External Attack Surface Management in Red Teaming

Rizwan Syed
@_r12w4n

About Me

Consultant - Cyber Risk Advisory

Certified Red Team Professional - CRTP

Penetration Tester| Offensive Cyber Security Enthusiast

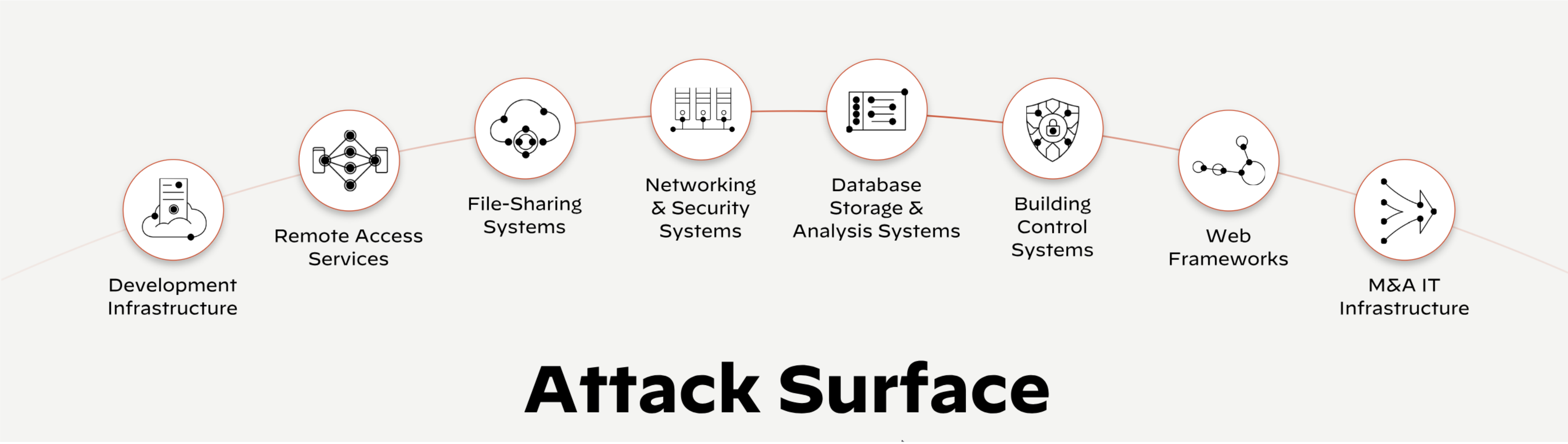
Attack Surface

Attack Surface Monitoring (ASM) refers to the **proactive** and **continuous process** of **identifying** and **assessing** an organization's external-facing assets, vulnerabilities, and potential points of entry for cyber threats.

You can't secure what you don't know.

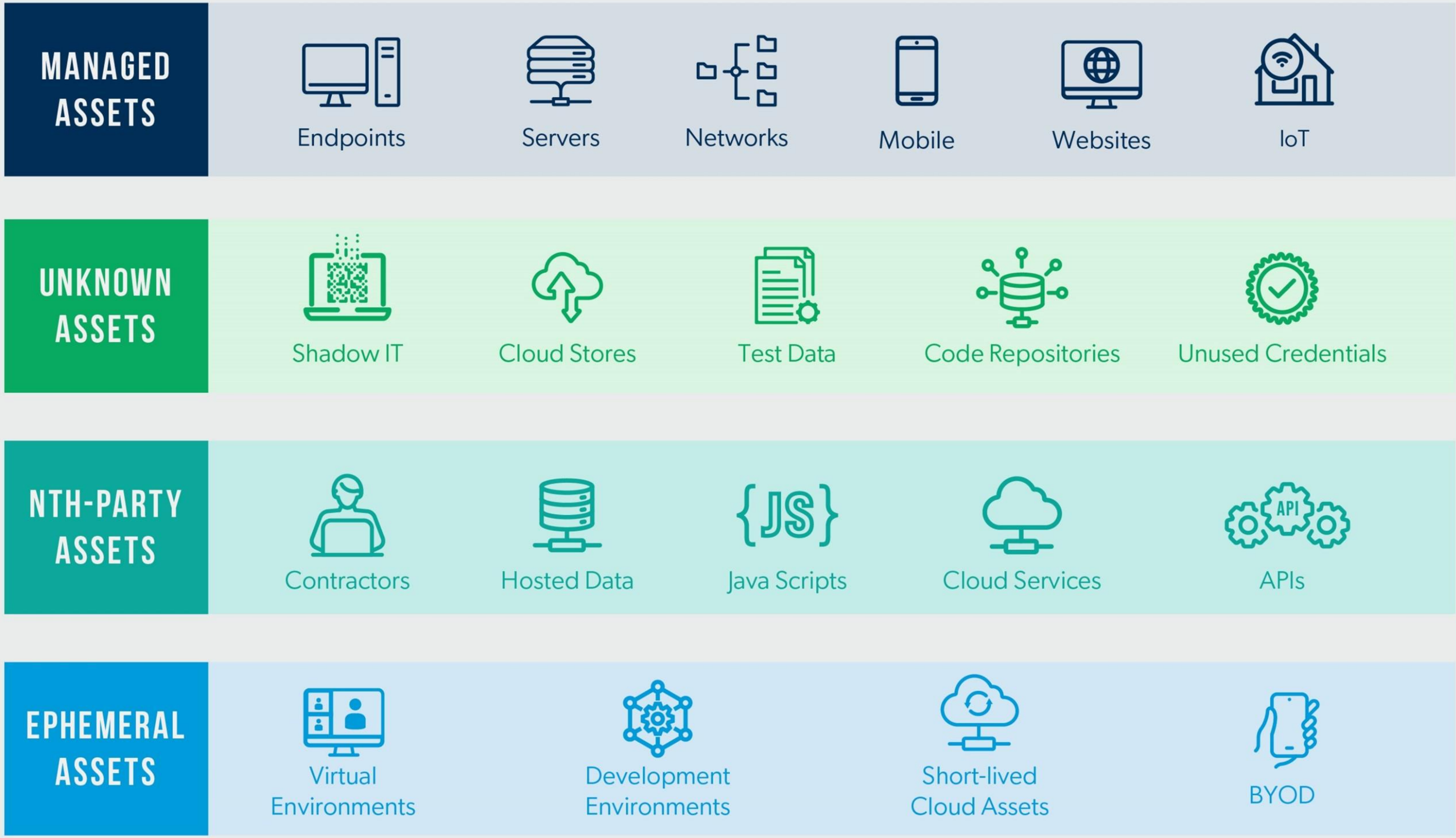
Attack Surface

Attack surface management enables organizations to enhance visibility and mitigate risks associated with their attack surface.



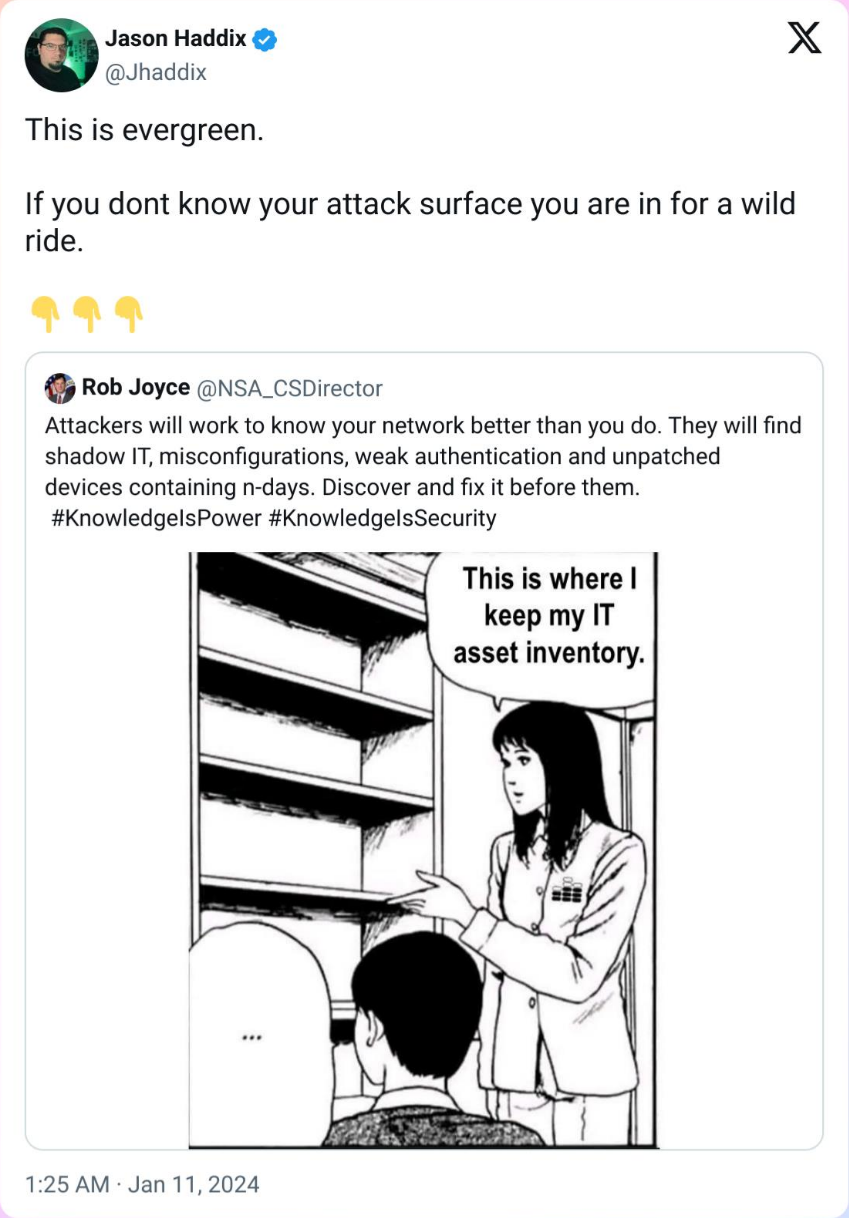
Source: Palo Alto Networks

Attack Surface Layers



MANAGED ASSETS	Endpoints	Servers	Networks	Mobile	Websites	IoT
UNKNOWN ASSETS	Shadow IT	Cloud Stores	Test Data	Code Repositories	Unused Credentials	
NTH-PARTY ASSETS	Contractors	Hosted Data	Java Scripts	Cloud Services	APIs	
EPHEMERAL ASSETS	Virtual Environments	Development Environments	Short-lived Cloud Assets	BYOD		

Source: Aite-Novarica Group



Jason Haddix
@Jhaddix

This is evergreen.

If you dont know your attack surface you are in for a wild ride.

👇👇👇

Rob Joyce @NSA_CSDirector

Attackers will work to know your network better than you do. They will find shadow IT, misconfigurations, weak authentication and unpatched devices containing n-days. Discover and fix it before them. #KnowledgeIsPower #KnowledgeIsSecurity

1:25 AM · Jan 11, 2024

External Attack Surface Management in Red Teaming

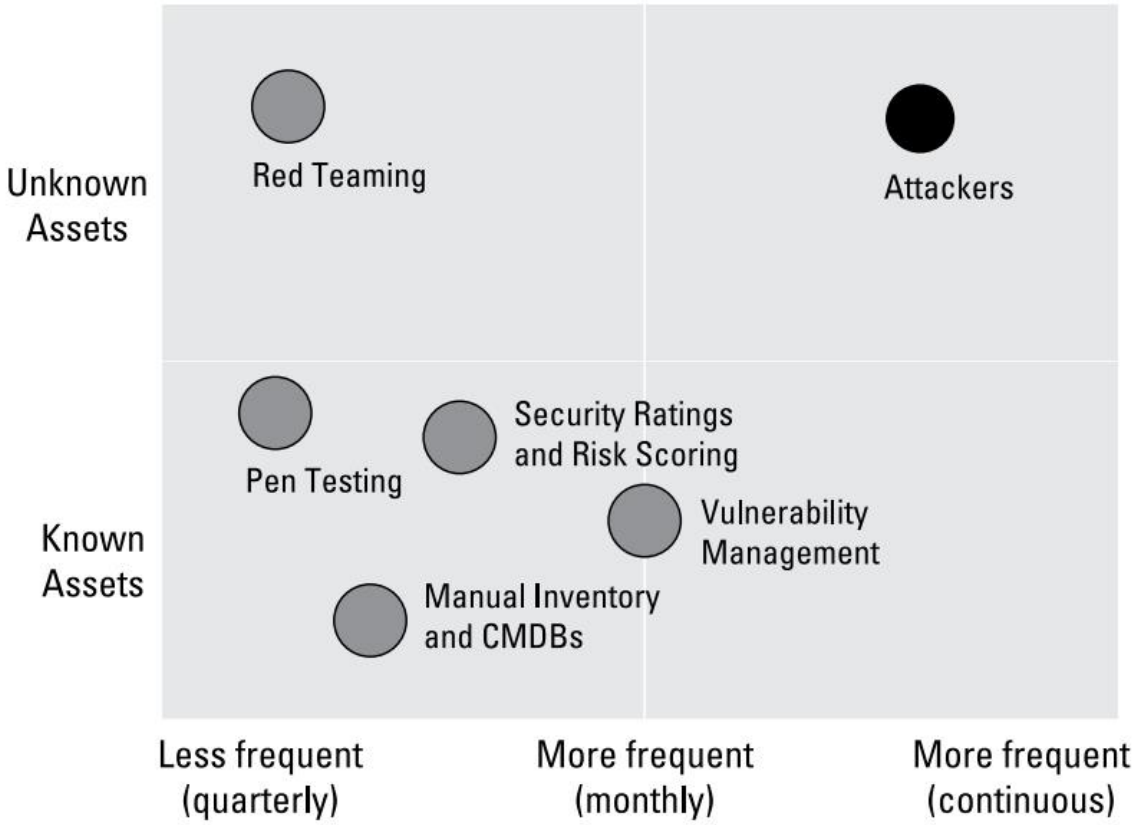
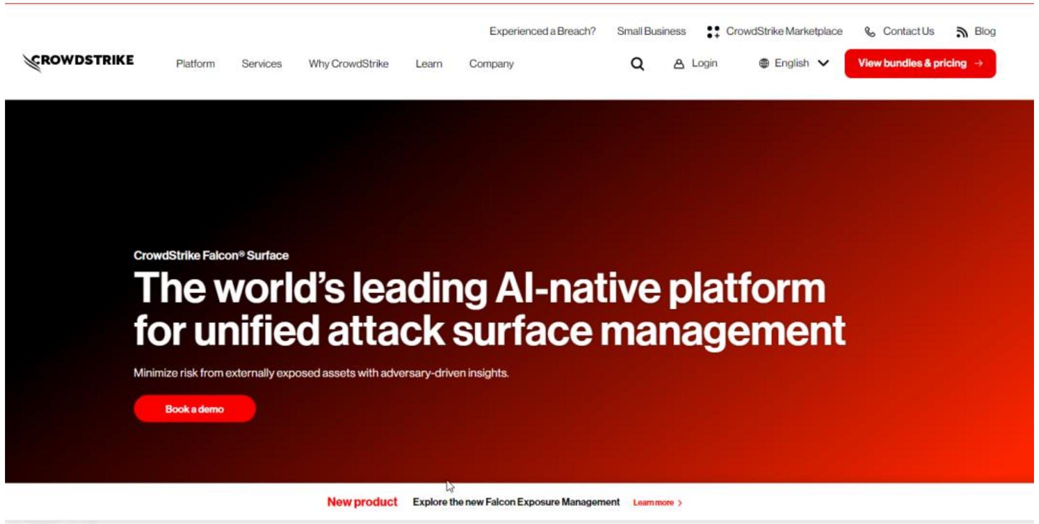


FIGURE 1-2: Attackers have the upper hand compared to traditional technologies and approaches for ASM.

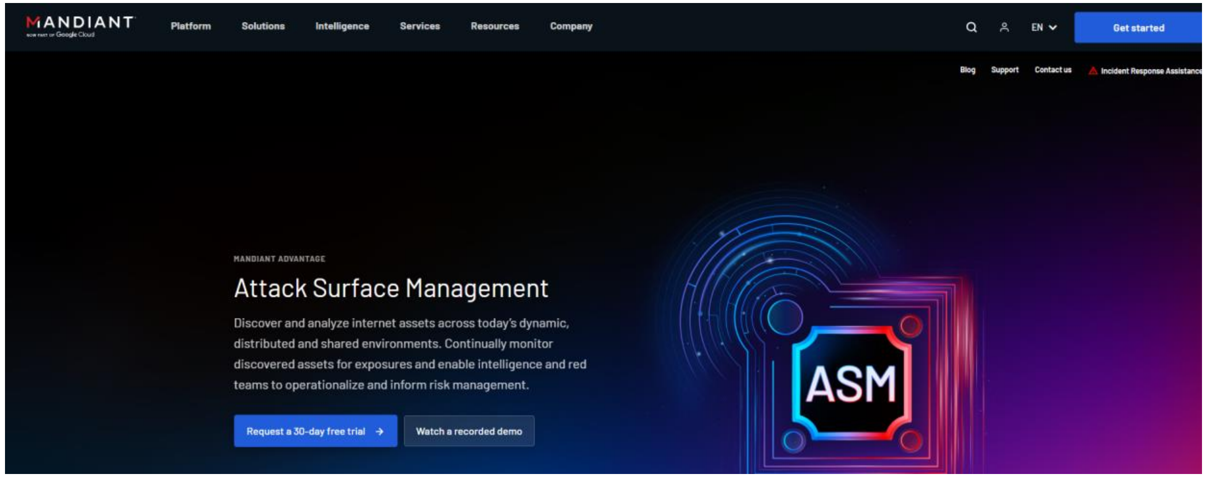


CrowdStrike Falcon® Surface

The world's leading AI-native platform for unified attack surface management

Minimize risk from externally exposed assets with adversary-driven insights.

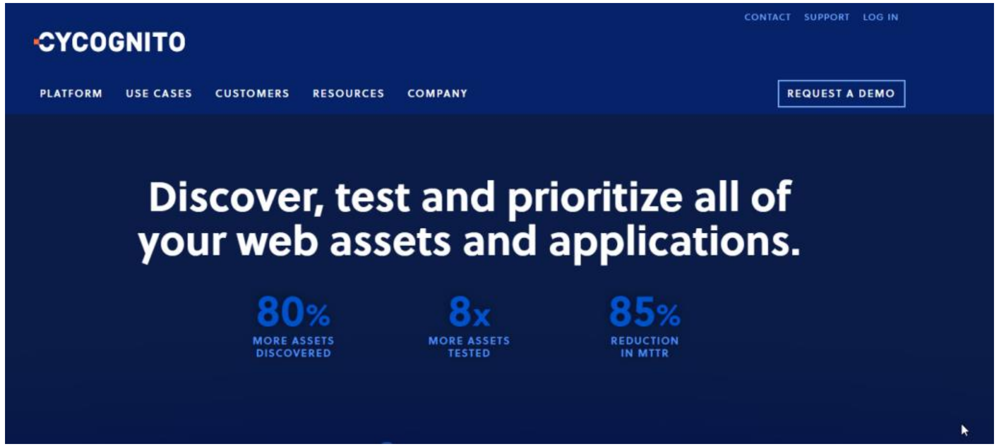
Explore the new Falcon Exposure Management



MANDIANT ADVANTAGE

Attack Surface Management

Discover and analyze internet assets across today's dynamic, distributed and shared environments. Continually monitor discovered assets for exposures and enable intelligence and red teams to operationalize and inform risk management.

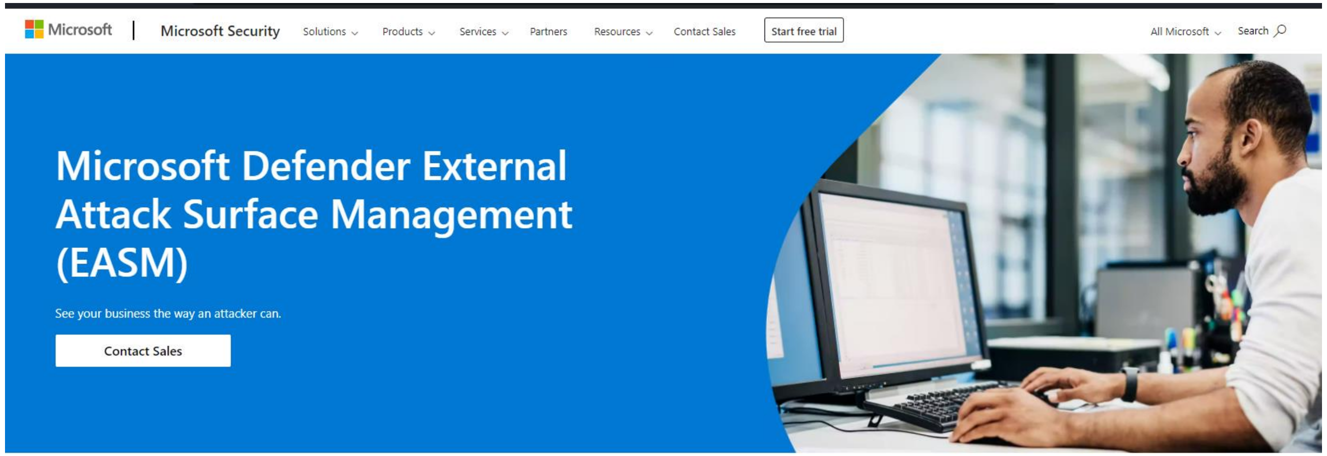


Discover, test and prioritize all of your web assets and applications.

80% MORE ASSETS DISCOVERED

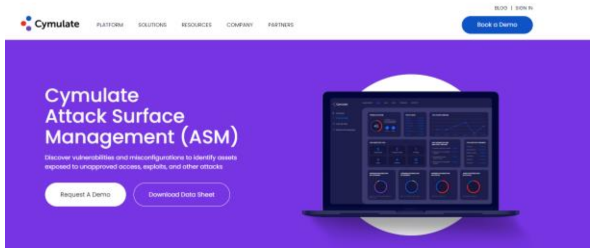
8x MORE ASSETS TESTED

85% REDUCTION IN MTTR



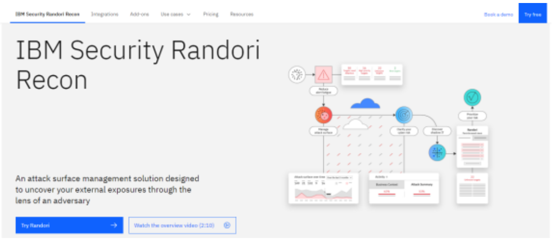
Microsoft Defender External Attack Surface Management (EASM)

See your business the way an attacker can.



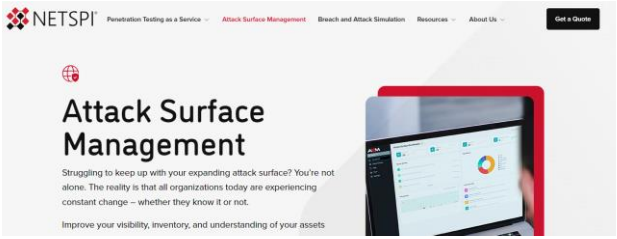
Cymulate Attack Surface Management (ASM)

Discover vulnerabilities and misconfigurations to identify assets exposed to unapproved access, exploits, and other attacks



IBM Security Randori Recon

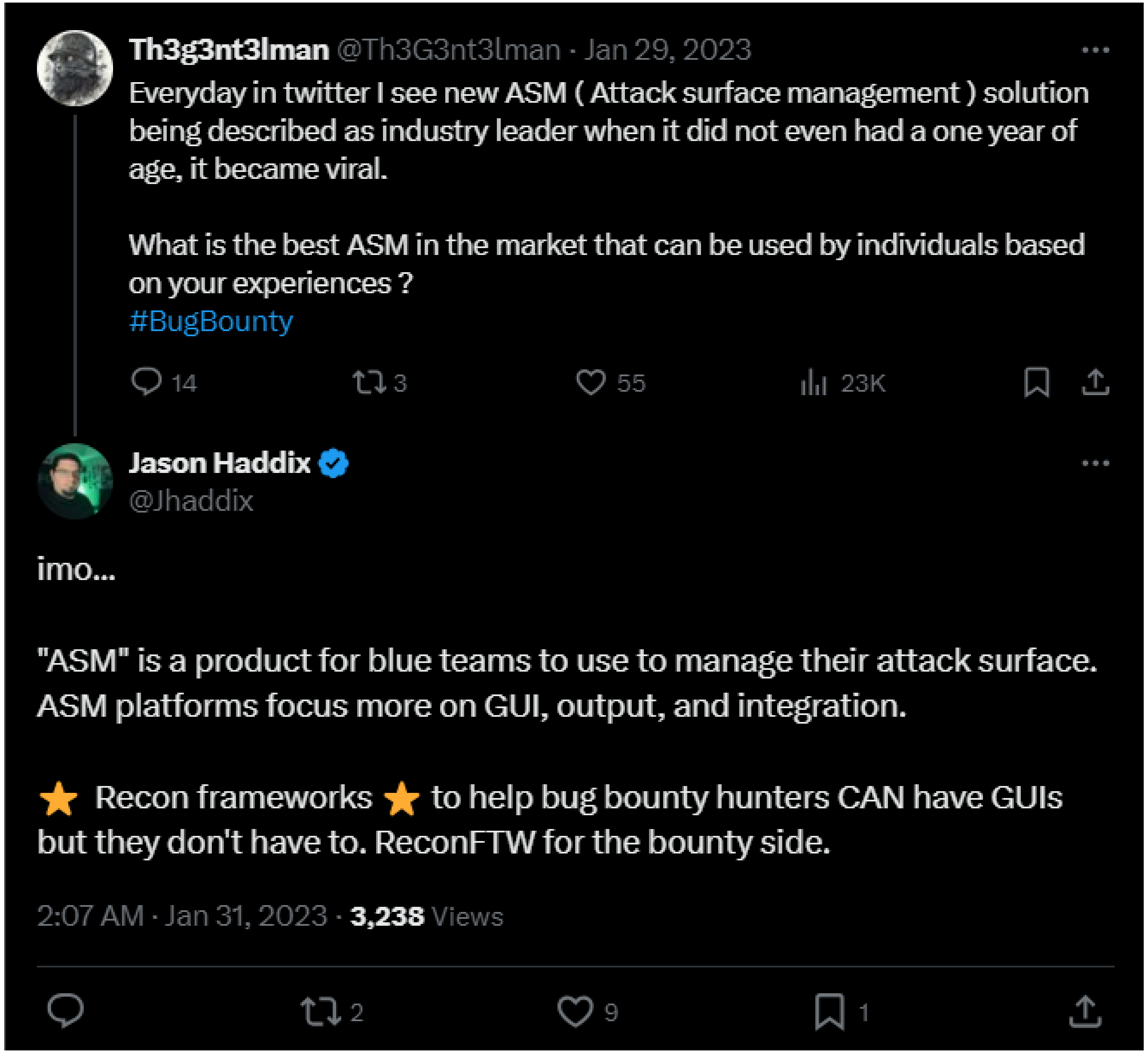
An attack surface management solution designed to uncover your external exposures through the lens of an adversary


NETSPI
Penetration Testing as a Service
Attack Surface Management
Breach and Attack Simulation
Resources
About Us
Get a Quote

Attack Surface Management

Struggling to keep up with your expanding attack surface? You're not alone. The reality is that all organizations today are experiencing constant change – whether they know it or not.

Improve your visibility, inventory, and understanding of your assets



Th3g3nt3lman @Th3G3nt3lman · Jan 29, 2023

Everyday in twitter I see new ASM (Attack surface management) solution being described as industry leader when it did not even had a one year of age, it became viral.

What is the best ASM in the market that can be used by individuals based on your experiences ?
#BugBounty

Jason Haddix @Jhaddix

imo...

"ASM" is a product for blue teams to use to manage their attack surface. ASM platforms focus more on GUI, output, and integration.

⭐ Recon frameworks ⭐ to help bug bounty hunters CAN have GUIs but they don't have to. ReconFTW for the bounty side.

2:07 AM · Jan 31, 2023 · **3,238** Views

SECURITY MANAGERS BE LIKE

SPENT $100K ON A NEW SECURITY TOOL
JUST REALIZED TEAM IS TOO BUSY TO USE IT

- Apex Domain Names
- Certificates
- Assets
  - Network Assets
    - ASN, IP’s, Ports, Services
  - Web Applications
    - Tech Stack, Endpoint URLs, Parameters
    - Exposed APIs
  - Cloud Infrastructure
    - Open Buckets/blobs/container etc
  - Public Repositories
- Data Breaches – Credential Leaks
- …

Attack Surface

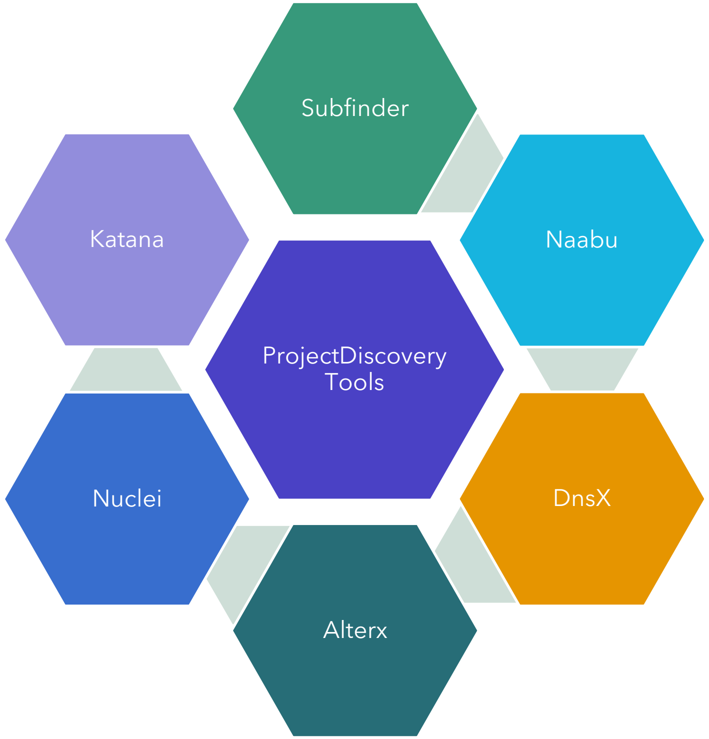
Reconnaissance & Enumeration

- Subdomain Discovery
- DNS Subdomain Bruteforcing
- Resolve DNS Records
- Extract IP Addresses
- Quick Port Scanning
- Service Enumeration
- HTTP Probing
- Detect Tech Stack
- URL Extraction and Validation

Vulnerability Scanning

- Exploitable Vulnerabilities
- Misconfigurations
- Deep Recon - Shodan
- Content Discovery Scans
  - Sensitive exposed files
  - Config files / PII Data / Secrets
  - Web path / Hidden directories
  - URLs Endpoints
- JavaScript Recon
  - Hard coded credentials
  - API endpoints
  - Variables / Parameters

Tools Available



Web

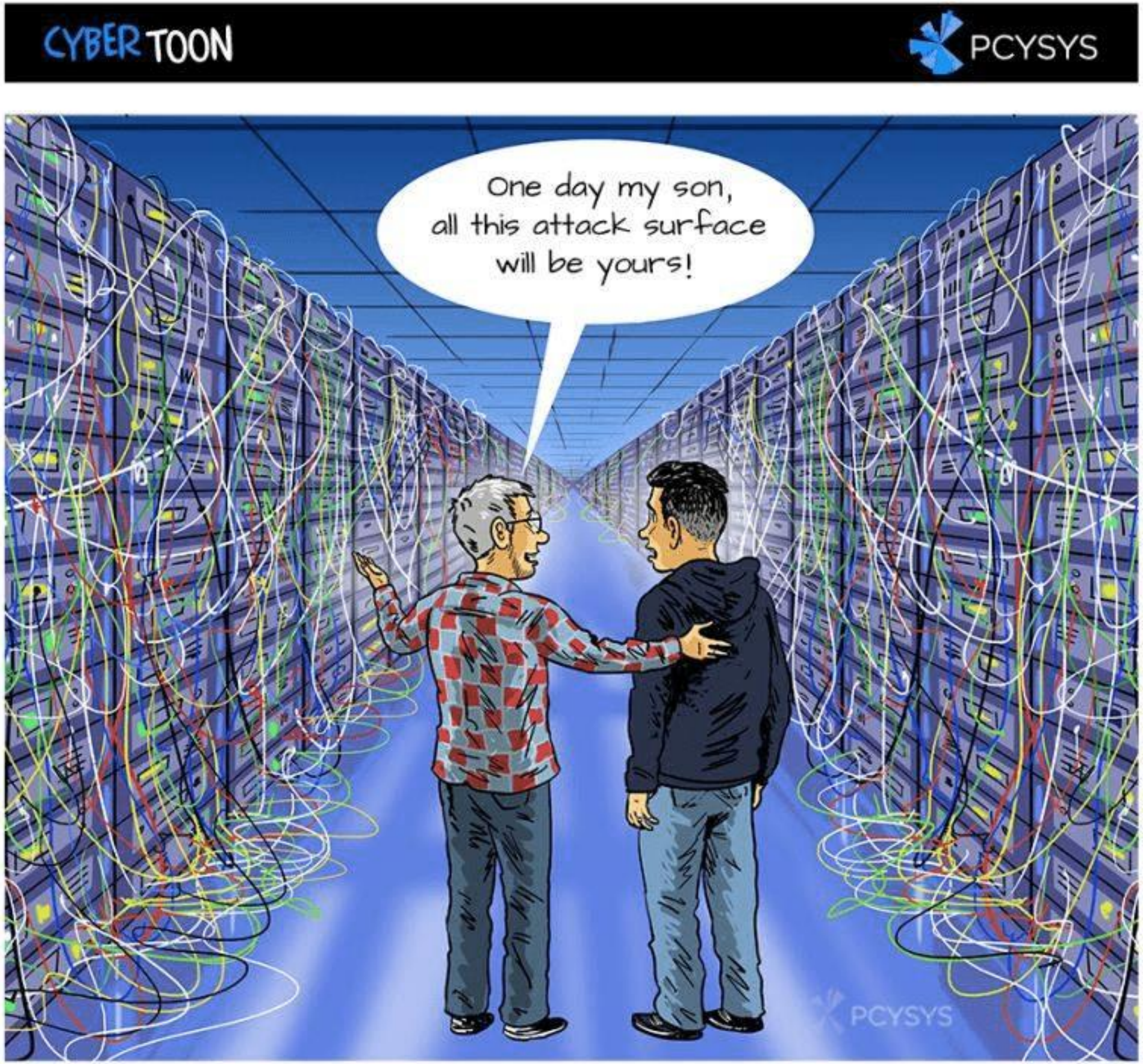
- WebAnalyze
- Dmut
- FFUF
- Dirsearch
- Trufflehog
- LinkFinder
- SecretFinder
- GAU
- GF
- qsinject
- Waymore
- xnLinkFinder

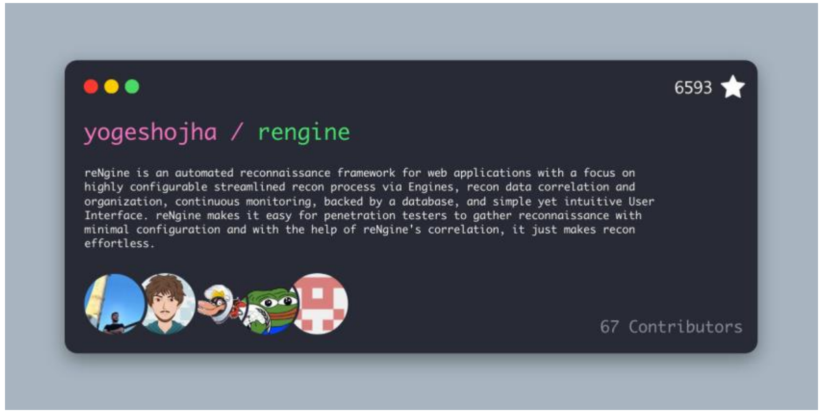
Network

- ASNMap
- MapCIDR
- Shodan-CLI
- NMAP

MISC

- TLSx
- Anew
- Nuclei Templates + Fuzzing Templates
- KnockKnock
- Subjack
- Interlace


CYBER TOON
PCYSYS
One day my son, all this attack surface will be yours!
PCYSYS

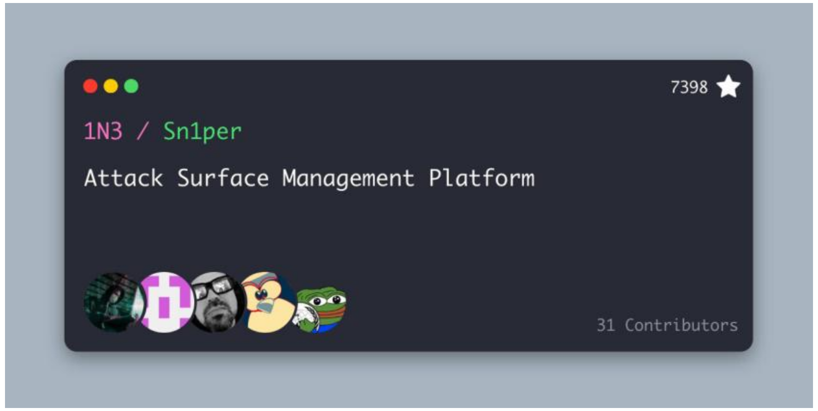


6593 ★

yogeshojha / rengine

reNgine is an automated reconnaissance framework for web applications with a focus on highly configurable streamlined recon process via Engines, recon data correlation and organization, continuous monitoring, backed by a database, and simple yet intuitive User Interface. reNgine makes it easy for penetration testers to gather reconnaissance with minimal configuration and with the help of reNgine's correlation, it just makes recon effortless.

67 Contributors

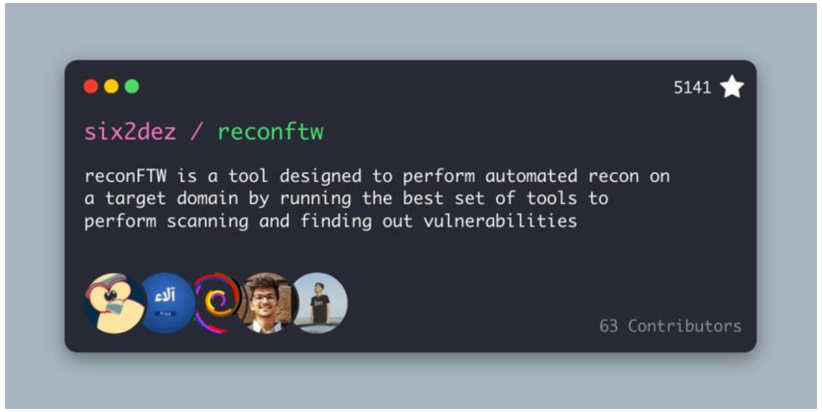


7398 ★

1N3 / Sn1per

Attack Surface Management Platform

31 Contributors

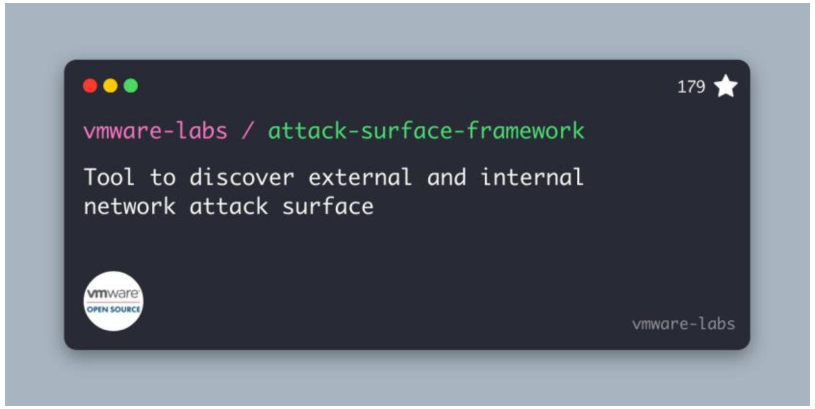


5141 ★

six2dez / reconftw

reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities

63 Contributors

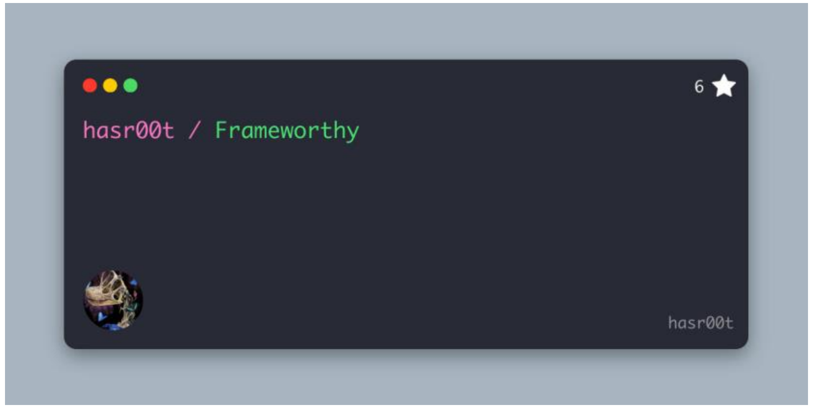


179 ★

vmware-labs / attack-surface-framework

Tool to discover external and internal network attack surface

vmware-labs



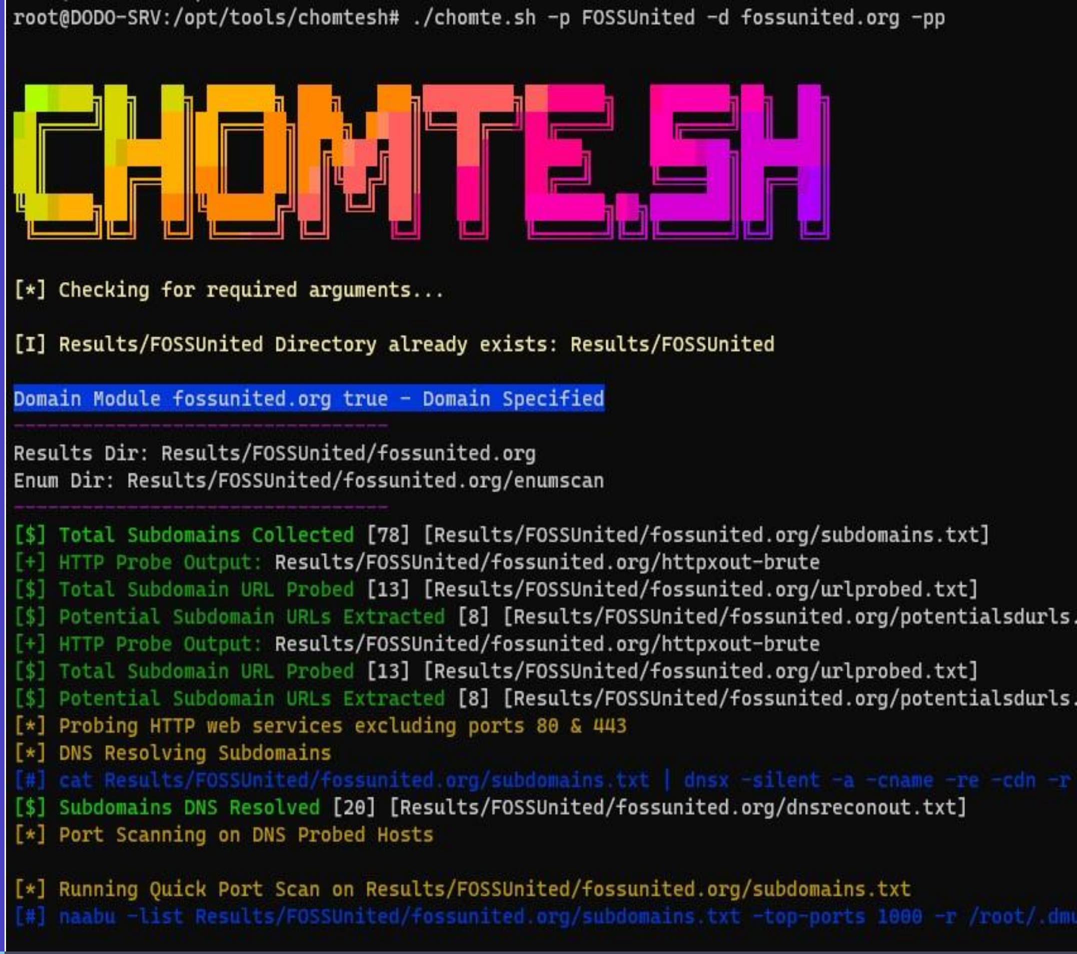
6 ★

hasr00t / Frameworthy

hasr00t

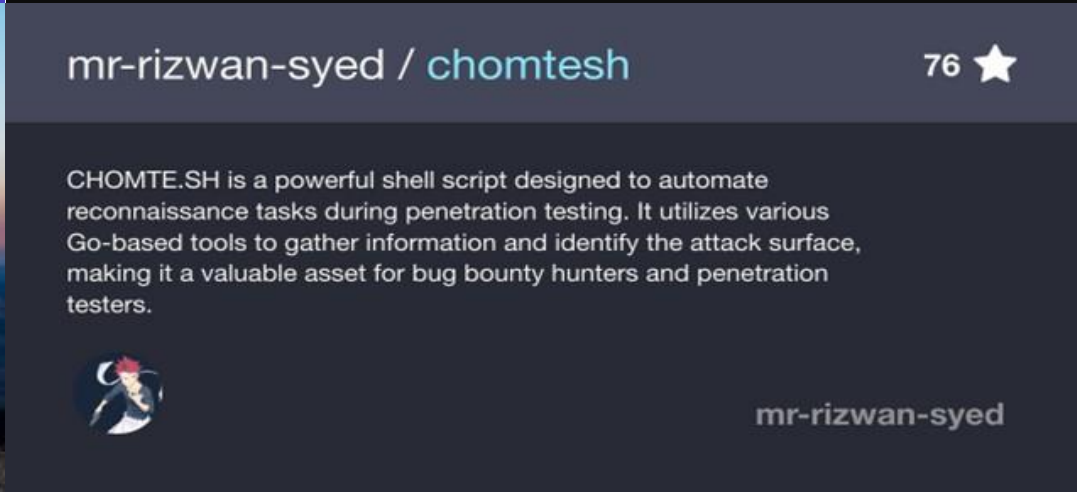
CHOMTE.SH

CHOMTE.SH is a versatile framework designed for automating reconnaissance tasks in penetration testing. It's useful for bug bounty hunters and penetration testers in both internal and external network engagements.



```
root@DODO-SRV:/opt/tools/chomtesh# ./chomte.sh -p FOSSUnited -d fossunited.org -pp

[*] Checking for required arguments...

[I] Results/FOSSUnited Directory already exists: Results/FOSSUnited

Domain Module fossunited.org true - Domain Specified
--------------------------------------
Results Dir: Results/FOSSUnited/fossunited.org
Enum Dir: Results/FOSSUnited/fossunited.org/enumscan
--------------------------------------
[$] Total Subdomains Collected [78] [Results/FOSSUnited/fossunited.org/subdomains.txt]
[+] HTTP Probe Output: Results/FOSSUnited/fossunited.org/httpxout-brute
[$] Total Subdomain URL Probed [13] [Results/FOSSUnited/fossunited.org/urlprobed.txt]
[$] Potential Subdomain URLs Extracted [8] [Results/FOSSUnited/fossunited.org/potentialsdurls.
[+] HTTP Probe Output: Results/FOSSUnited/fossunited.org/httpxout-brute
[$] Total Subdomain URL Probed [13] [Results/FOSSUnited/fossunited.org/urlprobed.txt]
[$] Potential Subdomain URLs Extracted [8] [Results/FOSSUnited/fossunited.org/potentialsdurls.
[*] Probing HTTP web services excluding ports 80 & 443
[*] DNS Resolving Subdomains
[#] cat Results/FOSSUnited/fossunited.org/subdomains.txt | dnsx -silent -a -cname -re -cdn -r
[$] Subdomains DNS Resolved [20] [Results/FOSSUnited/fossunited.org/dnsreconout.txt]
[*] Port Scanning on DNS Probed Hosts

[*] Running Quick Port Scan on Results/FOSSUnited/fossunited.org/subdomains.txt
[#] naabu -list Results/FOSSUnited/fossunited.org/subdomains.txt -top-ports 1000 -r /root/.dm
```

Exploring Attack Surface



mr-rizwan-syed / chomtesh

76 ★

CHOMTE.SH is a powerful shell script designed to automate reconnaissance tasks during penetration testing. It utilizes various Go-based tools to gather information and identify the attack surface, making it a valuable asset for bug bounty hunters and penetration testers.

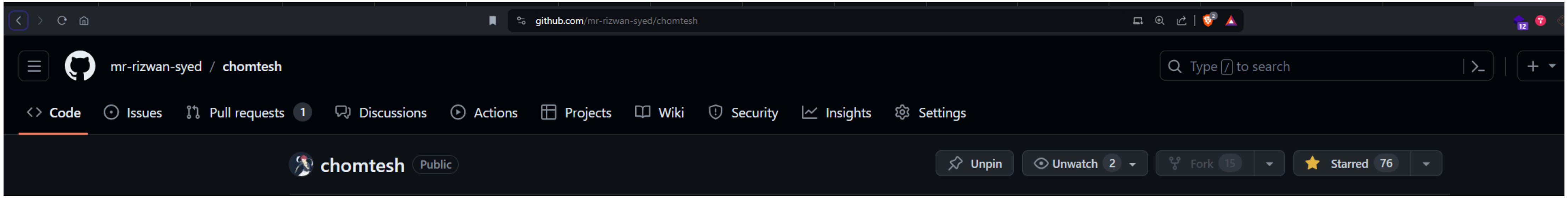
mr-rizwan-syed

CHOMTE.SH

1. Gather Subdomains
2. Domain to IP resolution of subdomains
3. Scanning for open ports resolved IP
4. Map the open ports to their corresponding subdomains
5. Perform an HTTP probing of each subdomain : port
6. Content discovery
7. Tech detect – run custom scan based on running technology
8. Gather URL, JS mining, potential URLs, param, secrets
9. Service enumeration using Nmap
10. Nmap report generation x3

https://github.com/mr-rizwan-syed/chomtesh

Installation



```
git clone https://github.com/mr-rizwan-syed/chomtesh
cd chomtesh
chmod +x *.sh
./install.sh
./chomte.sh
```

OR

```
docker pull r12w4n/chomtesh
```

```
docker run --rm -it -v "$(pwd)/Results:/app/chomtesh/Results"
r12w4n/chomtesh ./chomte.sh -p vulnweb -d vulnweb.com
```

The potential damage to your attack surface is real and substantial. Consider the following examples:

- Security researchers recently found 1.2 billion records with individuals' personal data aggregated by People Data Labs on an exposed Elasticsearch server.
- MoviePass exposed credit card information for thousands of customers on a server open to the Internet that was unencrypted and not password protected.
- Hackers compromised a reservation database for Marriott's Starwood division and accessed the data of 383 million guests.
- A database managed by the Indian government was left open to the Internet without a password, exposing the medical records of more than 12.5 million pregnant women.
- A brute-force attack on an exposed Remote Desktop Protocol (RDP) server from Labcorp resulted in 7,000 systems and 1,900 servers infected.

Rizwan Syed

github.com/mr-rizwan-syed
twitter.com/_r12w4n
linkedin.com/in/r12w4n/
BreachForce.net

Thank you