cisco Live!

Let's go

The bridge to possible

NetDevOps – Reducing the Attack Surface of IOS XE with Ansible

Tim Glen, Systems Architect

DEVNET-2111

Cisco Webex App

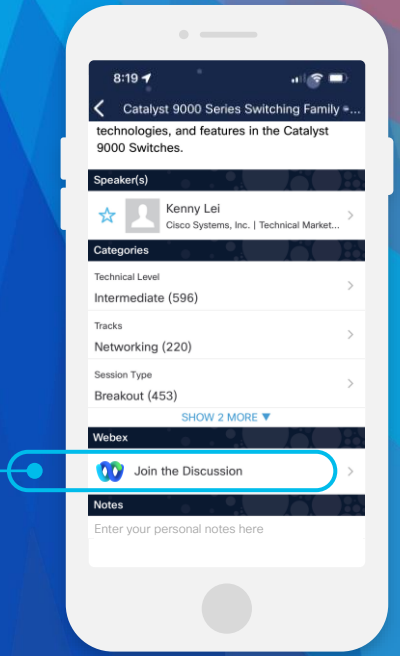
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

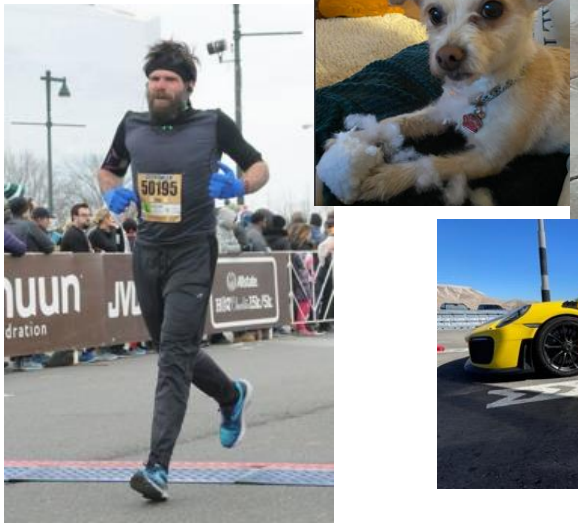
Webex spaces will be moderated by the speaker until June 9, 2023.

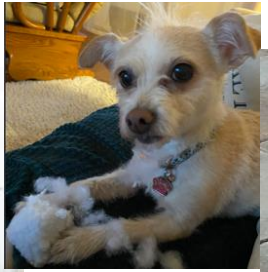


https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2111

Tim Glen (Personal)

- Husband to Hillary
- Father to Jenna
- 2 Dogs (Snickerdoodle & Autumn)
- Love the Outdoors
- Fitness, Running, Hiking
- Travel
- Driving Fast Cars,
  - esp Porsche!





Tim Glen (Professional)

- Started in IT in 1995 Telephone Tech Support
- Worked 23 years at Advertising Specialty
  - Web hosting provider, 500 employees, 30,000 hosted site
  - Managed all routers, switches, firewalls, wireless, security
- Employed at Cisco 3.5 years
  - Started September 2019
  - Systems Architect in Philly Metro area

github.com/timmayg

linkedin.com/in/timglen

cs.co/TimGlen

Agenda

- Secure Ansible Usage
- IOS XE Attack Surface
- Local User Hardening
- Protocol Hardening
- Over the Wire Encryption
- Conclusion

IOS XE Day Zero Config

IOS XE Programmability and Automation

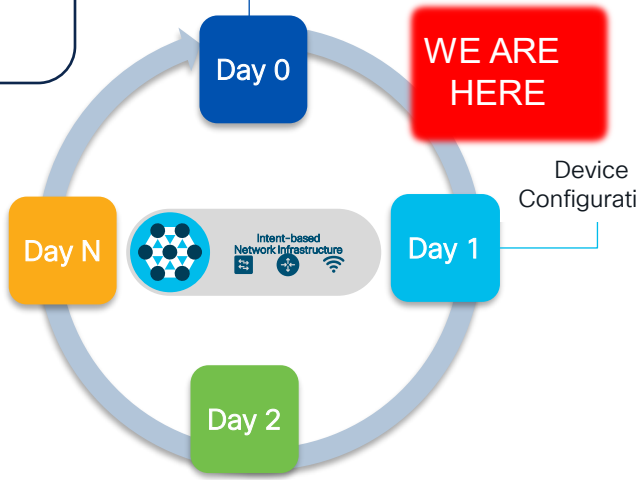
Pre-boot Execution Environment (iPXE)

Zero Touch Provisioning

Provisioning Automation

python™

Device Onboarding



WE ARE HERE

Device Configuration

Model Driven Programmability

Network Configuration Protocol (NETCONF), RESTCONF, gNMI

YANG Data Models, OpenConfig, and YANG Suite tooling

Terraform, Ansible, pyATS

Day 0 IOS XE Config (page 1)

- IP Address
- Default Gateway
- DNS
- Time Zone
- NTP

```
!
interface GigabitEthernet1/0/24
  no switchport
  ip address 10.1.1.5 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.3
!
ip name-server 208.67.222.222 208.67.220.220
!
clock timezone EST -5 0
clock summer-time EDT recurring
!
ntp server south-america.pool.ntp.org
ntp server europe.pool.ntp.org
ntp server pool.ntp.org
ntp server us.pool.ntp.org
ntp server north-america.pool.ntp.org
!
```

Day 0 IOS XE Config (page 2)

- AAA, Local User
- NetConf-YANG
- YANG AAA

```
!
username timmyg privilege 15 secret 8 $8$CvofI3VTja.....
!
aaa new-model
!
aaa authentication login CON-LOCAL local
aaa authorization exec CON-LOCAL local
aaa authorization console
!
line vty 0 15
 login authentication CON-LOCAL
 authorization exec CON-LOCAL
!
netconf
netconf-yang
!
yang-interfaces aaa authentication method-list CON-LOCAL
yang-interfaces aaa authorization method-list CON-LOCAL
!
```

What is the IOS XE Attack Surface

What is the IOS XE Attack Surface

- Open UDP \ TCP Ports
- Network facing services not optimized
- Insecure Username and Password
- Con, Aux, VTY lines
- Clear text data in Transit

What is the Attack Surface of IOS XE

What UDP Ports are listening ?

```
Cat9300-1#show ip sockets
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 10:17:08.583 EDT Tue Apr 11 2023
------------------ show ip sockets  ------------------

Proto        Remote       Port      Local       Port  In Out  Stat TTY OutputIF
 17        --listen--          10.65.0.2        123   0   0 2001001   1
 17(v6)    --listen--          --any--          123   0   0 2020001   1
 17      0.0.0.0             0 10.65.0.2       2228   0   0   211   0
 17      192.168.10.24   65109 10.65.0.2        161   0   0 2001001   0
 17        --listen--          10.65.0.2        162   0   0 2001011   0
 17        --listen--          10.65.0.2      51161   0   0 2001011   0
 17(v6)    --listen--          --any--          161   0   0 2020001   0
 17(v6)    --listen--          --any--          162   0   0 2020011   0
 17(v6)    --listen--          --any--        49646   0   0 2020001   0
 17      192.168.10.11     514 10.65.0.2      50379   0   0 400210   0
Cat9300-1#
```

udp/123 - NTP

udp/2228 - L2 traceroute

udp/161, 162 - SNMP

What is the Attack Surface of IOS XE

What TCP Ports are listening ?

```
Cat9300-1#
Cat9300-1#sh tcp brief all
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 10:25:44.229 EDT Thu Apr 13 2023
------------------ show tcp brief all  ------------------

TCB       Local Address               Foreign Address             (state)
7084B6CD29B0  10.65.0.2.22               192.168.8.70.53784          FINWAIT1
7084B6D68898  10.65.0.2.22               192.168.8.70.57451          ESTAB
7084B4759950  ::.21111                   *.*                         LISTEN
7084B4755E20  0.0.0.0.21111              *.*                         LISTEN
7084AC737C18  ::.443                     *.*                         LISTEN
7084B3BF4C18  0.0.0.0.443                *.*                         LISTEN
7084AC737000  ::.80                      *.*                         LISTEN
7084B3BF4000  0.0.0.0.80                 *.*                         LISTENLoad for five secs: 0%/0%; one minute: 0%;
Time source is NTP, 10:25:44.277 EDT Thu Apr 13 2023
------------------ show platform software portinfo TCP ------------------
% Error: Failed to open portinfo output file.


Cat9300-1#
```

Default SSH Config

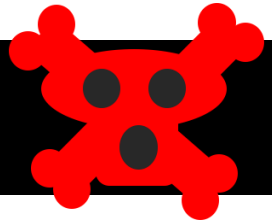
```
Cat9300-1#
Cat9300-1#sh ip ssh
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 10:57:00.307 EDT Mon Apr 17 2023
------------------ show ip ssh  ------------------

SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa
-sha2-nistp521,ssh-ed25519,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-e
cdsa-sha2-nistp521,rsa-sha2-256,rsa-sha2-512,x509v3-rsa2048-sha256
Hostkey Algorithms:rsa-sha2-512,rsa-sha2-256,ssh-rsa
Encryption Algorithms:chacha20-poly1305@openssh.com,aes128-gcm@openssh.com,aes256-gcm@ope
nssh.com,aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com
KEX Algorithms:curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha
2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): my-4096rsa-ssh-key
Modulus Size : 4096 bits
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDls7G6cS8k9ZBfgCAor2XbhQ20bidLB1gaVQ74Yon1
hPesx+LecWpSOkdA7QCWAMPDk1ARwspDChS7/8awamhpFPWZRa+msAC6nkC50KpQPR2MyqNjOeuceNn7
oLXT1/M5zYBB6D0AdNBjMA1PwoweDRqJjtXGvQZbX4daT6wvvVlAt6ZudDS1M+sTMWR6RPCgLOkdmKhM
```

Default HTTPS Config

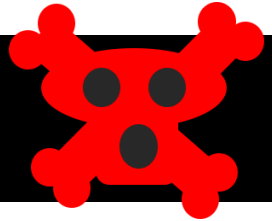
```
Cat9300-1#
Cat9300-1#sh ip http server status | beg HTTP secure
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite:  rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
        dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
        ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2 tls13-aes128-gcm-sha256
        tls13-aes256-gcm-sha384 tls13-chacha20-poly1305-sha256
HTTP secure server TLS version:  TLSv1.3 TLSv1.2
HTTP secure server client authentication: Disabled
HTTP secure server PIV authentication: Disabled
HTTP secure server PIV authorization only: Disabled
HTTP secure server trustpoint: TP-self-signed-4033093308
HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL
Cat9300-1#
```

IOS XE Local Passwords \ Secrets

```
Cat9300-1#
Cat9300-1#sh runn | inc username
username local-admin privilege 15 password 7 00071A1507545A545C
Cat9300-1#
Cat9300-1#
```



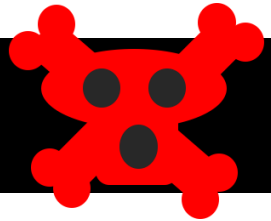
```
Cat9300-1#
Cat9300-1#sh runn | inc enable
enable secret 5 $1$ioti$MywYh5xXx4HAPpyEf77eQ.
Cat9300-1#
Cat9300-1#
```



Weak password hashing?
Weak methods for securing \ storing them?
Do these comply with business rules \ Password Compliance?

SNMPv2

```
Cat9300-1#
Cat9300-1#sh runn | inc snmp-server
snmp-server community MyBizNamePlus12345 RW
Cat9300-1#
Cat9300-1#
```



Ansible.cfg

```
timmay@ubuntu-01:/etc/ansible$
timmay@ubuntu-01:/etc/ansible$ cat ansible.cfg
[defaults]
inventory = ./inventories
timeout = 60
host_key_checking = false
forks = 25
command_timeout = 80
[persistent_connection]
connect_timeout = 60
timmay@ubuntu-01:/etc/ansible$
timmay@ubuntu-01:/etc/ansible$
```

Ansible Inventory \ Playbook Files

```yaml
---
iosxe:
  hosts:
    Cat9300-1:
      ansible_host: 10.65.0.2

  vars:
    ansible_network_os: ios
    ansible_user: ansible
    ansible_password: some-password-in-the-clear
```

Ansible Best Practices

SSH Key Checking

- Have you all seen this error ?
- First time Ansible connects to IOS XE, no host key

```
timmay@ubuntu-01:/etc/ansible$
timmay@ubuntu-01:/etc/ansible$ ansible-playbook -i inventories/cat9300-1v.yaml playbooks/show-serial.yaml --ask-vault-pass
Vault password:

PLAY [Define Parameters] ***********************************************************************************************
**************************

TASK [Get the facts] ***************************************************************************************************
***************************
fatal: [Cat9300-1]: FAILED! => {"changed": false, "msg": "\nlibssh: The authenticity of host '10.65.0.2' can't be established due to
'Host is unknown: 03:fc:b9:97:e3:42:be:1d:d4:55:19:63:88:5c:f2:e5:87:59:06:4a'.\nThe ssh-rsa key fingerprint is SHA1:s/y5l+NCvh3UVRlj
iFzy5YdZBko."}

PLAY RECAP *************************************************************************************************************
**************************
Cat9300-1                  : ok=0    changed=0    unreachable=0    failed=1    skipped=0    rescued=0    ignored=0

timmay@ubuntu-01:/etc/ansible$
```

The authenticity of host IP_ADDRESS can't be established due to Host is Unknown

SSH Key Checking

- Host key checking enabled by default

```
timmay@ubuntu-01:/etc/ansible$
timmay@ubuntu-01:/etc/ansible$ cat ansible.cfg | grep host_key_checking
host_key_checking = true
timmay@ubuntu-01:/etc/ansible$
timmay@ubuntu-01:/etc/ansible$
```

- Do NOT change this to false!
- Host keys stored in `~/.ssh/known_hosts`
- Use ssh-keyscan to ‘import’ the SSH host key!

SSH Known Hosts

- Host keys stored in ~/.ssh/known_hosts

```
GNU nano 4.8                                    /home/ciscolive/.ssh/known_hosts
```

1st host key — Hashed IP Addr \ Hostname

```
|1|cz9TY+PNWz7mm8/pQkRPWOE1oaU=|geksB4VwvGcURpXfx2u7b82eSyI= ssh-rsa AAAAB3NzaC1yc2EAAAADAQAE
```

Algorithm

2nd host key

```
10.1.1.5 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2Z1F8KECwluwLJ4VxeP91uHFkehyky3oxHGjLFexaKV2F
```

tcp/830 — Base64 Pub Key

```
[10.1.1.5]:830 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2Z1F8KECwluwLJ4VxeP91uHFkehyky3oxHGjLFe


|1|fuxSApwREqXhBANVXTMhoYq7zNk=|nt2/bcwepGjXa6DOecTbsK3l120= ssh-rsa AAAAB3NzaC1yc2EAAAADAQAE
```

5th host key, manually revoked

```
@revoked 10.1.1.55 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDeXTjtbHdjmHGEnzpH3qzgwgwvy+BnaUBh+N
```

You can also remove known host keys

```
ssh-keygen -f "/home/ciscolive/.ssh/known_hosts" -R "10.1.1.5"
```

ssh-keyscan options

- Let's add our 'unknown' device to ~/.ssh/known_hosts

```
ssh-keyscan -H {{FQDN or IP_ADDRESS}} >> ~/.ssh/known_hosts
```

```
timmay@ubuntu-01:/etc/ansible$ ssh-keyscan -H 10.65.0.2
# 10.65.0.2:22 SSH-2.0-Cisco-1.25
|1|mhQTwJdG8uisED+KeI7XSFk2S7E=|JHOJh62hnN4DfBfMaCoukJXsEYU= ssh-rsa AAAAB3NzaC1yc2EA
```

-H parameter will add Hashed IP Addr

```
ssh-keyscan {{FQDN or IP_ADDRESS}} >> ~/.ssh/known_hosts
```

```
timmay@ubuntu-01:/etc/ansible$ ssh-keyscan 10.65.0.2
# 10.65.0.2:22 SSH-2.0-Cisco-1.25
10.65.0.2 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC4b4j3sGxsc0IuZn+pMGswd2IxQV9/VfjrDna
```

```
ssh-keyscan -p 830 {{FQDN or IP_ADDRESS}} >> ~/.ssh/known_hosts
```

```
timmay@ubuntu-01:/etc/ansible$ ssh-keyscan -p 830 10.65.0.2
# 10.65.0.2:830 SSH-2.0-OpenSSH_7.9 PKIX[11.6]
[10.65.0.2]:830 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDbnvTIas5P5mpkrD3bdfZVrvxR4KTtWRUH/8FJ
```

NETCONF Port tcp/830

SSH Key Demo

ssh-keyscan Demo Steps

- Run simple playbook, watch fail

```
ansible-playbook -i inventories/cat9300-a.yaml playbooks/show-serial.yaml
```

- cat ~/.ssh/known_hosts
- ssh-keyscan 10.1.1.5
- ssh-keyscan 10.1.1.5 >> ~/.ssh/known_hosts
- ssh-keyscan -p 830 10.1.1.5 >> ~/.ssh/known_hosts
- nano ~/.ssh/known_hosts
- This only has to be done once!
- Run simple playbook, watch succeed

ssh-keyscan Demo Results


```
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
ciscolive@pod2-xelab:~/clus2023-devnet-2111$ ssh-keyscan 10.1.1.5
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
10.1.1.5 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC50NZ2EKMAVofhG47Im2TAxpYfV+ZeLG7ZdYiaM6E+BJxyuj27/+V0SnTSbNbXSXEcxDXMD
nvXJ9BzxjLiN16GOW9SdfLiNl9+KSrksCh58h/+SJqdI44mrMTIRylmcxd/5nzc3RPZhz9E0ncmskpvShtjE2uFn4oTvMiqi7QOKHRrGAOoEyG++a/4ED+
uTw5IJflvBqxDRZB8J1fAbs5Yjw6QacomR+PwKGPnfegDefJ1
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
```

```
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
ciscolive@pod2-xelab:~/clus2023-devnet-2111$ ssh-keyscan 10.1.1.5 >> ~/.ssh/known_hosts
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
# 10.1.1.5:22 SSH-2.0-Cisco-1.25
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
```

Ansible Vault Demo

Ansible Vault Demo Steps

- Show Inventory File, inventories/cat9300-a.yaml
- Discuss Username & Pass in the clear
- Remove U&P from Inventory
- Copy \ Paste into vaults/ciscolive.vault

```
ansible-vault encrypt vaults/ciscolive.vault
```

- Update Playbook

```
vars_files:
  - ~/clus2023-devnet-2111/vaults/ciscolive.vault
```

Secret Strength
&
Common Criteria
&
Local Users

Cisco Password Types

scan here for
config guide!!!

- 5,6,7,8,9 ??? What do we do ?

- Type 5 – MD5 hash, outdated, replace where possible
- Type 6 - reversable, Bulk Data Encryption, RADIUS, TACACS keys
- Type 7 - obfuscation, outdated stop using immediately
- Type 8 - HA256 Hash, NIST Approved!
- Type 9 - SCRYPT Hash, not NIST approved,

Common Criteria Policy

- Allows NetEng to enforce strong password policies on local users
- Enables InfoSec & Auditors to see validate password policy

```
Cat9300-1#
Cat9300-1#sh runn | section aaa common-criteria
aaa common-criteria policy COMMON-POLICY
 min-length 12
 max-length 127
 char-changes 5
 character-repetition 2
 restrict-consecutive-letters
Cat9300-1#
Cat9300-1#
Cat9300-1#
Cat9300-1#
Cat9300-1#
```

Password must contain at least 12 characters and no more than 127

PW change req's > 5 chars changed

Same character cannot be used 3x

qwer or asdf not permitted

Local Users

- Must use strong password, Common Criteria !!!
- Must use strong hashing algorithms, Type 8 NIST approved!
- Use masked-secret so ‘secret’ is NEVER displayed in the clear

```
Cat9300-1#
Cat9300-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cat9300-1(config)#username jhonny-apples common-criteria-policy COMMON-POLICY algorithm-type sha256 masked-secret
Enter secret: *****************
Confirm secret: *****************

Cat9300-1(config)#end
Cat9300-1#
Cat9300-1#show runn | inc jhonny-apples
username jhonny-apples common-criteria-policy COMMON-POLICY secret 8 $8$uDWzlCSGOwEgLE$m.QB4WF2pp1Fb2RxhYiYgw5x1wZrKE7
Cat9300-1#
```

Type 8

Password should never be displayed or logged

Secret Strength
&
Common Criteria
&
Local Users
Demo

PW Type & CC Policy User Demo Steps

- Show the PW Type & Common Criteria Playbook in VS Code
- Explain Connection Type = NETCONF
- Explain how the RPC was built in YANG Suite
- Run the PW Type & Common Criteria Playbook.

```
ansible-playbook -i inventories/cat9300-a.yaml playbooks/01-add-common-criteria-policy.yaml
```

- Note how we forgot to add --ask-vault-pass
- Run Playbook again with ask-vault this time ☺
- On Cat9K Show Common Criteria Policy

```
show runn | sec aaa common-criteria
```

Local User Demo Steps

- Creating this local user could occur on hundreds or thousands boxes
- We shouldn’t ever have the password displayed in the clear
- Show Playbook and Copy \ Paste Type 8
- Run Playbook

```
ansible-playbook -i inventories/cat9300-a.yaml playbooks/02-add-common-criteria-users.yaml --ask-vault-pass
```

- On Cat9K Show Newly Created Local User

```
show runn | inc username jhonny-apples
```

Harden
SSH & HTTPS

HTTPS Cipher Suites in IOS XE 17.11(1)

IOS XE Label	IANA Name	TLS Ver	Strength
aes-128-cbc-sha	TLS_RSA_WITH_AES_128_CBC_SHA	1.0	Weak
aes-256-cbc-sha	TLS_RSA_WITH_AES_256_CBC_SHA	1.0	Weak
dhe-aes-cbc-sha2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	1.2	Weak
dhe-aes-gcm-sha2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1.2	Secure
ecdhe-ecdsa-aes-gcm-sha2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	1.2	Recommended
ecdhe-rsa-aes-128-cbc-sha	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	1.0	Weak
ecdhe-rsa-aes-cbc-sha2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	1.2	Weak
ecdhe-rsa-aes-gcm-sha2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1.2	Secure
rsa-aes-cbc-sha2	TLS_RSA_WITH_AES_128_CBC_SHA256	1.2	Weak
rsa-aes-gcm-sha2	TLS_RSA_WITH_AES_128_GCM_SHA256	1.2	Weak
tls13-aes128-gcm-sha256	TLS_AES_128_GCM_SHA256	1.3	Recommended
tls13-aes256-gcm-sha384	TLS_AES_256_GCM_SHA384	1.3	Recommended
tls13-chacha20-poly1305-sha256	TLS_CHACHA20_POLY1305_SHA256	1.3	Recommended

CIPHERSUITE
https://ciphersuite.info

Harden SSH & HTTPS Demo

Harden SSH & HTTP Demo Steps

- Show the Hardening Playbook in VS Code
- On Cat9K Show SSH & HTTP Server Status

```
show ip http server status | sec ciphersuite

show ip ssh
```

- Run Playbooks

```
ansible-playbook -i inventories/cat9300-a.yaml playbooks/03-config-hard-ssh.yaml --ask-vault-pass

ansible-playbook -i inventories/cat9300-a.yaml playbooks/04-config-hard-https.yaml --ask-vault-pass
```

- On Cat9K Show SSH & HTTP Server Status

SNMPv2 vs SNMPv3

SNMPv2 Packet Capture

```
Tims-MacBook ~$
Tims-MacBook ~$snmpget -v2c -c cisco123 10.65.0.2 SNMPv2-SMI::enterprises.9.2.1.73.0
SNMPv2-SMI::enterprises.9.2.1.73.0 = STRING: "usbflash0:cat9k_iosxe.17.11.01.SPA.bin"
Tims-MacBook ~$
```

snmp

No.	Time	Delta	Source	SrcPort	Destination	DstPort	Protocol	Length	Info
164	2.924286	0.029298	192.168.10.181	59742	10.65.0.2	161	SNMP	89	get-request 1.3.6.1.4.1.9.2.1.73.0
165	2.925380	0.001094	10.65.0.2	161	192.168.10.181	59742	SNMP	127	get-response 1.3.6.1.4.1.9.2.1.73.0

```
> Frame 165: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface en4, id 0
> Ethernet II, Src: Cisco_4e:e6:c6 (2c:ab:eb:4e:e6:c6), Dst: Universa_b8:e0:64 (3c:e1:a1:b8:e0:64)
> Internet Protocol Version 4, Src: 10.65.0.2, Dst: 192.168.10.181
> User Datagram Protocol, Src Port: 161, Dst Port: 59742
v Simple Network Management Protocol
    version: v2c (1)
    community: cisco123
  v data: get-response (2)
    v get-response
        request-id: 857263308
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.4.1.9.2.1.73.0: "usbflash0:cat9k_iosxe.17.11.01.SPA.bin"
            Object Name: 1.3.6.1.4.1.9.2.1.73.0 (iso.3.6.1.4.1.9.2.1.73.0)
            Value (OctetString): "usbflash0:cat9k_iosxe.17.11.01.SPA.bin"
    [Response To: 164]
    [Time: 0.001094000 seconds]
```

SNMP Response

SNMPv3 Packet Capture

```
Tims-MacBook ~$
Tims-MacBook ~$snmpget -v3 -l authPriv -a SHA -u charlie-ReadOnly -A ciscolive123 -x AES -X ciscolive123 10.65.0.2 SNMPv2-SMI::enterprises.9.2.1.73.0

SNMPv2-SMI::enterprises.9.2.1.73.0 = STRING: "usbflash0:cat9k_iosxe.17.11.01.SPA.bin"
Tims-MacBook ~$
```

snmp

No.	Time	Delta	Source	SrcPort	Destination	DstPort	Protocol	Length	Info
51	3.175727	0.058855	192.168.10.181	49447	10.65.0.2	161	SNMP	186	encryptedPDU: privKey Unknown
52	3.176758	0.001031	10.65.0.2	161	192.168.10.181	49447	SNMP	223	encryptedPDU: privKey Unknown

```
> Frame 52: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface en4, id 0
> Ethernet II, Src: Cisco_4e:e6:c6 (2c:ab:eb:4e:e6:c6), Dst: Universa_b8:e0:64 (3c:e1:a1:b8:e0:64)
> Internet Protocol Version 4, Src: 10.65.0.2, Dst: 192.168.10.181
> User Datagram Protocol, Src Port: 161, Dst Port: 49447
v Simple Network Management Protocol
    msgVersion: snmpv3 (3)
  > msgGlobalData
  > msgAuthoritativeEngineID: 800000090300dc774c78f080
    msgAuthoritativeEngineBoots: 115
    msgAuthoritativeEngineTime: 2783
    msgUserName: charlie-ReadOnly
    msgAuthenticationParameters: fce6c75ab711a2dc760ea8cb
    msgPrivacyParameters: 271ce9e510efa310
  v msgData: encryptedPDU (1)
      encryptedPDU: fd65ee713ceda4dc42790d63e0ae409bd11203a5b1e0f56ca3ecb3e3ef3f42e2b043f46d…
```

SNMP Response

SNMPv3 Basics

- View – What OIDs can be queried
- Group – Logical grouping of users
- User – Assign a user for each SNMP Monitoring Workstation
  - Auth Protocol - MD5 \ SHA
  - Auth Key – Shared Secret, verifies the integrity of the messages
  - Privacy Protocol – DES \ AES-128 \ AES-192 \ AES-256
  - Privacy Key – Shared Secret, used for bulk data encryption

SNMPv3 Template Demo

SNMP Demo Steps

- Show SNMPv2 Config
- Run Simple SNMP Get

```
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
ciscolive@pod2-xelab:~/clus2023-devnet-2111$ snmpget -v3 -l authPriv -a SHA -U charli
snmpget:
Error generating a key (Ku) from the supplied privacy pass phrase.
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
ciscolive@pod2-xelab:~/clus2023-devnet-2111$
```

```
snmpget -v2c -c cisco123 10.1.1.5 SNMPv2-MIB::sysName.0
```

- Show SNMPv3 Playbook in VS Code
- Run Playbook

```
ansible-playbook -i inventories/cat9300-a.yaml playbooks/05-add-snmp-v3-
framework.yaml --ask-vault-pass
```

- Show SNMPv3 Config
- Run same Simple SNMP Get using SNMPv3

```
snmpget -v3 -l authPriv -a SHA -u charlie-ReadOnly -A ciscolive123 -x AES -X
ciscolive123 10.1.1.5 SNMPv2-MIB::sysName.0
```

Type 6 Encryption

Type 6 Encryption

- Supported since 2006 \ IOS 12.3 and possibly earlier
- Strong AES 128-bit encryption
- Encrypts RADIUS & TACACS, MACsec & IPsec PSK
- Type 6 passwords need to be reversed by IOS XE

Type 6 Demo

Type 6 Demo Steps

- Show Type 6 Playbook in VS Code
- Run Type 6 Playbook

```
ansible-playbook -i inventories/cat9300-a.yaml playbooks/06-config-type6.yaml --ask-vault-pass
```

- No Type 6 Passwords exist now

MACsec PSK

MACsec Switch to Switch with PSK

- Dance like no one is watching
- Encrypt like everyone is watching
- Lightweight L2 encryption
- Cat9K Line Rate encryption AES128 \ AES256
- <1% CPU Impact only during ReKey
- Bulk Data encryption occurs on PHY,

MACsec PSK Demo

MACsec Demo Steps

- Show MACsec Playbook in VS Code
- Run MACsec Playbook

```
ansible-playbook -i inventories/devnet-switches.yaml playbooks/07-config-macsec-psk.yaml --
ask-vault-pass
```

- Show MKA session on Cat9K
- Show MACsec session on Cat9K

Other Hardening Best Practices ...

- Harden NTP
  - Serve
  - Serve-Only
  - Querty
- VTY ACLs
- HTTP Modules
- Enable Config Archiving

3,2,1
Action Items

- Breathe, Relax
- Scan QR Codes
- Clone Git Repo
- Test Playbooks
- Execute

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

Lots of extra slides in this deck!

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

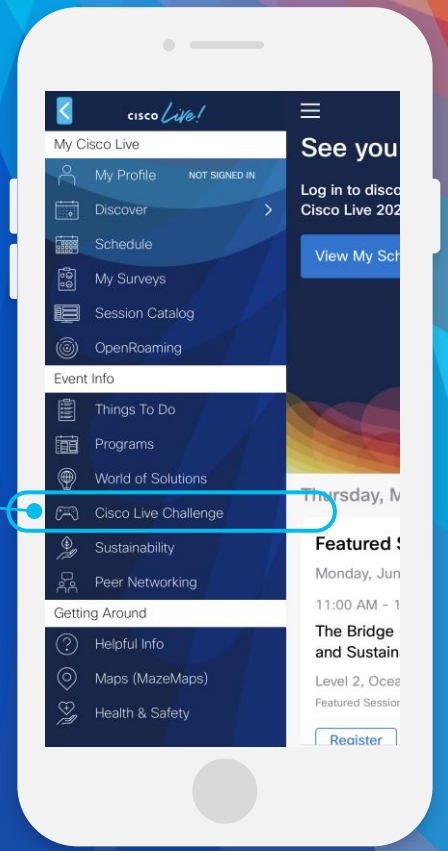
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

Let's go