AUTOMATED APPROACH TO THE ANALYSIS OF NETWORK DEVICES SECURITY

Khodukina Natalia @khodunken
Loginov Nikita @nepJIywa
Driagunov Mikhail @AetherEternity

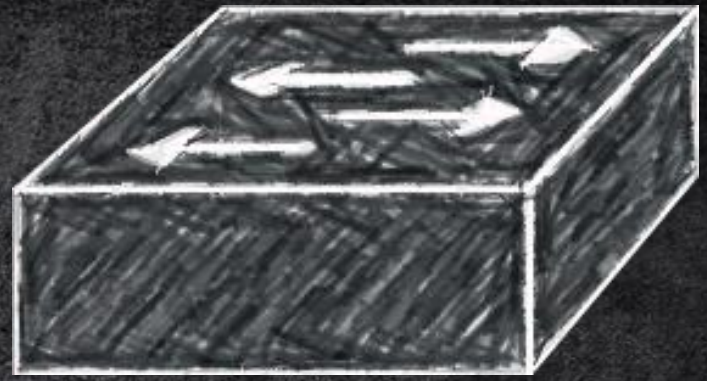
ZERO NIGHTS 2018

ZERO NIGHTS 2018

2^3 EDITION

Nice to meet you

Switch



Configuration file

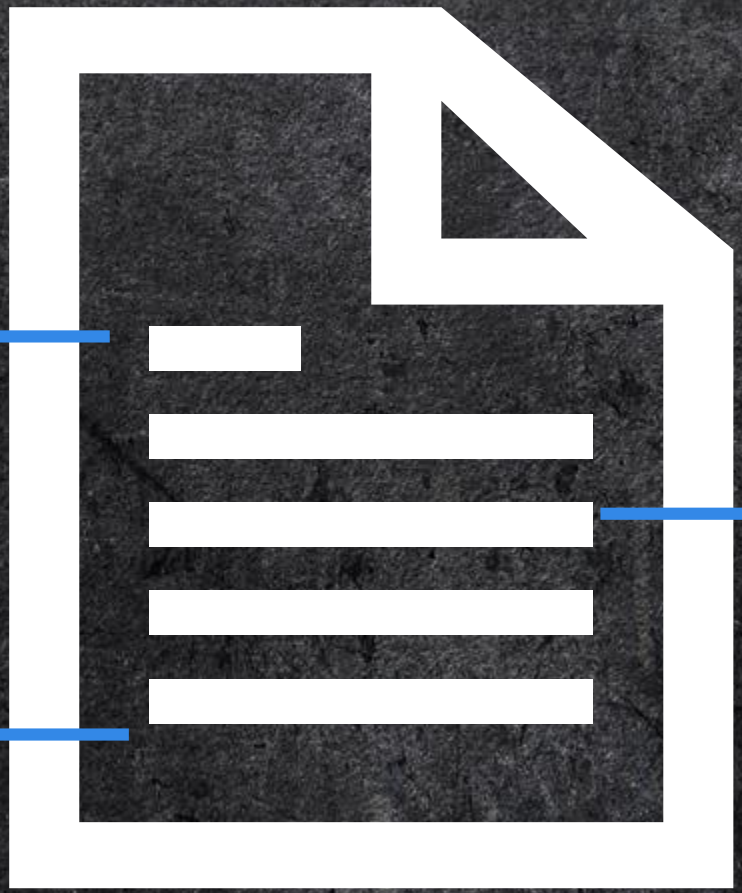
ZERO NIGHTS 2018

2^3 EDITION

Problems

PASSWORDS

DOS

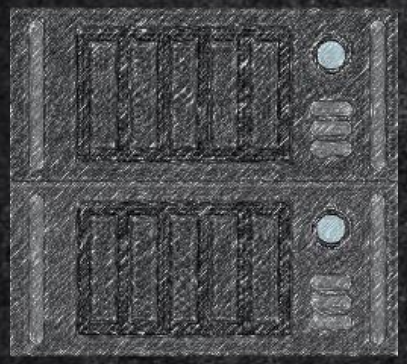


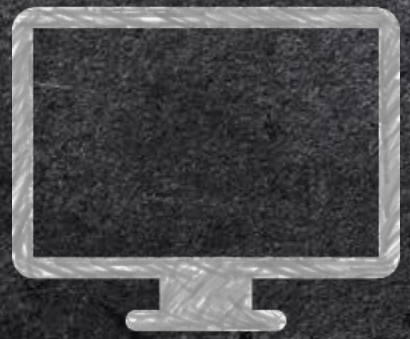
MITM

ZERO NIGHTS 2018

2^3 EDITION

Where is it?



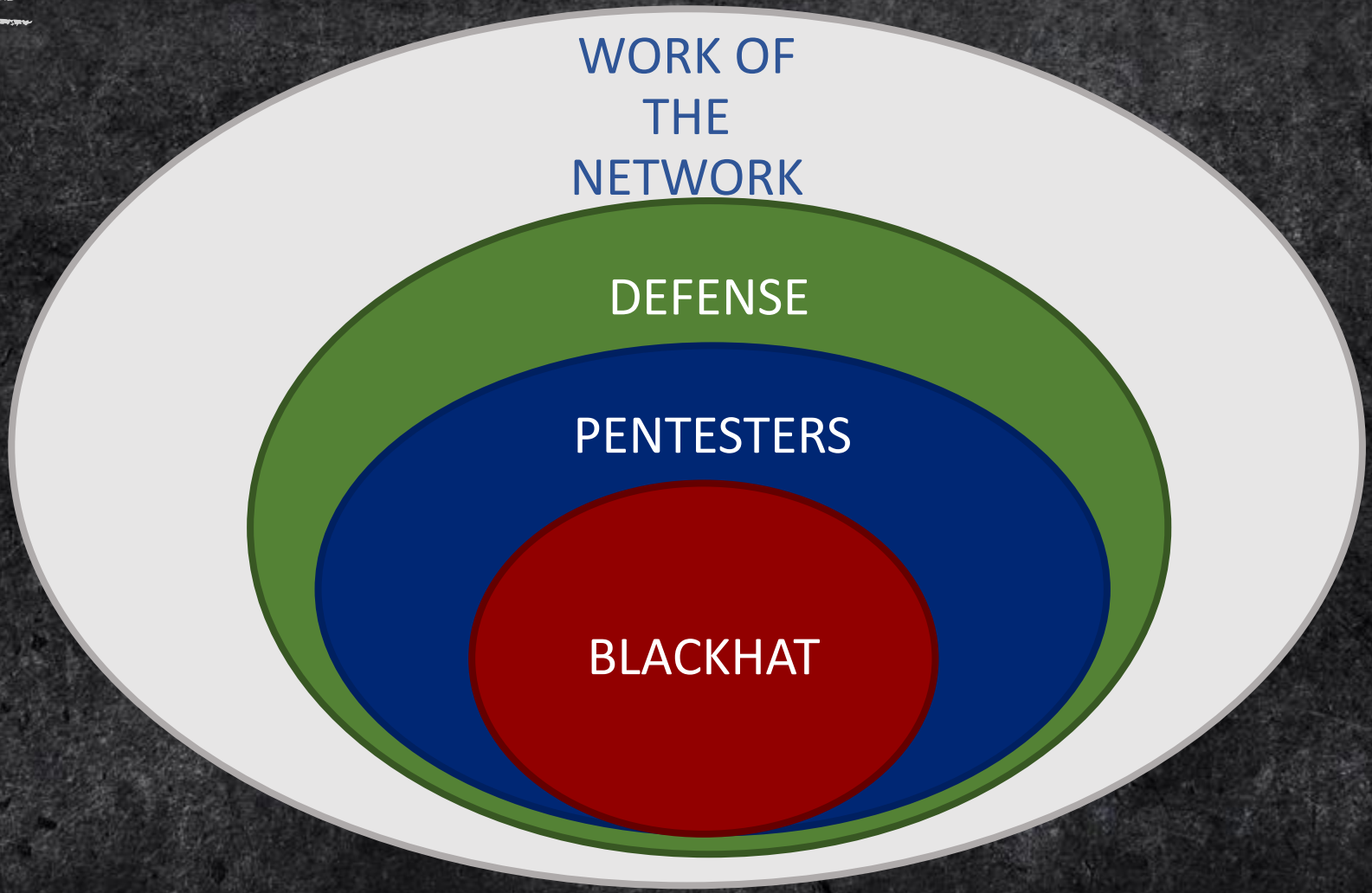


- TFTP backups
- SSH/Telnet
- Smart Install

ZERO NIGHTS 2018

2^3 EDITION

Useful configs



ZERO NIGHTS 2018

2³ EDITION

Config structure

General

- Hostname
- AAA
- Services
- ....

```
version 15.2
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
```

```
switchport access vlan 2
switchport mode access
!
interface Ethernet0/3
switchport access vlan 2
switchport mode access
!
interface Vlan1
!
line con 0
!
end
```

ZERO NIGHTS 2018

2³ EDITION

Config structure

- VLAN
- mode
- Services
- ....

Interfaces

```
!
version 15.2
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
!
interface Ethernet0/0
switchport access vlan 2
switchport mode access
!
interface Ethernet0/1
```

```
!
interface Ethernet0/2
switchport access vlan 2
switchport mode access
!
```

```
!
line con 0
!
end
```

Security misconfig

15.2

Spoofing

- ARP
- DHCP

```
hostname SW
boot-start-marker
boot-end-marker
no aaa new-model
interface Ethernet0/0
switchport access vlan 2
switchport mode access
!
interface Ethernet0/1
switchport access vlan 2
switchport mode access
```

2^3 EDITION

Security misconfig

Protection

- ARP
- DHCP

```
hostname SW1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip arp inspection vlan 2
ip dhcp snooping vlan 2
!
interface Ethernet0/0
switchport access vlan 2
switchport mode access
!
interface Ethernet0/1
switchport access vlan 2
switchport mode access
```

ZERO NIGHTS 2018

2^3 EDITION

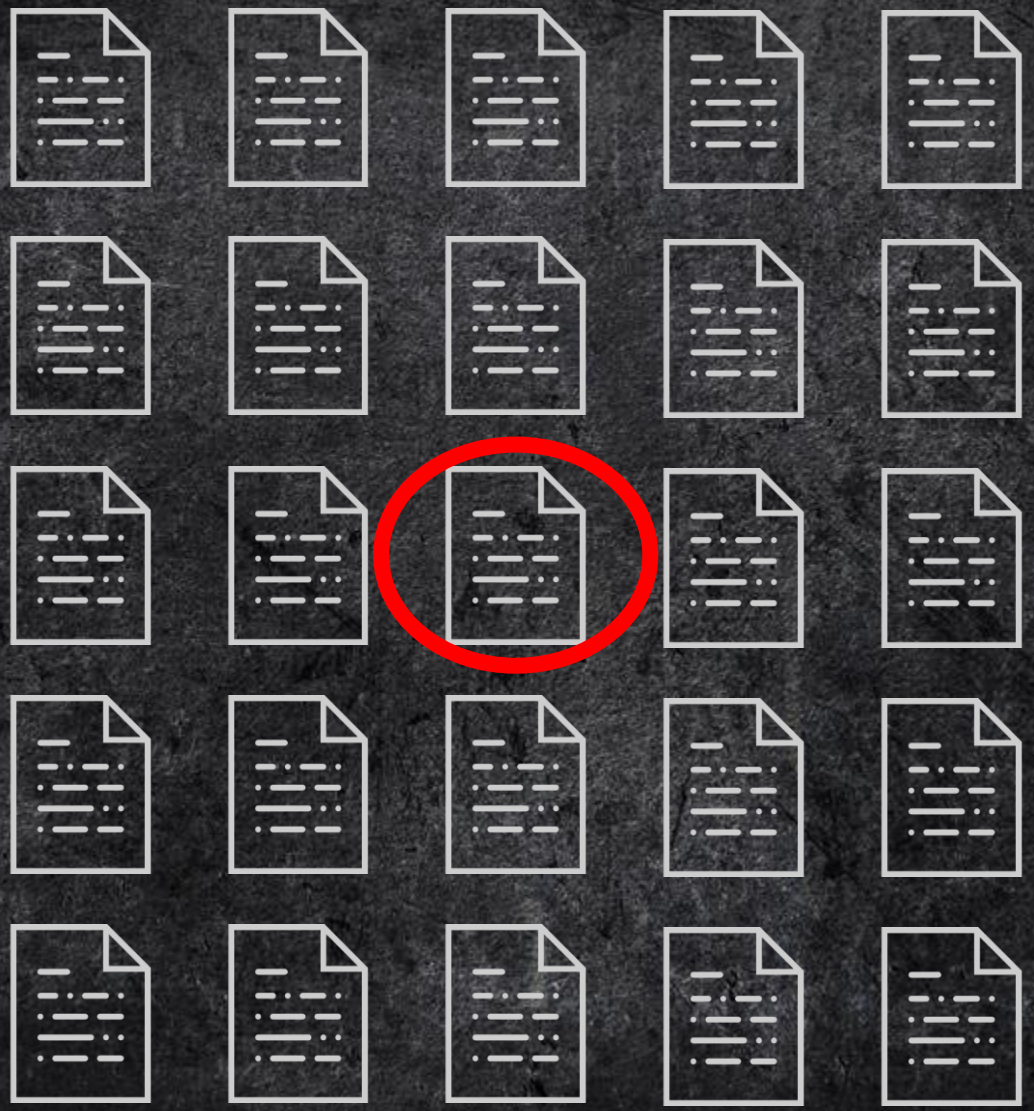
Default problems

- Smart install
- MOP
- PAD
- CDP
- DTP

2^3 EDITION

LAN network

Configuration file

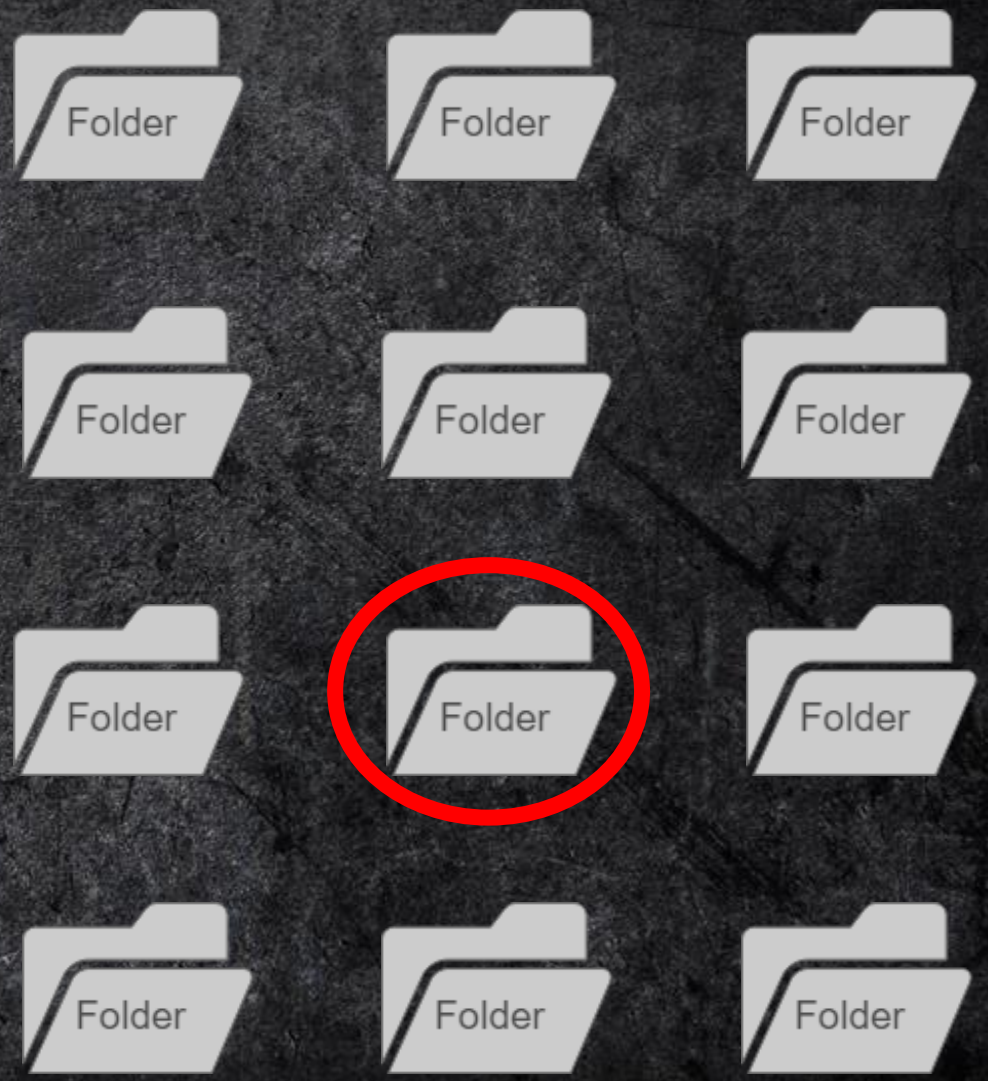


ZERO NIGHTS 2018

2^3 EDITION

Many LANs

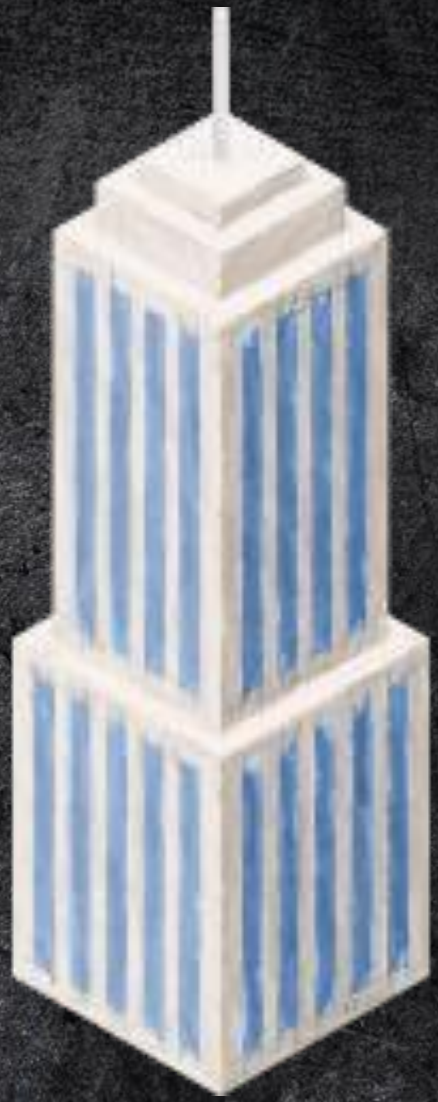
LAN network



ZERO NIGHTS 2018

2^3 EDITION

Scale



Len(Nginx config)~50

Len(CISCO config)~400

ZERO NIGHTS 2018

2³ EDITION

Existing solutions

About the Cisco CLI Analyzer

The Cisco CLI Analyzer is a smart SSH client designed to help troubleshoot and check the overall health of your supported device.

CLI Analyzer

Release 3.6.2

Notifications

Related Links and Documentation

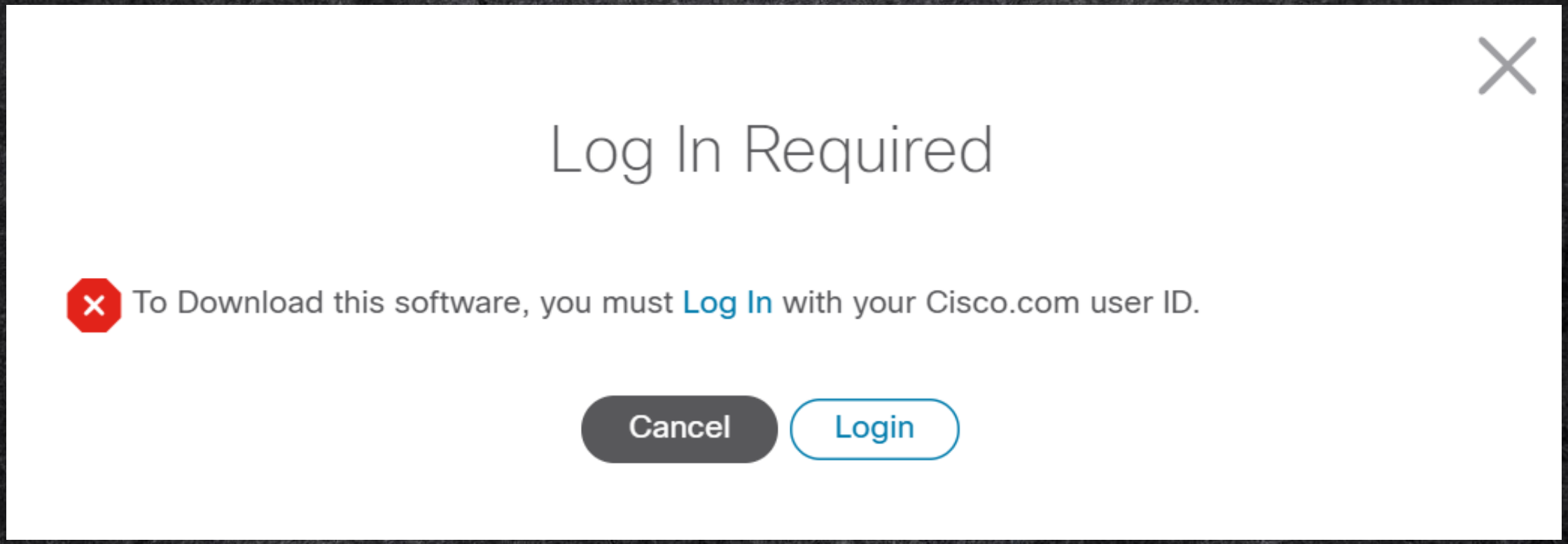
- No related links or documentation -

File Information	Release Date	Size
Cisco CLI Analyzer SSH client software Cisco-CLI-Analyzer.3-6-2.x64.msi	04-OCT-2018	121.64 MB

ZERO NIGHTS 2018

2^3 EDITION

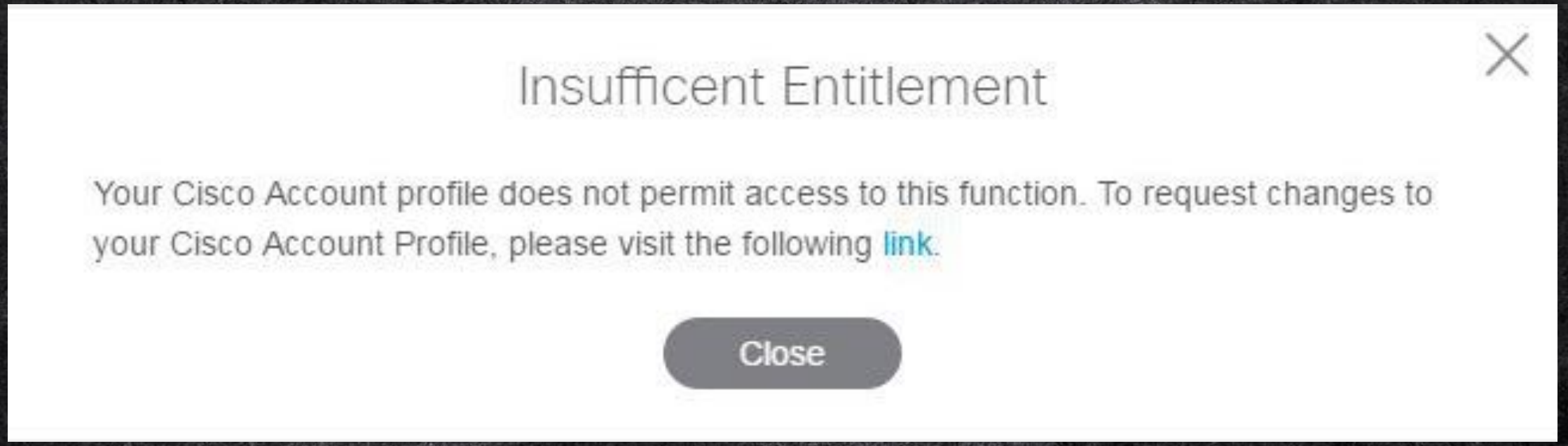
Existing solutions



ZERO NIGHTS 2018

2^3 EDITION

Existing solutions



ZERO NIGHTS 2018

2^3 EDITION

Existing solutions

Nipper studio

open source 2008

proprietary software

Existing solutions

Nipper Studio

Audit Report

Sunday, November 11, 2018

Summary

Nipper Studio performed an audit on Sunday, November 11, 2018 of the network device detailed in the scope. The audit consisted of the following components:

- a best practice security audit (Part 2);
- a software vulnerability audit report (Part 3);
- a configuration report (Part 4).

Scope

The scope of this audit was limited to the device detailed in Table 1.

Device	Name	OS

ZERO NIGHTS 2018

2^3 EDITION

Existing solutions

Nipper Studio

Audit Report

Sunday, November 11, 2018

Support Option: *	No. of devices: *	Subscription length: *	Currency: *	Price:	Multi-year saving:	Total:	
Nipper Studio - Bronze Support	25	1 year	USD	$44.00	0%	$1,100.00	Add to cart

- a best practice security audit (Part 2);
- a software vulnerability audit report (Part 3);
- a configuration report (Part 4).

Scope

The scope of this audit was limited to the device detailed in Table 1.

Device	Name	OS

ZERO NIGHTS 2018

2^3 EDITION

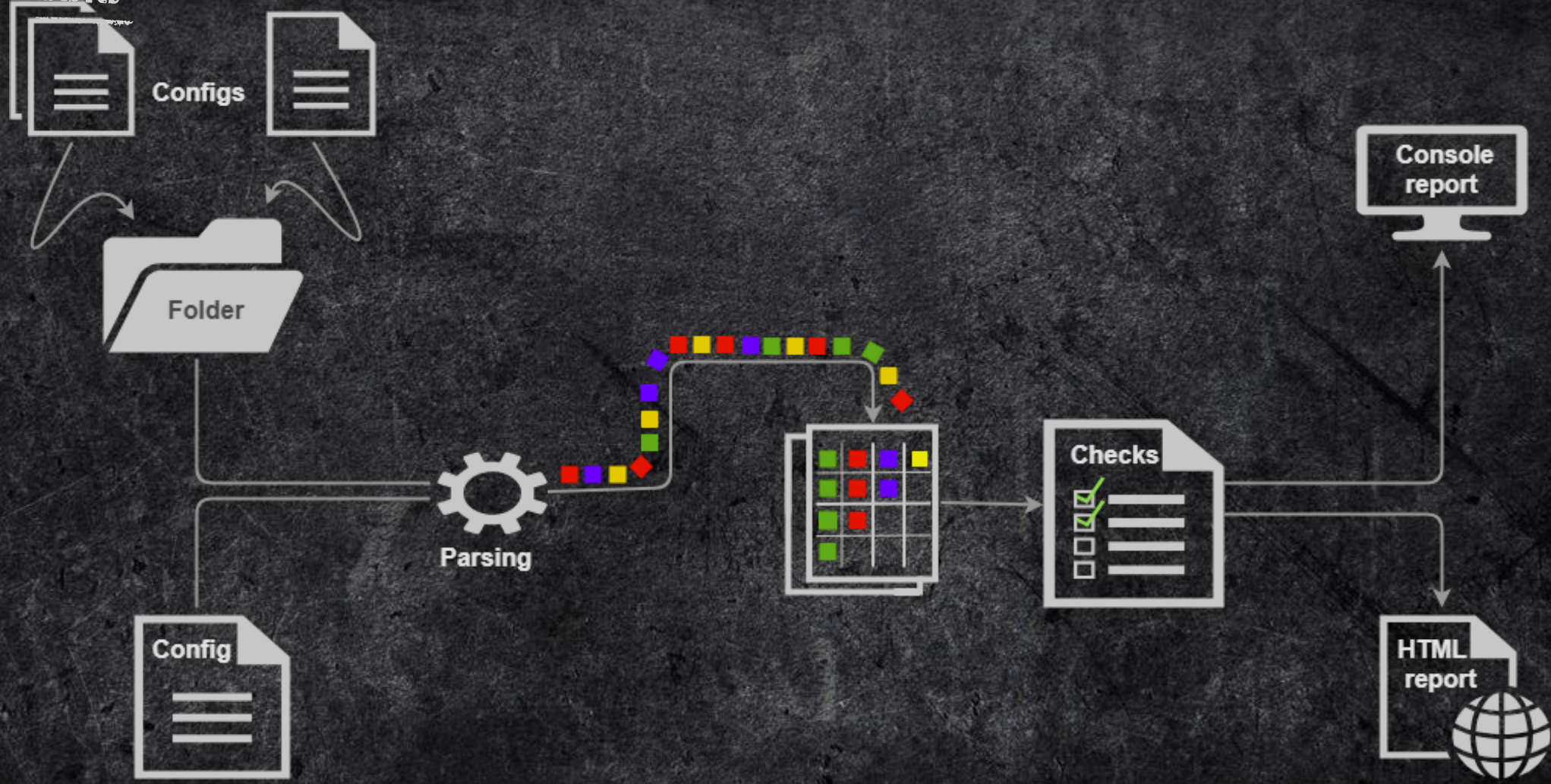
Advantages

- Open Source
- Cross-platform
- Easy to go
- A lot of checks
- Vlanmap

ZERO NIGHTS 2018

2^3 EDITION

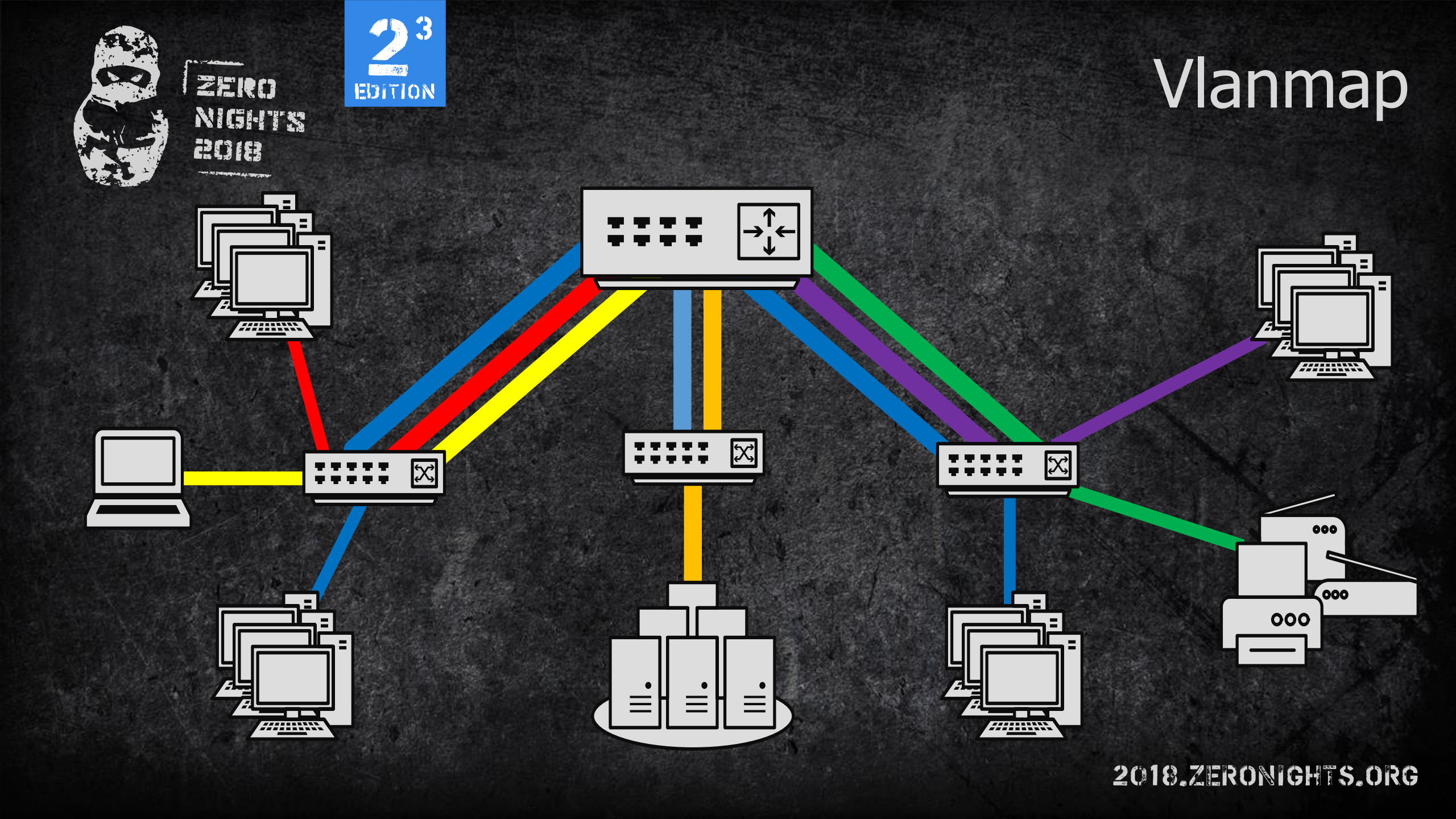
How does it work?

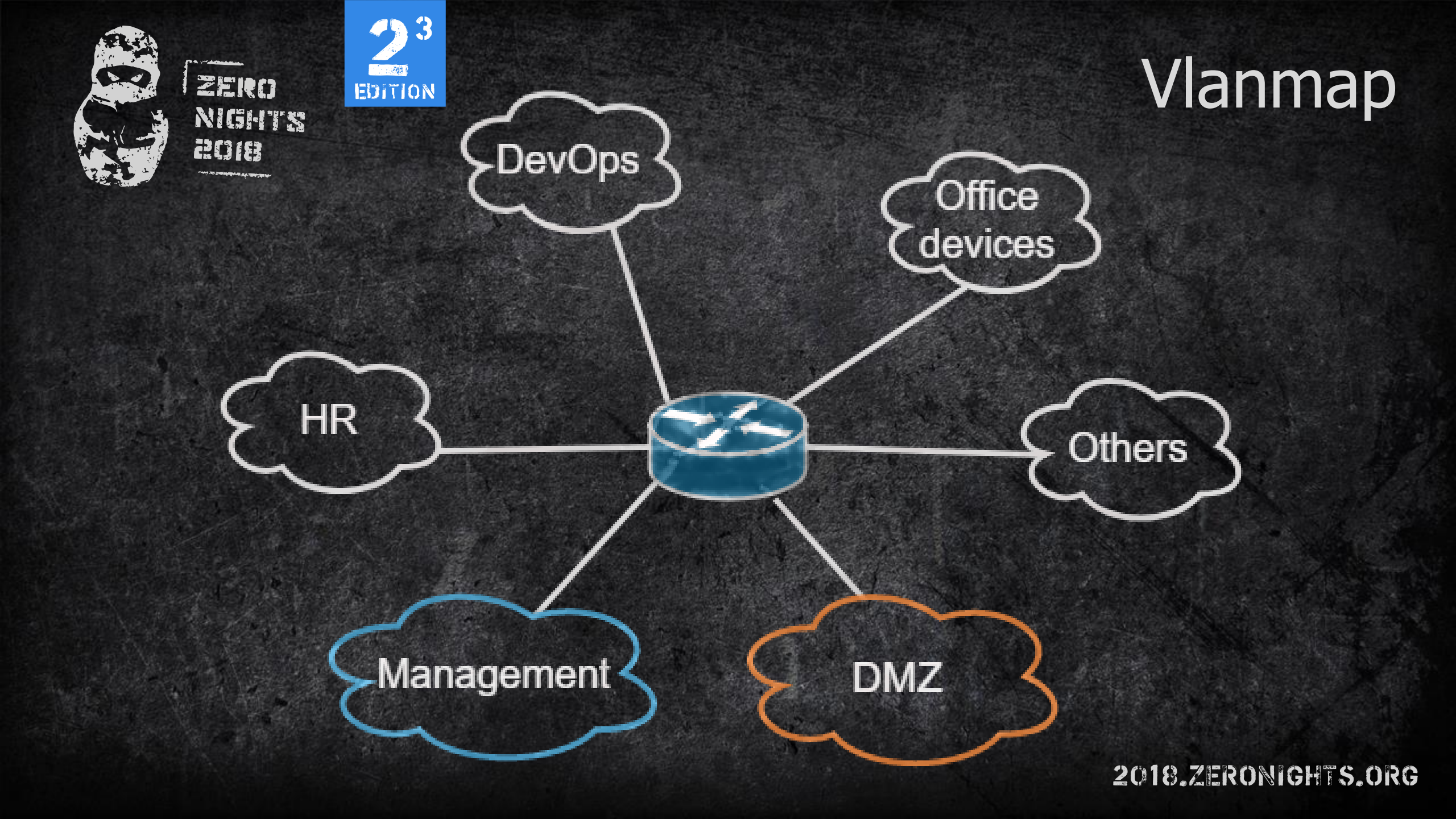


2^3 EDITION

A lot of checks

BPDUguard
TACACAS+
CDP
Radius
version
DTP
Loopguard
SSH
DHCPsnooping
LLDP
StormControl
Sourceguard
Telnet
IPv6
auth-retries
AAA
Portfast
Inbound
DAI
Timeout
LinesProtocol
NativeVLAN
Outbound
maxstartups
VTP
ARPproxy
Port-security


ZERO NIGHTS 2018
2^3 EDITION
Vlanmap
2018.ZERONIGHTS.ORG


ZERO NIGHTS 2018
2^3 EDITION
Vlanmap
DevOps
Office devices
HR
Others
Management
DMZ
2018.ZERONIGHTS.ORG

ZERO NIGHTS 2018

2^3 EDITION

Vlanmap

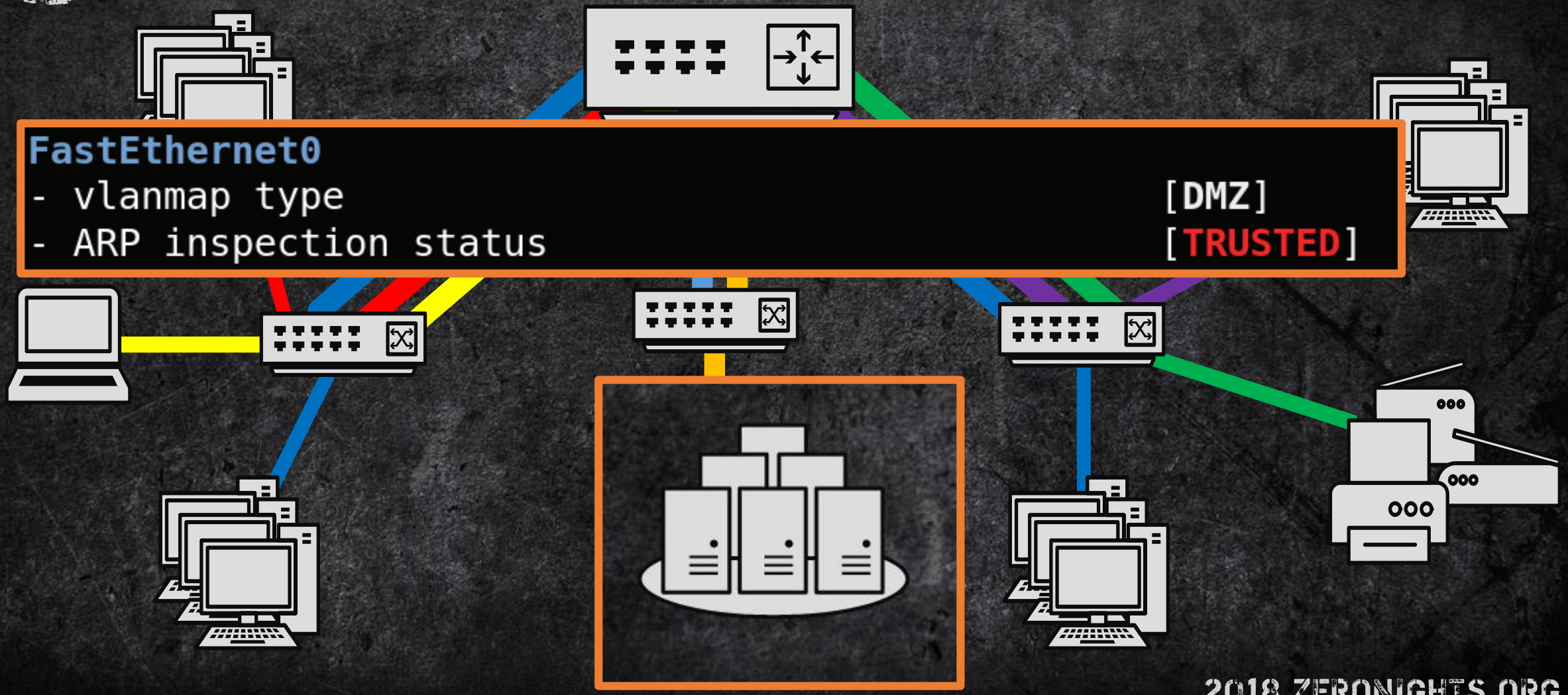
```
FastEthernet1
- vlanmap type                    [MANAGEMENT]
- ARP inspection status           [TRUSTED]
```

2018.ZERONIGHTS.ORG

ZERO NIGHTS 2018

2^3 EDITION

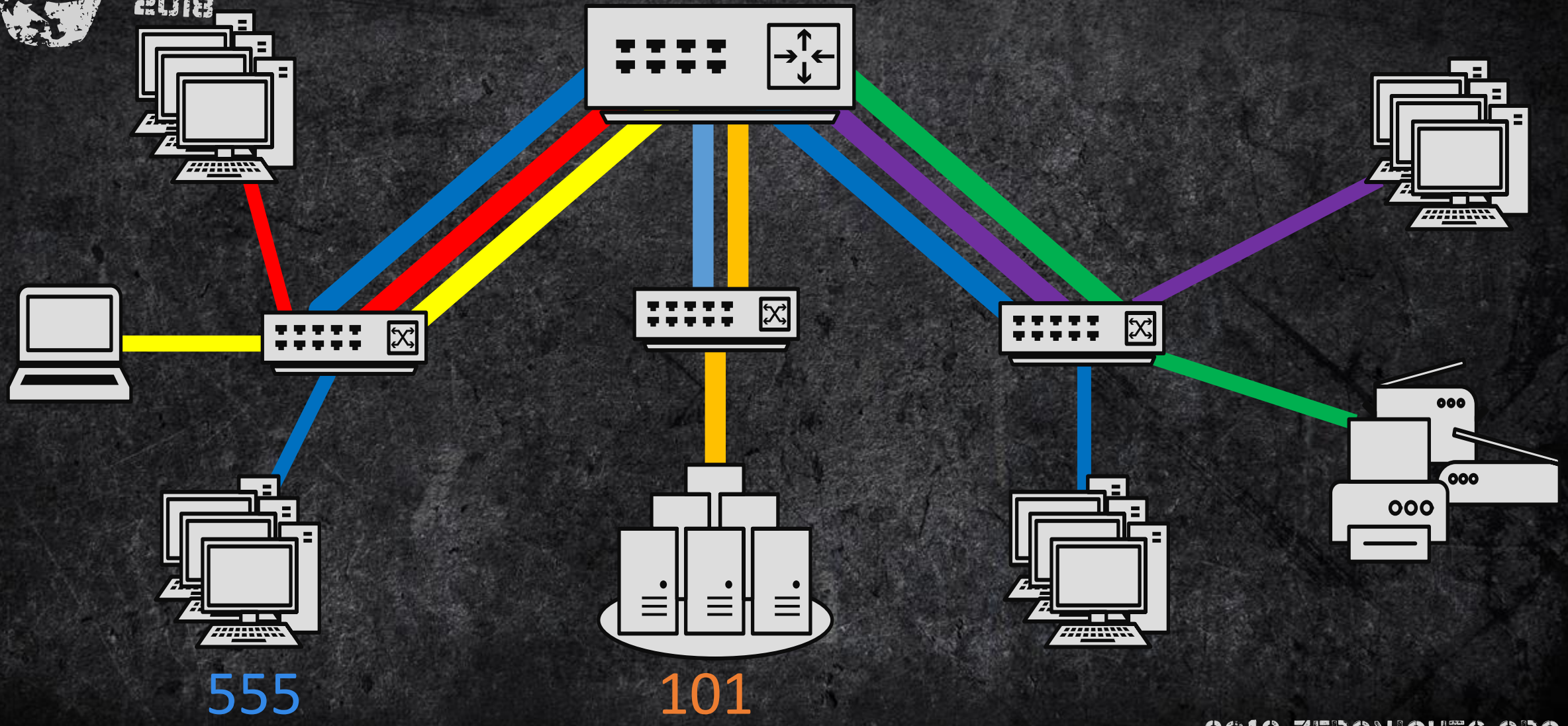
Vlanmap



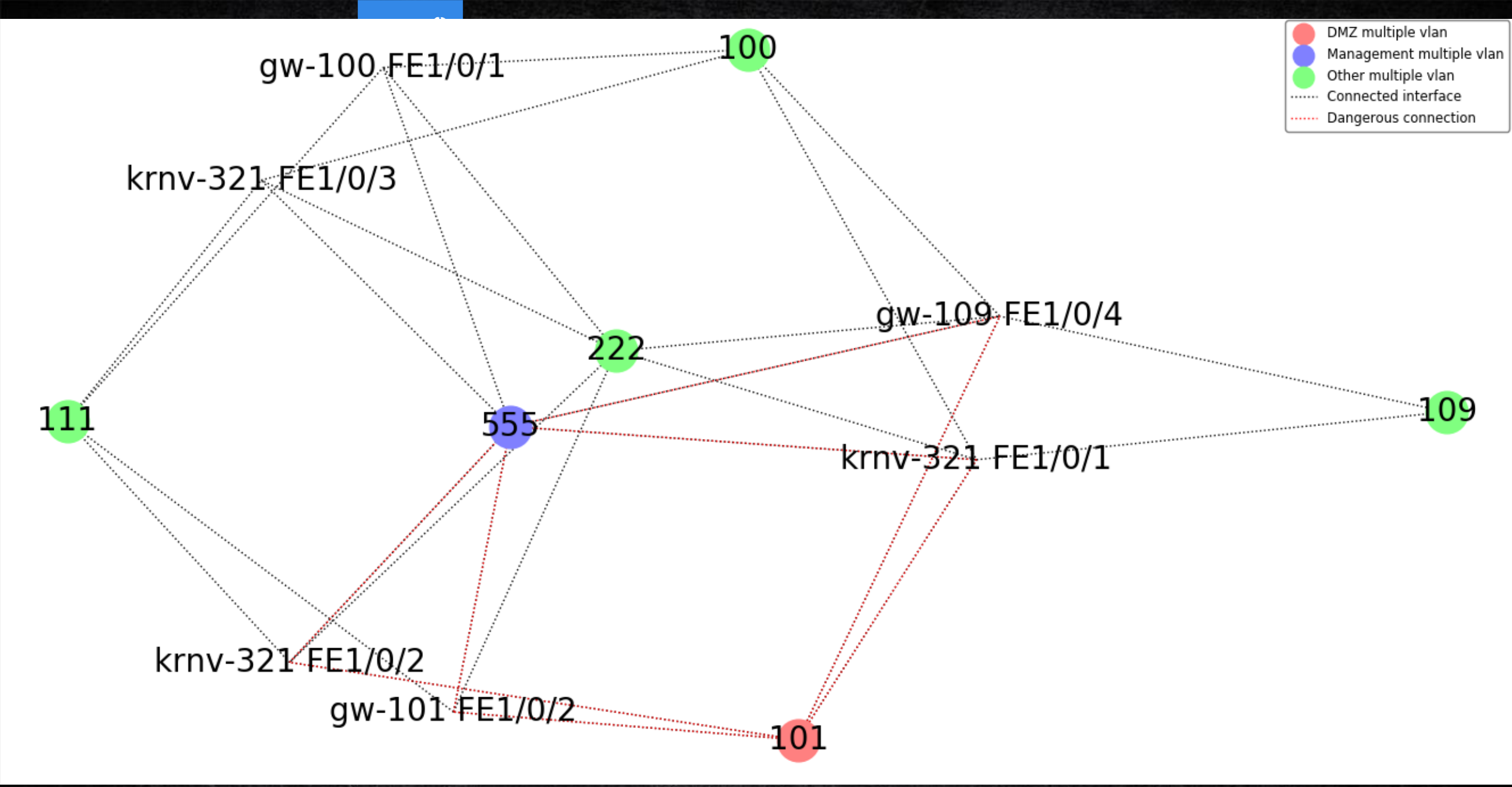
ZERO NIGHTS 2018

2^3 EDITION

Map



2018.ZERONIGHTS.ORG


DMZ multiple vlan
Management multiple vlan
Other multiple vlan
Connected interface
Dangerous connection
100
gw-100 FE1/0/1
krnv-321 FE1/0/3
222
gw-109 FE1/0/4
111
555
109
krnv-321 FE1/0/1
krnv-321 FE1/0/2
gw-101 FE1/0/2
101

ZERO NIGHTS 2018

2^3 EDITION

Reports

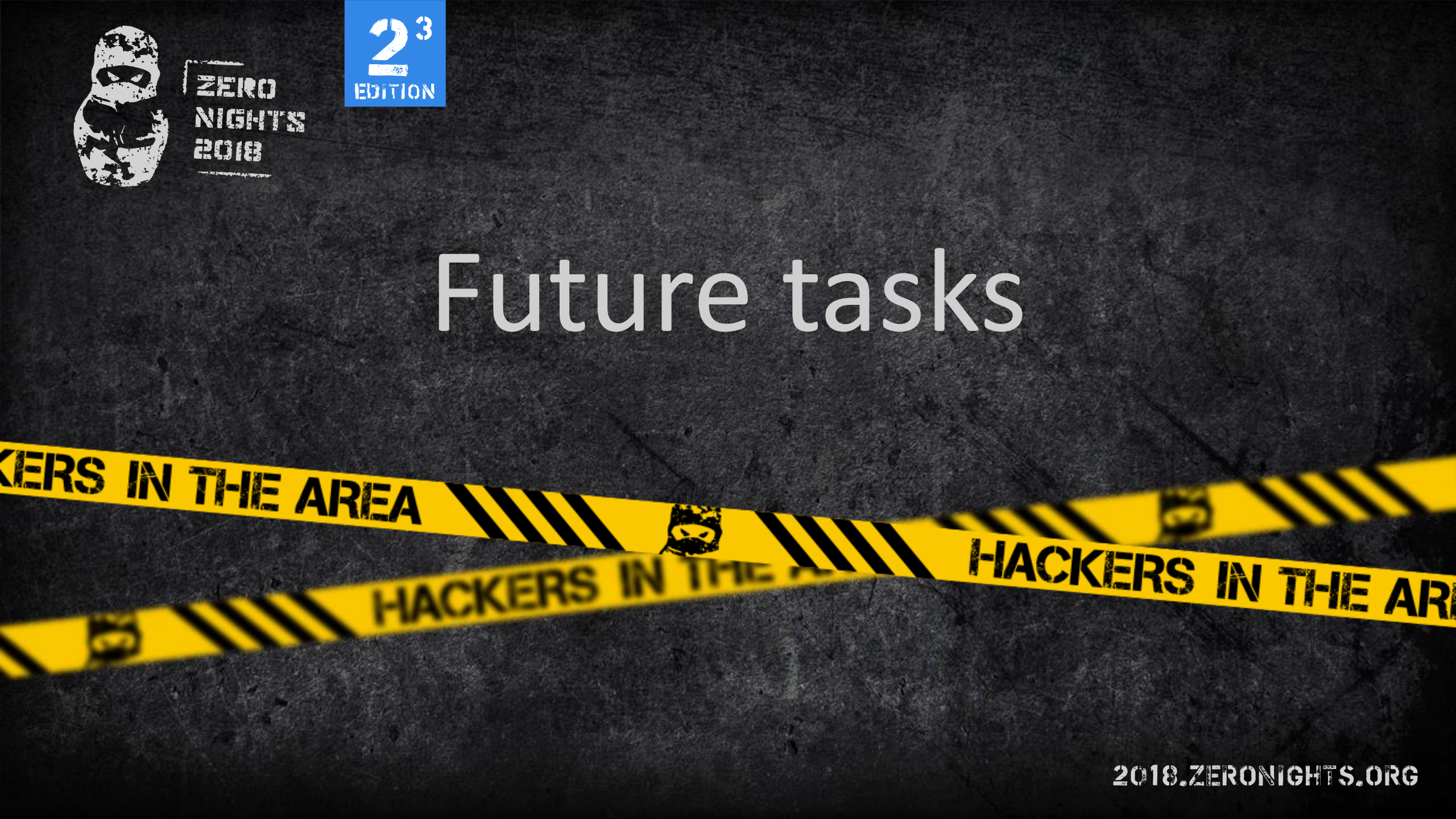
Terminal

```
root@kali:~/ZN# python3 ccat.py config/ -vl map


------------------- RESULTS FOR: ip.conf--------------------

 Services
 - password encryption                                [DISABLED]
 - tcp keepalives in                                  [DISABLED]
 - tcp keepalives out                                 [DISABLED]
 - pad                                                [ENABLED]
 - config                                             [DISABLED]
 - smart install                                      [ENABLED]
 - udp small servers                                  [DISABLED]
 - tcp small servers                                  [DISABLED]
```

HTML

Services

- password encryption [DISABLED]
- tcp keepalives in [DISABLED]
- tcp keepalives out [DISABLED]
- pad [ENABLED]
- config [DISABLED]
- smart install [ENABLED]
- udp small servers [DISABLED]
- tcp small servers [DISABLED]


ZERO
NIGHTS
2018
2^3
EDITION
Future tasks
KERS IN THE AREA
HACKERS IN THE
HACKERS IN THE ARE
2018.ZERONIGHTS.ORG

ZERO NIGHTS 2018

2^3 EDITION

Automatic correction

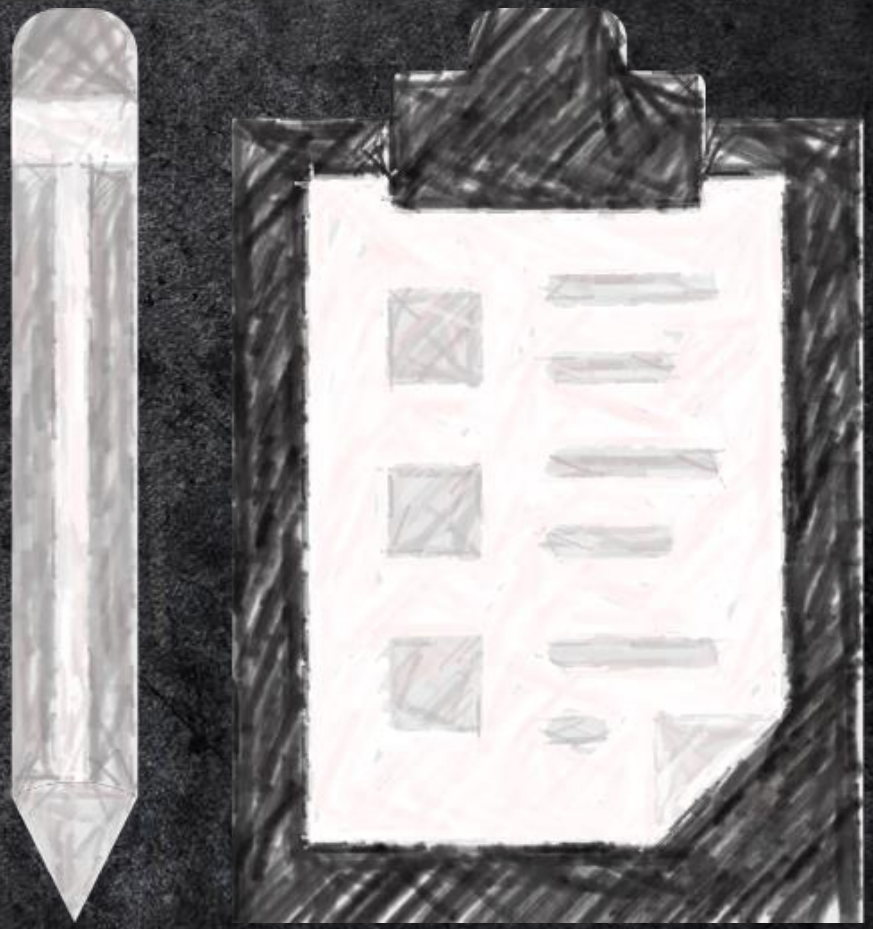
```
vtp mode transparent
!
spanning-tree mode rapid-pvst
!
```

```
vtp mode off
ip arp inspection
!
ip dhcp snooping
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
```

2^3 EDITION

Additional tasks

- Checks filter
- Check IOS version via:
  - Exploit-DB API
  - Cisco openVuln API



ZERO NIGHTS 2018

2^3 EDITION

And a little bit more...

- Assigning criticality by VLANs desc
- NTP
- SNMP options
- ICMP Filtering
- Syslog
- IPv6 bad policies
- Getting configs list by IP
- Tool banner

Thanks

Special thanks to our mentors:

Alexander Evstigneev @sab0tag3d

Kirill Vorobiev @whitel1st

We wouldn't be here without your help

GitHub: https://github.com/cisco-config-analysis-tool/ccat