

ATTACK ORIGINS

#	Country
365	China
244	South Korea
138	United States
26	Canada
23	Mil/Gov
22	Hong Kong
18	Netherlands
14	Russia
12	India
9	Colombia

ATTACK TARGETS

#	Country
840	United States
26	Hong Kong
13	Canada
10	Portugal
10	Thailand
7	Russia
6	Austria
5	Netherlands
5	France
4	Germany

ATTACKS

ATTACK TYPES

Timestamp

Attacker

Target

Type

Organization	Location	IP	Location	Service	Port
Norse Corporation	Kirkville, United States	205.251.21.40	Mountain View, United States	unknown	62180
Telstra Internet	Laverton, Australia	203.45.44.113	Seattle, United States	microsoft-ds	445
SunnyVision Limited	unknown, Hong Kong	124.248.211.81	unknown, Hong Kong	CrazyNet	17500
Gemzo Information	unknown, Palestinian	178.215.217.53	Kirkville, United States	telnet	23
CHTD, Chunghwa Telecom	unknown, Taiwan	1.162.30.193	Saint Louis, United States	unknown	58455
Norse Corporation	Kirkville, United States	205.251.21.40	Mountain View, United States	unknown	59616
N/A	unknown, Mil/Gov	103.224.165.47	Perth, Australia	vnc	5900
ChinaNet Guangdong	Guangzhou, China	183.9.154.50	Saint Louis, United States	telnet	23

#

Service

Port

482	ssh	22
98	telnet	23
34	http	80
34	domain	53
31	netbios-ns	137
27	netbios-dgm	138
25	microsoft-ds	445
22	CrazyNet	17500

Nessus Network Scan Summary

Switch Dashboard

Options

Nessus Network Scan Summary - Last Scanned Observed in 14 Days

IP Address	Total
10.3.1.1	18
192.168.1.1	3
10.3.1.104	1
10.3.1.104.0/24	1

Nessus Network Scan Summary - Last Scanned Observed between 15 to 30 Days

IP Address	Total
10.3.1.1	1
10.3.1.104.0/24	1

Nessus Scan Summary

Switch Dashboard

Options

Nessus Scan Summary - Nessus Scan Time

	Percentage of Total Scans Conducted
2 Minutes or Less	31%
Over 2 Minutes to 5 Minutes	9%
Over 5 Minutes to 10 Minutes	4%
10 Minutes or More	3%

Last Updated: 48 minutes ago

Nessus Scan Summary - Credentialed Checks

	Credentialed Acco...	Total Count per Cr...	Total Credential Sc...
Administrator	0%	0	42
root	7%	3	42
Admin	0%	0	42
via SMB	5%	2	42
via SSH	7%	3	42
Local Host	21%	9	42
SNMP	0%	0	42
No Account Name	67%	28	42

Last Updated: 48 minutes ago

Nessus Scan Summary - Scan Problems

	Host Count	% Affected
Total Systems Scanned	67	
Authentication Failure	123	65%
Scan Not Performed with...	115	63%
Cannot Access the Windo...	10	13%
Linux Elevated Privileges ...	0	0%

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Scanner Version

	>6.7.1	6.7.0	6.6.2	6.6.1	6.6.0	6.5.6	<6.0.0
Scanner...	0	31	21	0	2	1	3

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Agent Status

	Hosts	Ratio
Windows Agent	27	40%
Unix Agent	8	12%
Nessus in NSX	0	0%
Normal	29	43%
Type Undetermined	0	0%
Total	67	N/A

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Scan Options Status

	Enabled/Yes	Disabled/No	Total Scans
Thorough Tests	0%	100%	67
Experimental Tests	0%	100%	67
Safe Checks	100%	0%	67
Optimize the Tests	100%	0%	67
Credentialed Checks	63%	37%	67
Patch Mgmt. Chec...	0%	100%	67
CGI Scanning	3%	97%	67

Last Updated: 48 minutes ago

Nessus Scan Summary - Web App Tests

	Enabled/Yes	Disabled/No	Total Web App Tes...
Web App Tests - T...	50%	0%	2
Try all HTTP Metho...	0%	100%	2
Stop at First Flaw	50%	0%	2

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Port Scanner Types

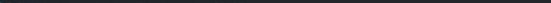
	WMI NET...	SYN Sc...	NETSTAT...	TCP Scan...	SNMP Sc...	Total Port...
Port Scan...	33%	33%	33%	0%	0%	9

Last Updated: 49 minutes ago

Nessus Scan Summary - Nessus Scanner Errors

IP Address	MAC Addr...	D...	NetBI...	Last Obser...
10.3.1.1	ff:ff:ff:ff:ff:ff	dc...	MELC...	59 minutes ...
10.3.1.1	ff:ff:ff:ff:ff:ff	xe...		59 minutes ...
10.3.1.1	ff:ff:ff:ff:ff:ff	xe...		59 minutes ...
10.3.1.1	ff:ff:ff:ff:ff:ff	ac...		59 minutes ...
10.3.1.1	ff:ff:ff:ff:ff:ff	sc...		59 minutes ...

Last Updated: Less than a minute ago



A terminal window titled "CyberRecon - python - python scan.py - 92x25". The prompt is "christianbutler@Christians-MacBook-Pro-7 CyberRecon %". The command entered is "python scan.py".

CyberRecon Interactive Scan Processor

Welcome! This tool will guide you through processing a Nessus scan.

Step 1: Select Nessus File

Opening file picker...

- Selected File
- File Size

Scan Processing Options

VERBOSE MODE

```
Shows detailed progress and
Enable verbose output? [y/N]
```

```
christianbutler@Christians-MacBook-Pro-7 CyberRecon % python update_map.py
```

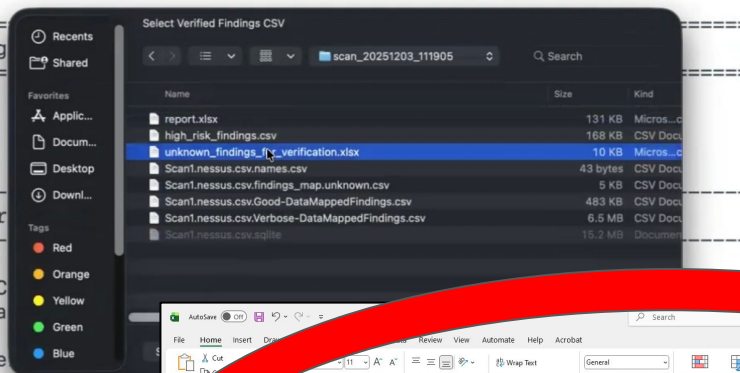
CyberRecon Finding

This tool updates

Step 1: Select Ver

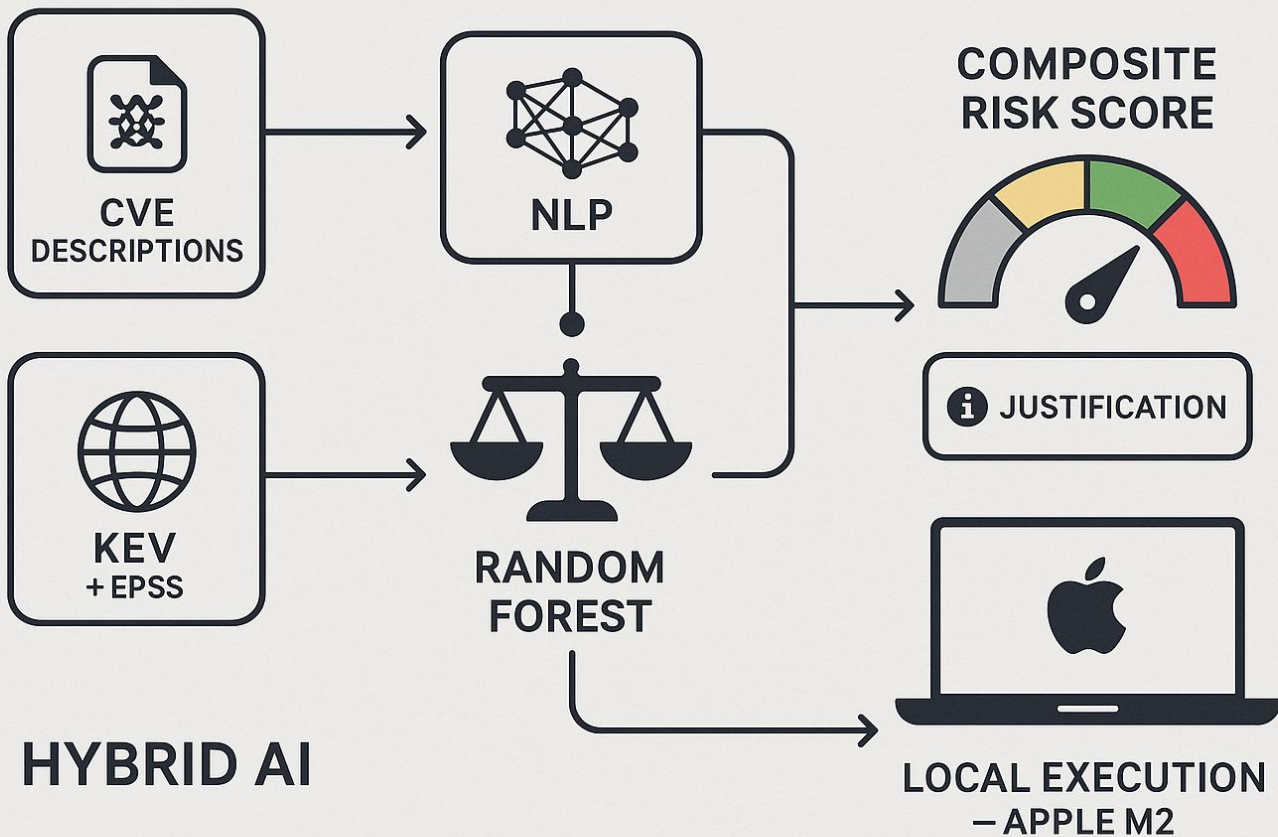
This should be a C
(Usually created a

Opening file picke

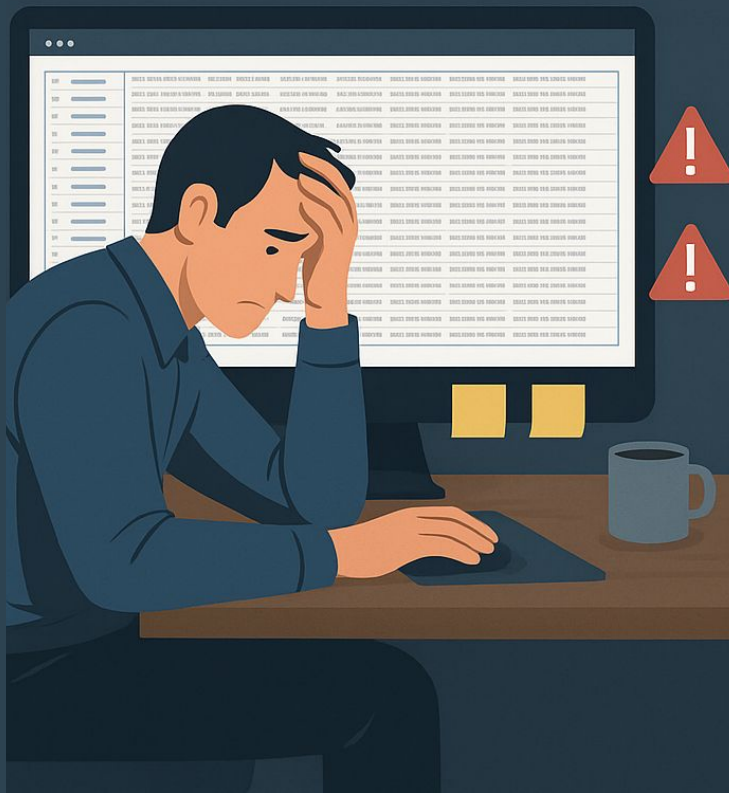


The screenshot shows a Microsoft Excel spreadsheet with a table of findings. A large red circle highlights a section of the table, specifically rows 4 through 10. The table has the following columns: Finding#, Findings(PluginID), MapName, HV_Severity, HV_Notes, HV_Status, Exploitable, ReportItem, Severity, CVE, VSS, Con, Servation, Reporting, Links, Fomks, Checkin, Resear, and T. The highlighted section contains rows 4 through 10, showing findings related to 'AI predicts' and 'Proof-of-concept code found'.

Finding#	Findings(PluginID)	MapName	HV_Severity	HV_Notes	HV_Status	Exploitable	ReportItem	Severity	CVE	VSS	Con	Servation	Reporting	Links	Fomks	Checkin	Resear	T
4			2-Medium	AI predicts: 2-Medium (confidence: 0.77) Proof-of-concept code found o Yes	None	Report				3.6	The versic	Version sc	1	1	[OK]			
5			2-Medium	AI predicts: 2-Medium (confidence: 0.77) Proof-of-concept code found o Yes	None	Report				3.6	The versic							
6			2-Medium	AI predicts: 2-Medium (confidence: 0.77) Proof-of-concept code found o Yes	None	Report				3.6	The versic							
7			2-Medium	AI predicts: 2-Medium (confidence: 0.77) Proof-of-concept code found o Yes	None	Report				3.6	The versic							
8			2-Medium	AI predicts: 2-Medium (confidence: 0.77) Proof-of-concept code found o Yes	None	Report				3.6	The versic							
9			2-Medium	AI predicts: 2-Medium (confidence: 0.77) Proof-of-concept code found o Yes	None	Report				3.6	The versic							
10			1-Low	AI predicts: 1-Low (confidence: 0.80) Proof-of-concept code found on Git Yes	None	Report				8.5	The versic							



BEFORE



AFTER





https://sce.nau.edu/capstone/projects/CS/2025/Cyber%20Recon_S25/