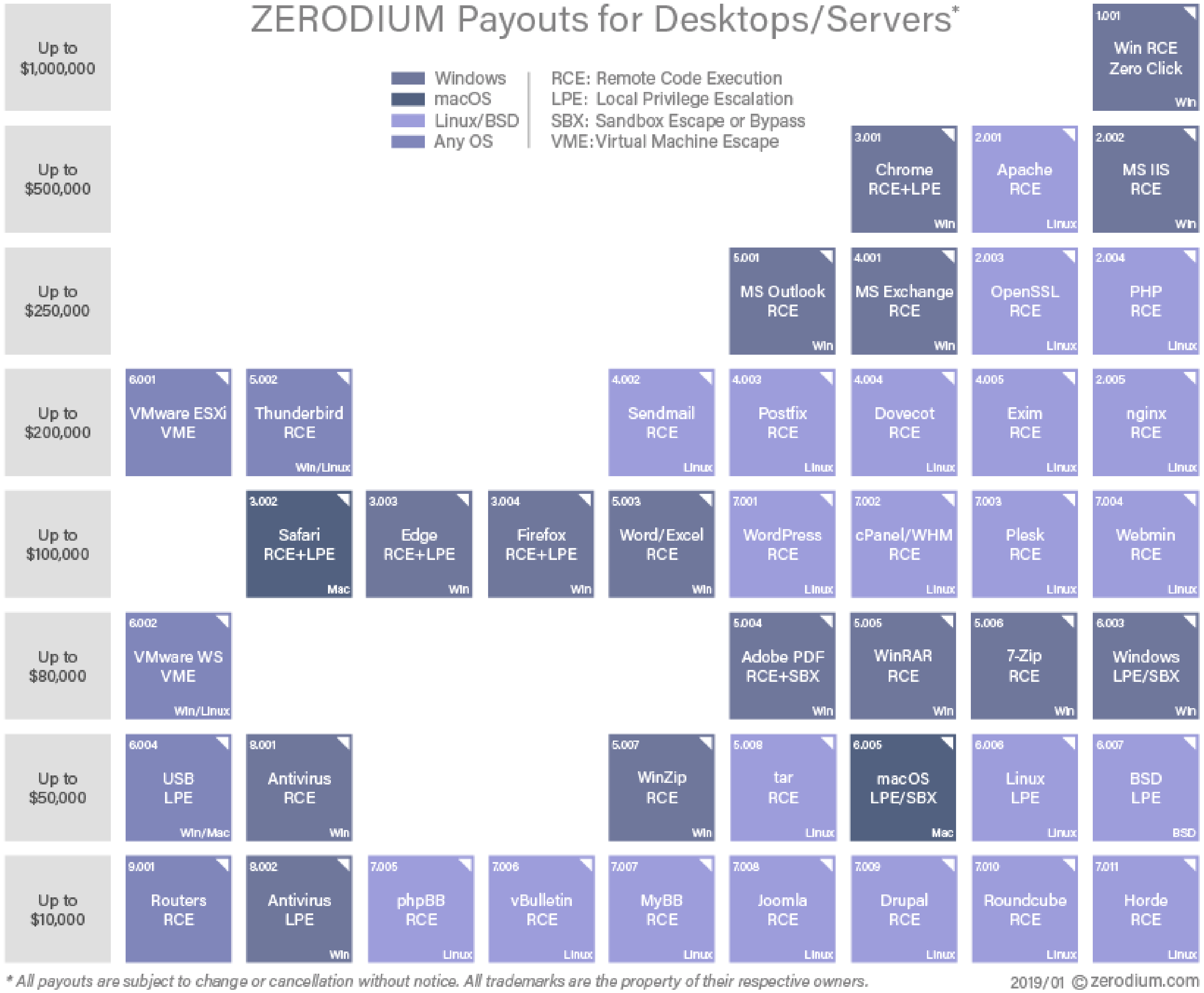


Figure 19. Survival analysis of CISA KEV vulnerabilities

Verizon Data Breach Investigation Report, 2024



ZERODIUM Payouts for Desktops/Servers*

■ Windows
■ macOS
■ Linux/BSD
■ Any OS

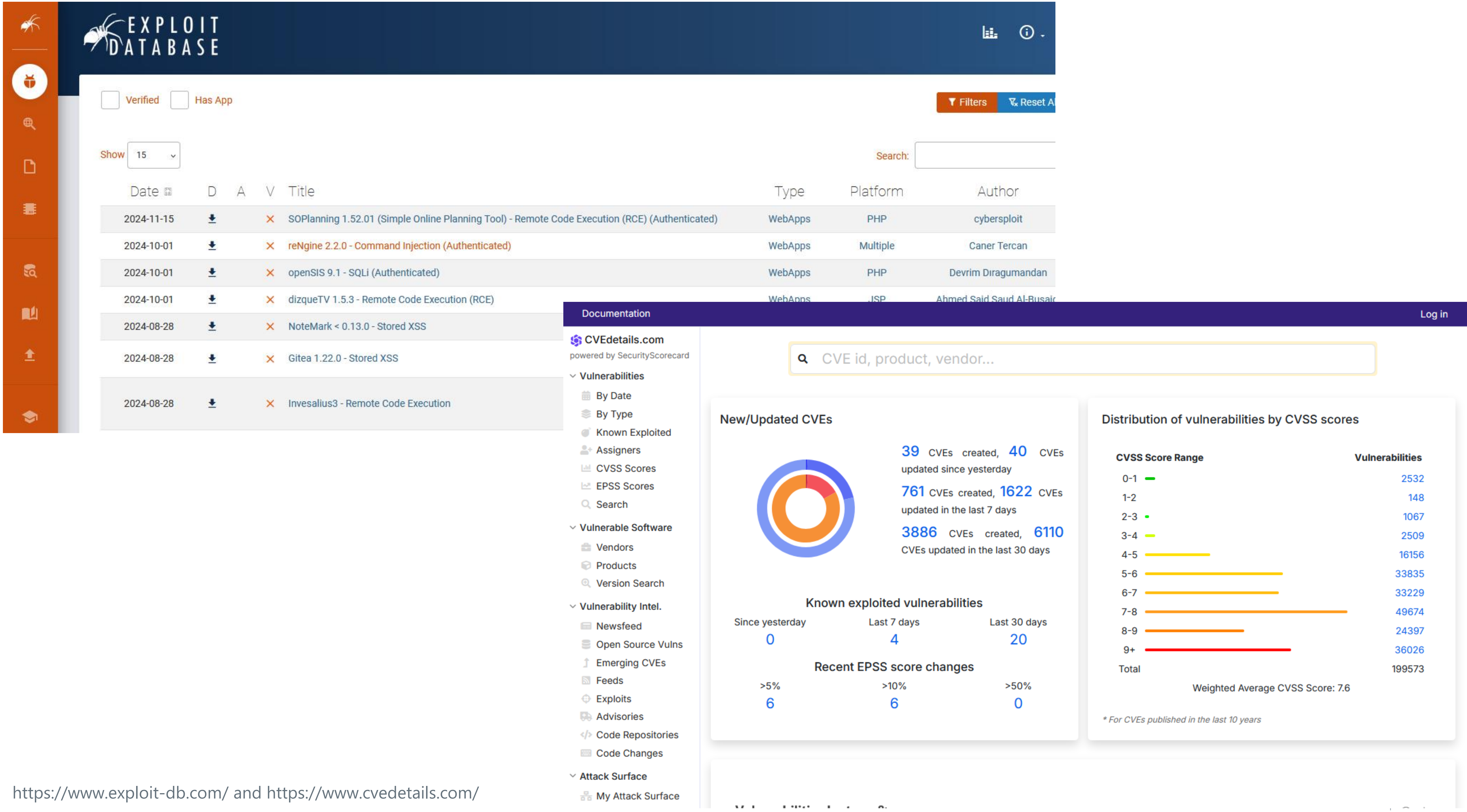
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/01 © zerodium.com

https://zerodium.com/program.html



Date	D	A	V	Title	Type	Platform	Author
2024-11-15	⭳		✕	SOPlanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	cybersploit
2024-10-01	⭳		✕	reNgine 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Caner Tercan
2024-10-01	⭳		✕	openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Dragumandan
2024-10-01	⭳		✕	dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said Saud Al-Busaid
2024-08-28	⭳		✕	NoteMark < 0.13.0 - Stored XSS			
2024-08-28	⭳		✕	Gitea 1.22.0 - Stored XSS			
2024-08-28	⭳		✕	Invesalius3 - Remote Code Execution			

New/Updated CVEs

39 CVEs created, 40 CVEs updated since yesterday

761 CVEs created, 1622 CVEs updated in the last 7 days

3886 CVEs created, 6110 CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
0	4	20

Recent EPSS score changes

>5%	>10%	>50%
6	6	0

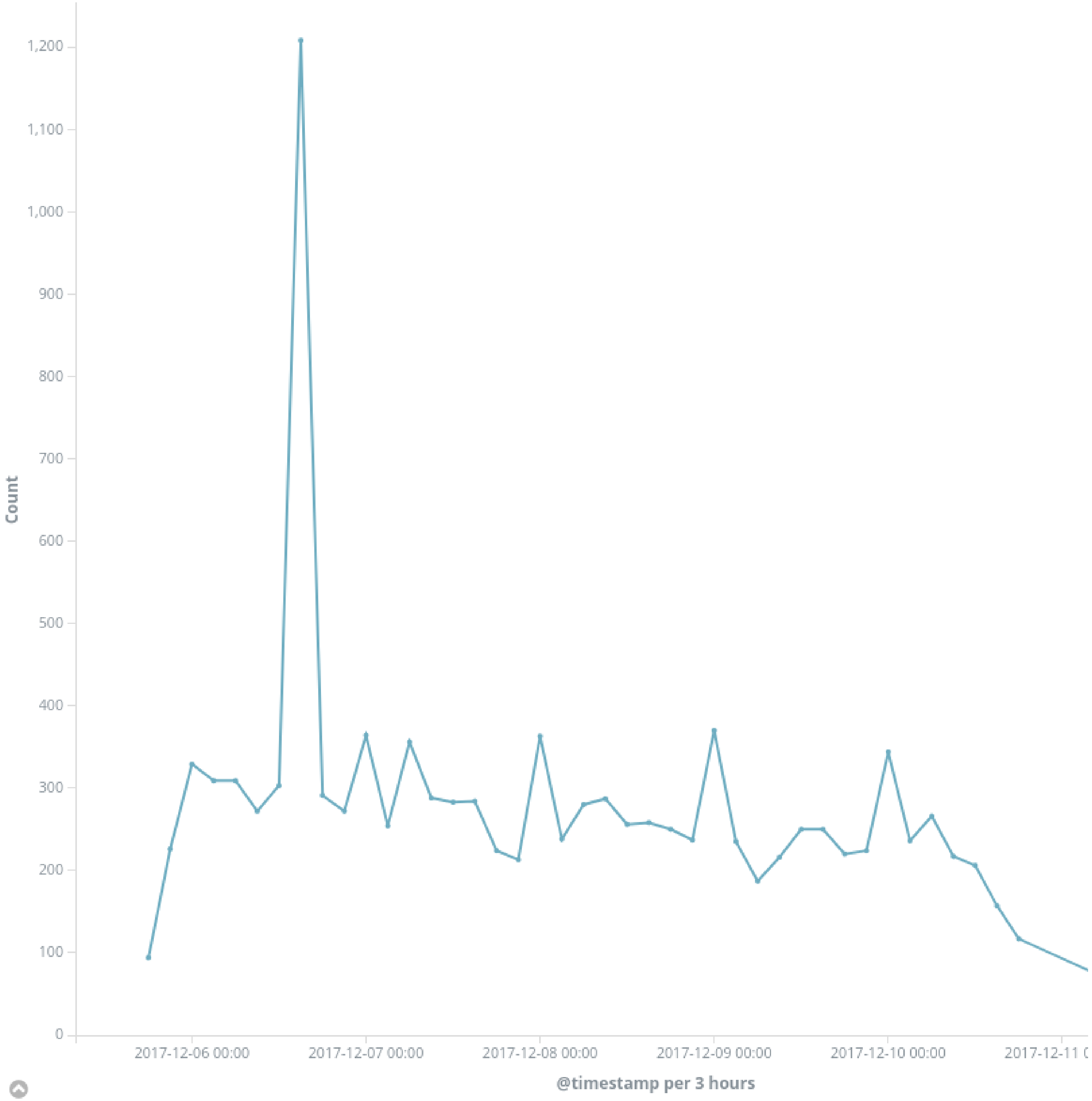
Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	2532
1-2	148
2-3	1067
3-4	2509
4-5	16156
5-6	33835
6-7	33229
7-8	49674
8-9	24397
9+	36026
Total	199573

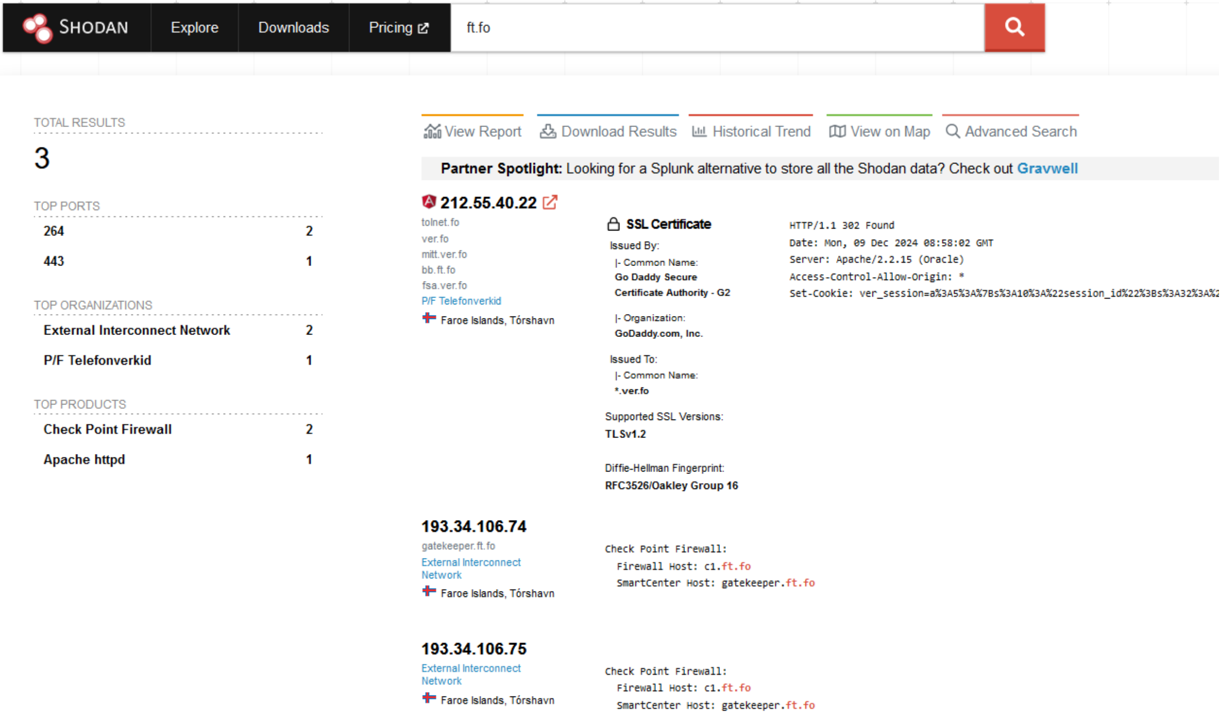
Weighted Average CVSS Score: 7.6

** For CVEs published in the last 10 years*

https://www.exploit-db.com/ and https://www.cvedetails.com/


Count
1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
2017-12-06 00:00
2017-12-07 00:00
2017-12-08 00:00
2017-12-09 00:00
2017-12-10 00:00
2017-12-11 0
@timestamp per 3 hours

Try this: ***https://www.shodan.io/search?query=has_screenshot%3Atrue+encrypted+attention***



TOTAL RESULTS

3

TOP PORTS

264	2
443	1

TOP ORGANIZATIONS

External Interconnect Network	2
P/F Telefonverkid	1

TOP PRODUCTS

Check Point Firewall	2
Apache httpd	1

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out **Gravwell**

212.55.40.22

tolnet.fo
ver.fo
mitt.ver.fo
bb.ft.fo
fsa.ver.fo
P/F Telefonverkid
Faroe Islands, Tórshavn

SSL Certificate

Issued By:
|- Common Name:
Go Daddy Secure Certificate Authority - G2

|- Organization:
GoDaddy.com, Inc.

Issued To:
|- Common Name:
***.ver.fo**

Supported SSL Versions:
TLSv1.2

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 16

```
HTTP/1.1 302 Found
Date: Mon, 09 Dec 2024 08:58:02 GMT
Server: Apache/2.2.15 (Oracle)
Access-Control-Allow-Origin: *
Set-Cookie: ver_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%2
```

193.34.106.74

gatekeeper.ft.fo
External Interconnect Network
Faroe Islands, Tórshavn

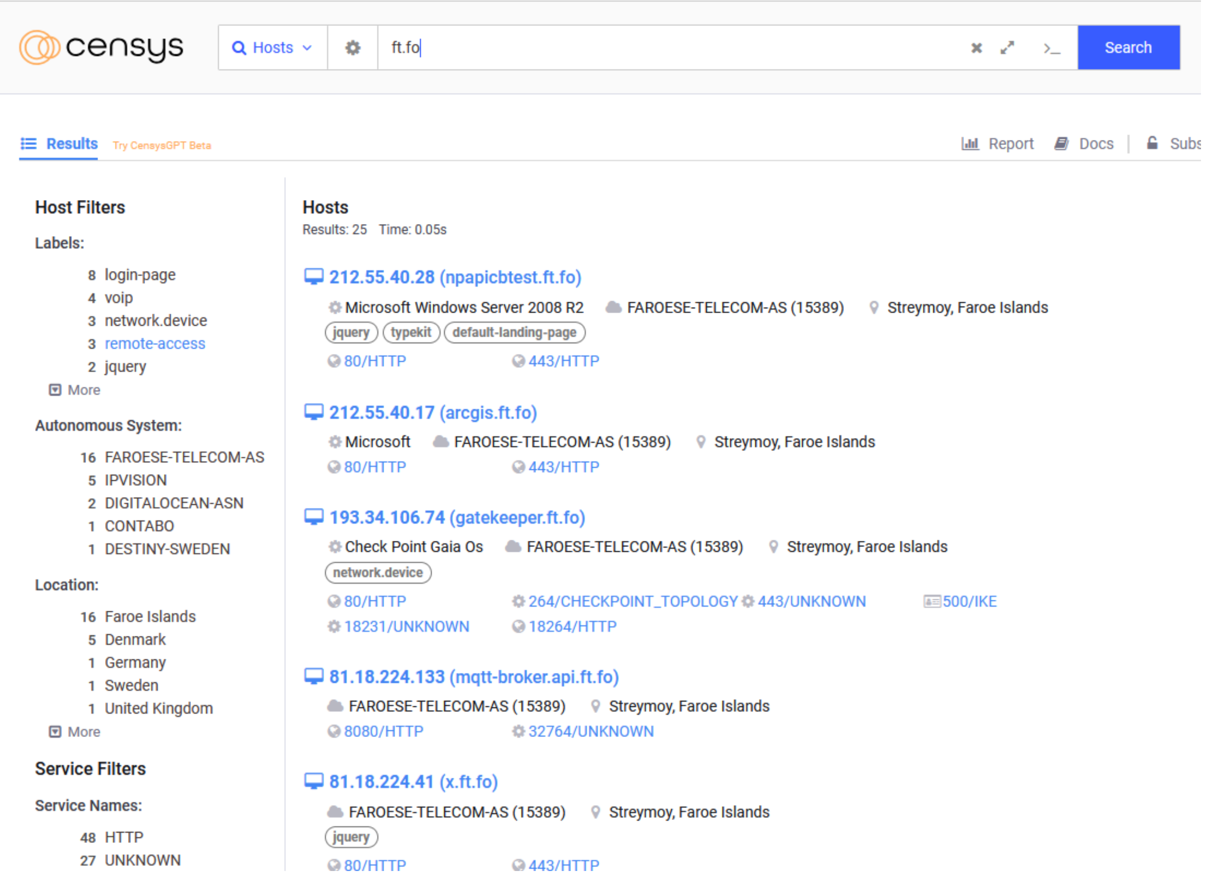
```
Check Point Firewall:
  Firewall Host: c1.ft.fo
  SmartCenter Host: gatekeeper.ft.fo
```

193.34.106.75

External Interconnect Network
Faroe Islands, Tórshavn

```
Check Point Firewall:
  Firewall Host: c1.ft.fo
  SmartCenter Host: gatekeeper.ft.fo
```

https://www.shodan.io/search?query=ft.fo



Host Filters

Labels:

8	login-page
4	voip
3	network.device
3	remote-access
2	jquery

More

Autonomous System:

16	FAROESE-TELECOM-AS
5	IPVISION
2	DIGITALOCEAN-ASN
1	CONTABO
1	DESTINY-SWEDEN

Location:

16	Faroe Islands
5	Denmark
1	Germany
1	Sweden
1	United Kingdom

More

Service Filters

Service Names:

48	HTTP
27	UNKNOWN

Hosts

Results: 25 Time: 0.05s

212.55.40.28 (npapicbtest.ft.fo)
Microsoft Windows Server 2008 R2 · FAROESE-TELECOM-AS (15389) · Streymoy, Faroe Islands
jquery · typekit · default-landing-page
80/HTTP · 443/HTTP

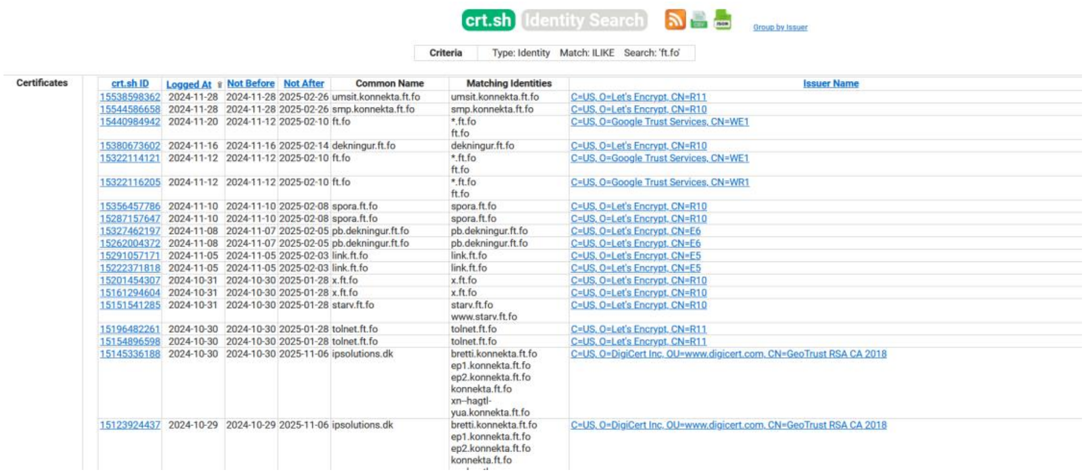
212.55.40.17 (arcgis.ft.fo)
Microsoft · FAROESE-TELECOM-AS (15389) · Streymoy, Faroe Islands
80/HTTP · 443/HTTP

193.34.106.74 (gatekeeper.ft.fo)
Check Point Gaia Os · FAROESE-TELECOM-AS (15389) · Streymoy, Faroe Islands
network.device
80/HTTP · 264/CHECKPOINT_TOPOLOGY · 443/UNKNOWN · 500/IKE
18231/UNKNOWN · 18264/HTTP

81.18.224.133 (mqtt-broker.api.ft.fo)
FAROESE-TELECOM-AS (15389) · Streymoy, Faroe Islands
8080/HTTP · 32764/UNKNOWN

81.18.224.41 (x.ft.fo)
FAROESE-TELECOM-AS (15389) · Streymoy, Faroe Islands
jquery
80/HTTP · 443/HTTP

https://search.censys.io/search?resource=hosts&q=ft.fo



Criteria	Type: Identity Match: ILIKE Search: 'ft.fo'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
15538598362	2024-11-28	2024-11-28	2025-02-26	umsit.konnekta.ft.fo	umsit.konnekta.ft.fo	C=US, O=Let's Encrypt, CN=R11
15544586658	2024-11-28	2024-11-28	2025-02-26	smp.konnekta.ft.fo	smp.konnekta.ft.fo	C=US, O=Let's Encrypt, CN=R10
15440984942	2024-11-20	2024-11-12	2025-02-10	ft.fo	*.ft.fo ft.fo	C=US, O=Google Trust Services, CN=WE1
15380673602	2024-11-16	2024-11-16	2025-02-14	dekningur.ft.fo	dekningur.ft.fo	C=US, O=Let's Encrypt, CN=R10
15322114121	2024-11-12	2024-11-12	2025-02-10	ft.fo	*.ft.fo ft.fo	C=US, O=Google Trust Services, CN=WE1
15322116205	2024-11-12	2024-11-12	2025-02-10	ft.fo	*.ft.fo ft.fo	C=US, O=Google Trust Services, CN=WR1
15356457786	2024-11-10	2024-11-10	2025-02-08	spora.ft.fo	spora.ft.fo	C=US, O=Let's Encrypt, CN=R10
15287157647	2024-11-10	2024-11-10	2025-02-08	spora.ft.fo	spora.ft.fo	C=US, O=Let's Encrypt, CN=R10
15327462197	2024-11-08	2024-11-07	2025-02-05	pb.dekningur.ft.fo	pb.dekningur.ft.fo	C=US, O=Let's Encrypt, CN=E6
15262004372	2024-11-08	2024-11-07	2025-02-05	pb.dekningur.ft.fo	pb.dekningur.ft.fo	C=US, O=Let's Encrypt, CN=E6
15291057171	2024-11-05	2024-11-05	2025-02-03	link.ft.fo	link.ft.fo	C=US, O=Let's Encrypt, CN=E5
15222371818	2024-11-05	2024-11-05	2025-02-03	link.ft.fo	link.ft.fo	C=US, O=Let's Encrypt, CN=E5
15201454307	2024-10-31	2024-10-30	2025-01-28	x.ft.fo	x.ft.fo	C=US, O=Let's Encrypt, CN=R10
15161294604	2024-10-31	2024-10-30	2025-01-28	x.ft.fo	x.ft.fo	C=US, O=Let's Encrypt, CN=R10
15151541285	2024-10-31	2024-10-30	2025-01-28	starv.ft.fo	starv.ft.fo www.starv.ft.fo	C=US, O=Let's Encrypt, CN=R10
15196482261	2024-10-30	2024-10-30	2025-01-28	tolnet.ft.fo	tolnet.ft.fo	C=US, O=Let's Encrypt, CN=R11
15154896598	2024-10-30	2024-10-30	2025-01-28	tolnet.ft.fo	tolnet.ft.fo	C=US, O=Let's Encrypt, CN=R11
15145336188	2024-10-30	2024-10-30	2025-11-06	ipsolutions.dk	bretti.konnekta.ft.fo ep1.konnekta.ft.fo ep2.konnekta.ft.fo konnekta.ft.fo xn--hagtl-yua.konnekta.ft.fo	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
15123924437	2024-10-29	2024-10-29	2025-11-06	ipsolutions.dk	bretti.konnekta.ft.fo ep1.konnekta.ft.fo ep2.konnekta.ft.fo konnekta.ft.fo	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018

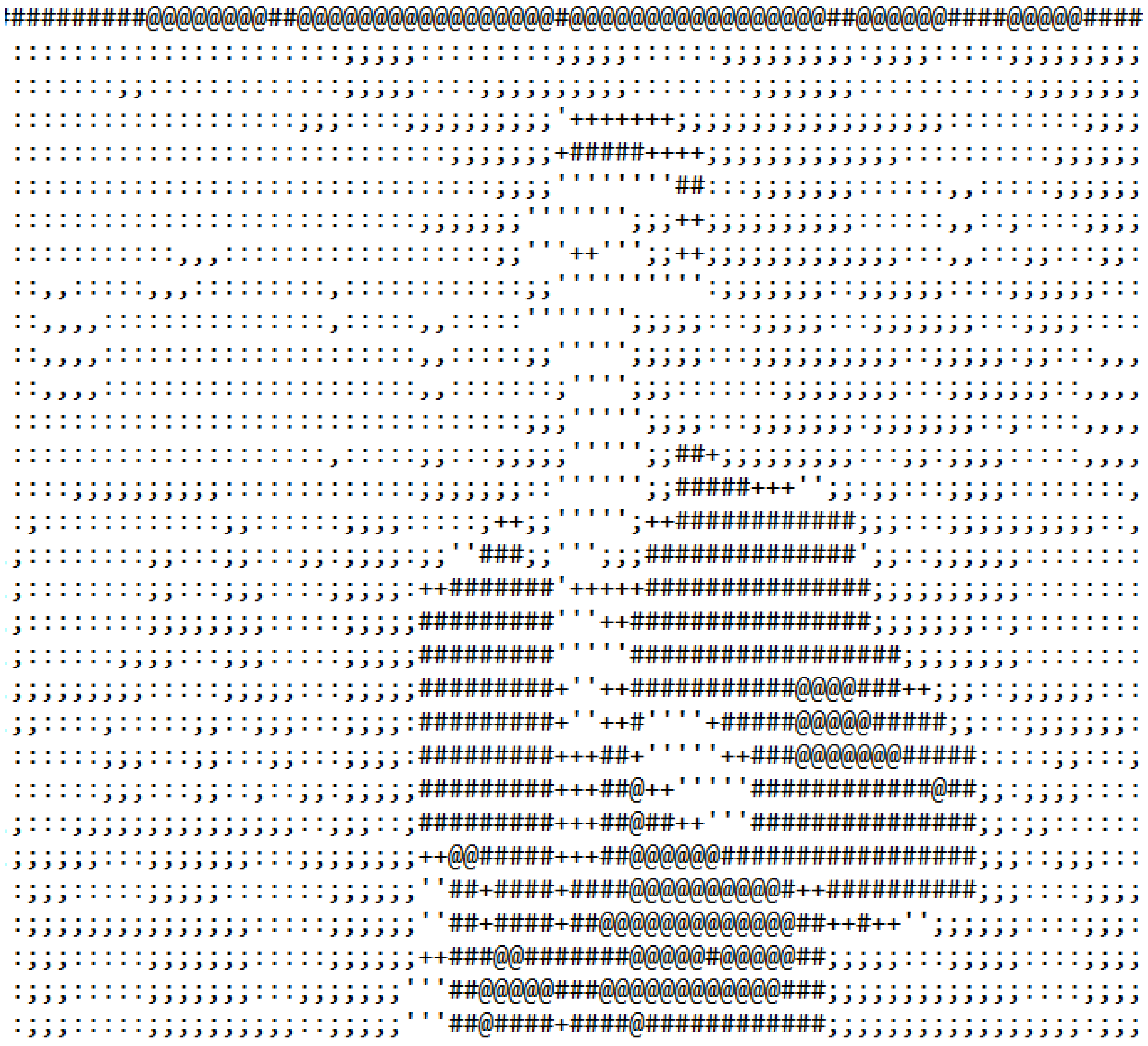
https://crt.sh/?q=ft.fo

Demo

Behind the scenes

I am never going to give you up!

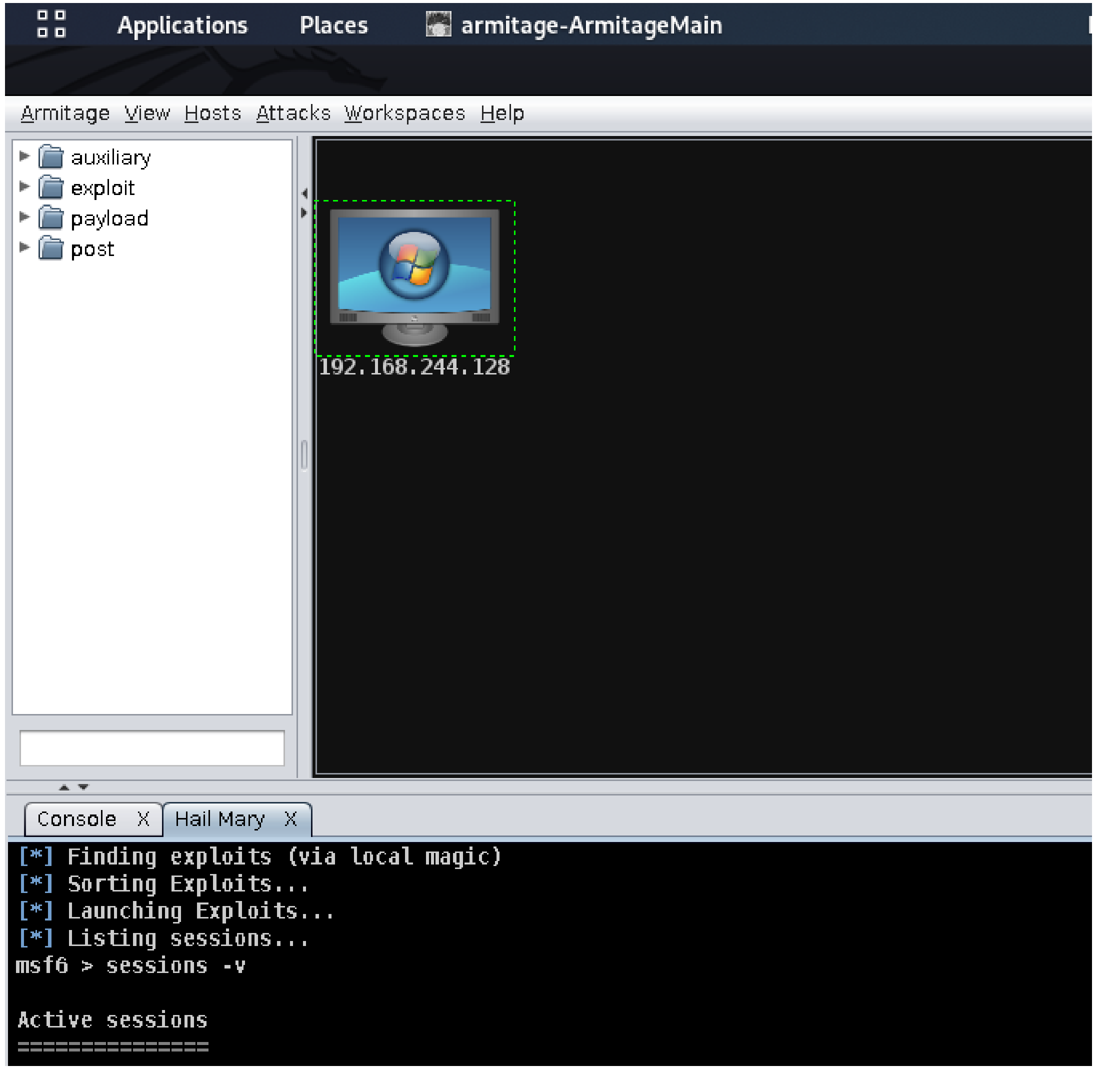
Eternalblue and Doublepulsar and Armitage



Demo

It is not going to get easier!

Armitage – Hacking like you do not know what you are doing!



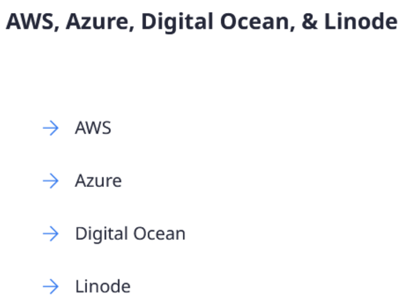
```
[*] Finding exploits (via local magic)
[*] Sorting Exploits...
[*] Launching Exploits...
[*] Listing sessions...
msf6 > sessions -v

Active sessions
===============
```

Thought Experiment

.... Okay, it may actually be even easier....

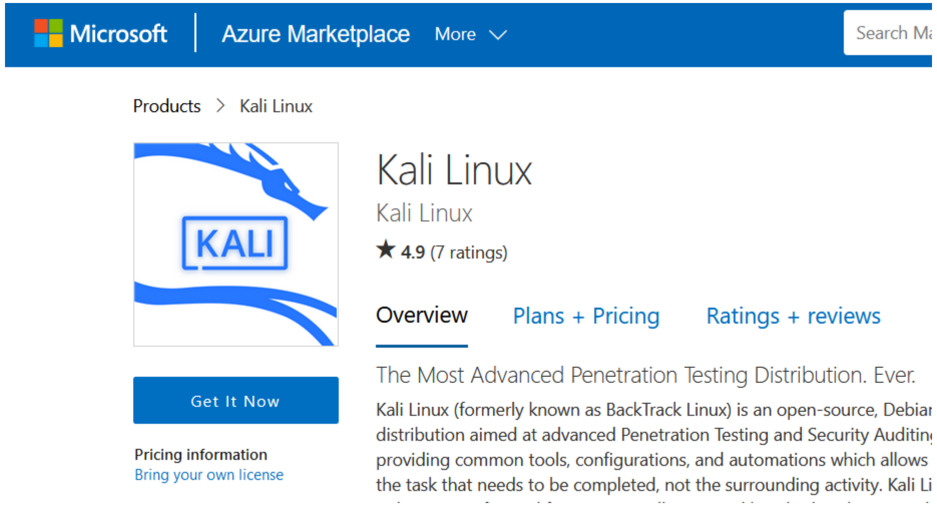
Hacking like you do not know what you are doing (and really you do not)



AWS, Azure, Digital Ocean, & Linode

- AWS
- Azure
- Digital Ocean
- Linode

https://www.kali.org/docs/cloud/



Kali Linux

Kali Linux

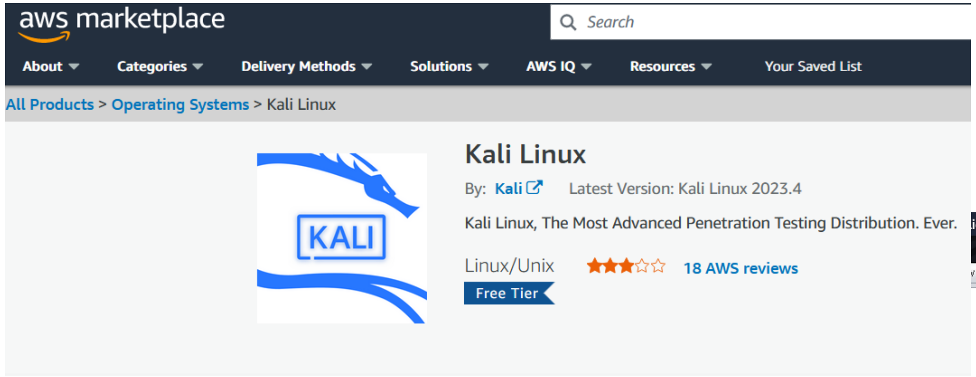
★ 4.9 (7 ratings)

The Most Advanced Penetration Testing Distribution. Ever.

Kali Linux (formerly known as BackTrack Linux) is an open-source, Debiar distribution aimed at advanced Penetration Testing and Security Auditin providing common tools, configurations, and automations which allows the task that needs to be completed, not the surrounding activity. Kali Li

Pricing information
Bring your own license

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/kali-linux.kali



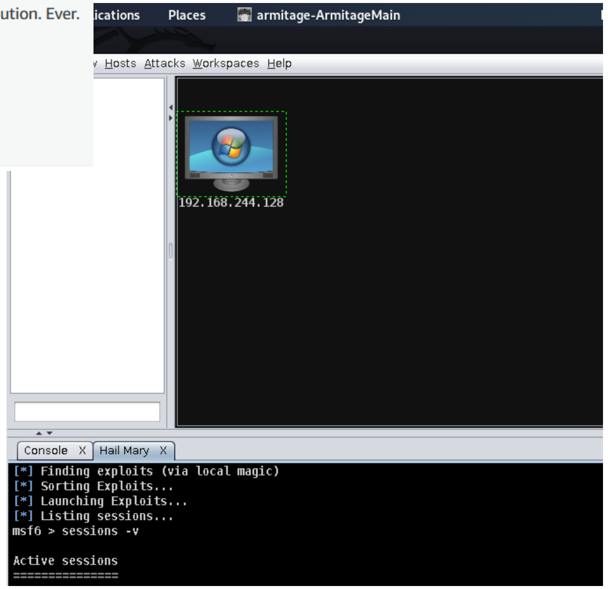
Kali Linux

By: Kali   Latest Version: Kali Linux 2023.4

Kali Linux, The Most Advanced Penetration Testing Distribution. Ever.

Linux/Unix ★★★☆☆ 18 AWS reviews

https://aws.amazon.com/marketplace/pp/prodview-fznsw3f7mq7to



```
[*] Finding exploits (via local magic)
[*] Sorting Exploits...
[*] Launching Exploits...
[*] Listing sessions...
msf6 > sessions -v

Active sessions
===============
```

WelcomeSecurity
Enabling value through IT security

Thanks!

Thomas Ljungberg Kristensen

www.welcomesecurity.net

+45 2158 1410
thomas@welcomesecurity.net