4/5/25

Discord Unit 2 session

19:00 I must participate in the discussions
Last week ① Rate Yourself ② Post a job MUST DO
Unit 2 I ① How was week 1 ② ... ③ ...
II SELinux .....

Use screen or tmux to make sure you log/reload your commands
Console or IPMI
cd /etc/yum.repos.d ; dnf repolist
epel
#ip addr #ip route
#ip -br addr #ip neigh ⇒ shows app info
ESXi
Everything we do is either checking a value or setting values
/etc/nsswitch.conf
hosts: files dns
/etc/resolv.conf
nameserver 8.8.8.8
dig -t 6 www.yahoo.com
#systemctl status sshd
#ss -ntulp
#firewall-cmd --info-zone=public
ls /usr/lib/firewalld/services/ss*.xml
#nc hostname port#

The USE Method

Utilization - Resource busy time

S

E

minutes 1 thru 6

Security Unit 1 Video

COURSE
- HOW TO SECURE LINUX IN A CORPORATE ENVIRONMENT
- REGULATIONS, BEST PRACTICES & INDUSTRY STNDS
- CONCEPTS OF CONTROLS, THEIR IMPLEMENTATION & SECURITY POSTURE
- PRACTICE SECURELY BUILDING, DEPLOYING, INTEGRATING & MONITORING
- SECURITY DOCUMENTATION & REPORTING

- BUILD STANDARDS AND COMPLIANCE
- SECURING THE NETWORK CONNECTION
- USER ACCESS & SYSTEM INTEGRATION (LDAP, etc)
- BASTION HOSTS & AIR-GAPS
- UPDATING SYSTEMS AND PATCH CYCLES (LIFECYCLE MGMT)
- MONITORING & PARSING LOGS (KAFKA, LOKI, etc
- MONITORING AND ALERTING (KAFKA, LOKI, etc.)
- CONFIGURATION DRIFT & REMEDIATION
- CERTIFICATE & KEY MADNESS (we will build certs for earlier steps)

TWO PARTS TO OBJECTIVE
① Show you can do the specific buzzwords

- BUILD & CONFG LINUX SYSTEM TO ADHERE TO COMPLIANCE FRAMEWORKS
- INTEGRATING LINUX TO A NETWORK IN A SECURE FASHION
- INTEGRING LINUX W/ ENTERPRISE IDENTITY & ACCESS (IAM) FRAMEWORKS
- IMPLEMENT USER INGRESS CONTROLS TO A SYS/NET W/ BASTION FRAMEWORKS
- UPDATING LINUX TO RESOLVE SECURITY VULNS & REPORTING OUT TO SECURITY TEAMS
- DESIGN LOGGING WORKFLOWS TO MOVE EVENT LOGGING OFF for Real Time Monitoring
- MONITORING & ALERTING ON EVENTS IN LINUX
- MAINTAINING SYSTEM CONFIGURATION & REMEDIATING DRIFT

minute 10

Final Project - 15 to 20 pages

1. HIPAA Compliance Standard (or GDPR)
2. Build docs for HIPAA compliance
   a. explain/detail Risk analysis & management
   b. safeguards
      Admin
      Physical
      Technical
   c. Business Associate Agreements - "how we pass data between"
      "how we pass data between people
   Documentation Policies "how we handle, tag, ownership of data"
      Procedures "how we deploy, remediate, fix breach"
      Update & review cadence
3. Presentation "www.overleaf.com (Powerpoint)". 20 slide deck
   i. PURPOSE ii. DIAGRAM iii BUILD PROCESS iv WHAT I LEARNED v. FUTURE

* I have to deliver the slide presentation to Scott

minute 14~

Discussions

Topic 1 - What is Security

Topic 2 Find a STIG requirement I do not agree with

OVERVIEW

WHAT IS SECURITY

COMMON COMPLIANCE STANDARDS

TYPES OF CONTROLS

- DOWNLOADING
- REVIEWING
- SCANNING
- REMEDIATING
- REPORTING

CATEGORIES
- TECHNICAL
- MANAGERIAL
- OPERATIONAL
- PHYSICAL

CONTROL TYPES
- PREVENTATIVE
- DETTERENT
- DETECTIVE
- CORRECTIVE
- COMPENSATING
- DIRECTIVE

STIG OVERVIEW
- DOWNLOADING
- REVIEWING
- SCANNING
- REMEDIATING
- REPORTING

Drisc minute 29 ↓

POST #1

minute 28

Downlodd STIG VIEWER & MariDB 10x V2R3

1 Confidentiality: whose eyes can see the data
↳ The data must be categorized (H,M,L) & who owns, location

Integrity: who can change the data

Availability: Is the system available when we need it

AUTHORITY: Some that may or may not be respected

WILL: RESPECT OF AUTHORITY

FORCE: CONTROLS PUT INTO PLACE TO ENFORCE THE WILL OF AUTHORITY

↓ minute 34

TYPES

POST #2 → FIND AN EXAMPLE STIG TO DISAGREE WITH

1. WHAT IS THE STIG TRYING TO DO? e.g. managerial directive
2. WHAT CATEGORY & TYPE OF CONTROL e.g.
3. DEFEND WHY U THINK IT'S NOT NECESSARY e.g. Because it doesn't do anything that others do don't already do better

1. Same 2. managerial directive 3. Because it was tested in darknet & found to break the app. As a result Other → corrective controls were put in place to correct it like being air gapped or in a locked room

Digging Deeper

3. ALE: AVERAGE LOSS EXPECTANCY
   SLE: SINGLE LOSS EX
   ARO: AVERAGE RATE OF OCCURENCE

minute 37

LABS LAB 1

1.1 #mount | grep -i
1.2 #sysctl -a | grep -i ipv4
#lsmod | grep -i tables

2

3 #dnf install mariadb-server
#systemctl start mariadb ; systemctl status mariadb
#ss -ntulp | grep 3306
*NOTE GENERATE A NEW CHECKLIST IN STIG VIEWER
#mysql
> SELECT user, max_user_connections FROM mysql.user;
> GRANT USAGE ON *.* TO 'root'@'localhost'
WITH MAX_USER_CONNECTIONS 2;

UNIT 2

Categories of Controls
Technical - applied to system
Managerial } rules to respect
Operational } authority
Physical - applied to real world

(+)

Control types
Preventative
Deterrent
Detective
Corrective
Compensating
Directive

example

TECHNICAL ⊕ PREVENTATIVE CONTROL is a control placed on a system that prevents something from happening.
OPERATIONL ⊕ PREVENTATIVE CONTROL is a recommendation inside of a Std Operating Procedure stating that you DON'T DO (CERTAIN THINGS)
People either ⊖ Get around controls (easier to set around) e.g. find someone's user/pass on paper || ⊖ Or they Get Through Controls (hard - must defeat tech) hack/crack the system

---

TOPIC 1 - Stigs & their focus
TOPIC 2 - Name resolution in Linux - securing the network

How do we secure our network : stigs & tools
How do we verify the security settings : config ports, traffic flow
How do we report out the security settings : stig viewer

minute 7

DISCUSSION #1

401 STIGs for RHEL 9.

Search/Filter for sysctl shows 33

ssh shows 39

network 58

1. As Sys. engineers WHY ARE FOCUSED ON PROTECTING THE NETWORK PORTION OF OUR SERVER BUILDS?

   OUR NETWORK PORTION IS HOW WE INTERACT WITH THE SERVER AND HOW WE MAKE VALID CONNECTIONS TO THE SERVER

   HACKERS WILL ENTER SYSTEMS THROUGH NETWORK VULNERABILITIES

   THE NETWORK IS OUR PRIMARY INGRESS & EGRESS.

   OUR PRIMARY POINT OF FAILURE for UNAUTHORIZED ACCESS

2. WHY IS IT IMPORTANT TO UNDERSTAND ALL THE POSSIBLE INGRESS POINTS TO OUR SERVER THAT EXIST

   AND WHY IS IT SO IMPORTANT TO UNDERSTAND THE BEHAVIORS OF PROCESSES THAT ARE CONNECTING ON THOSE INGRESS POINTS

   *STRACE & LTRACE ALLOW US TO WATCH PROCESSES READ, WRITE & SYSTEM CALLS

DISCUSSION POST #2

READ ARTICLE ABOUT DNS NAME RESOLUTION & how it works

- DNS
- LOCAL HOST CONFIGURATIONS

1. WHAT IS THE SIGNIFICANCE OF THE NSSWITCH.CONF FILE

2. WHAT ARE SECURITY PROBLEMS ASSOCIATED WITH DNS AND COMMON EXPLOITS?

DIGGING DEEPER

1. LOOK FOR DIAMOND MODEL OF INTRUSION reports about DNS exploits
   ↳ past primary actors & actions from previous attacks

THE AVAILABILTY IS THE NUMBER ONE KEY PERFORMANCE INDICATOR
→ AVAILABLE & NOT COMPROMISED

minute 15

LAB

© # sysctl -a | grep -i ipv4 | grep -i forward
net.ipv4.ip_forward = 0
martian ③ panic ④ crypto
cat /proc/cmdline
fips-mode-setup --check
cat /etc/selinux/config

CAN YOU VERIFY SELINUX STATUS ?
CAN YOU VERIFY FIPS STATUS ? FIPS 140-2

STIGS are released quarterly (3 months- so stay current

ssh via putter to his hammerlab
Examine STIG V-257957 ⇒ Create a checklist in the app ⇒ Read STIG
sysctl -a | grep -i syncookies
↳ net.ipv4.tcp_syncookies = 1
Update the STIG with the output ⇒ Right click to mark as not a finding
rpm -qa | grep -i firewall ⇒ Update STIG w/ output & mark
systemctl status firewalld ⇒ Update STIG w/ output & mark
grep nftables /etc/firewalld/firewalld.conf ⇒ " " "
ss -ntulp | grep node-exporter
firewall-cmd --get-services | grep -i node-exp
ls /usr/lib/firewalld/services | node-exp
firewall-cmd --info-zone=public
firewall-cmd --permanent --add-service=prometheus-node-exp
↳ firewall-cmd --reload
firewall-cmd --list-services

Adding any new firewall ports can be done by pushing out a firewall rule using xml file

#cd /usr/lib/firewalld/services

↳ this is where all the files live

vi <------>.xml

```
<service>
    <short> this is the name of the service listed in checks </short>
    <description> ... </description>
    <port protocol="tcp" port="#####" />
</service>
```

— X — AUTOMATE STIG REMEDIATION

#mkdir -p /root/stigs ; cd /root/stigs

#wget -O U_RHEL_"9_V2R3"_Ansible.zip https://dl.dod.... zip

#unzip U_RHEL... ; mkdir ansible ; mv ... ; cd ... ; unzip ...

#cd /root/stigs/ansible/roles/rhel9STIG/

#ls defaults/main.yml tasks/main.yml

— X — OPENSCAP

#mkdir /root/openscap ; cd /root/openscap ;

#dnf -y install openscap-scanner openscap-utils open... guide

#openscap xccdf generate fix --profile ospp --fix-type ansible > d-d-r.yml

#openscap xccdf generate fix --profile ospp --fix-type bash > d-d-r.sh

end video

8pm 4/12

LINUX SECURITY ENGINEERING
UNIT 3

Last Week - SHgs • Name resolution •
NOTE CrowdStrike • Nessus • ⇒ Apps that get root access
How DOES A CONNECTION HAPPEN? SSH, PAM, SSSD, Active Directory
Microsoft has 99% market share - Active Directory & SSSD essential
LDAP server
FINAL PROJECT - HIPAA Compliance
5 policies & 5 procedures - > Linux Focused
& IN SECURITY - YOU HAVE TO BE A BLOWHARD
YOU HAVE TO BE A SELF-ASSURANCED POMPOS type of person
*Everyone in that field thinks their perfect & act that way
↳ SECURITY IS NOT FOR ME
ROCKYLINUX.ORG / GUIDES / SECURITY / PAM
↳ Answers to the Unit 3 Discussion Post 1

UNIT 3 D.P. 3
1. → Because I dont want to have to manage passwords
2. → Real & (ex) (dev home dirs are usually shared but no shared prod home dir)
SSSD allows you to trust to allow someone to get into your system
(lock box with a key (

Digging Deeper
/etc/security/access.conf
↳

Archer - big companies use

Have to turn off the wareuilt client

#systemctl stop wwclient

edit /etc/hosts & append to host entry

↳ ldap.prolug.lan ldap

#dnf

#dnf

#dnf

#systemctl start slapd

#ss -ntulp

#firewall-cmd --add-service

#firewall-cmd --reload

--list-all

#slappasswd

#salted password ⇒ save this output Keep into a file

#vi ↳

#ldapadd -Y

:

#edit the olcRootPW (in set domain.ldif) to the salted PW

#ldapadd * -D

#ldapadd

#Active Directory is more important than ldap itself

LSE

UNIT 3

PAM - Privileged access management

173P1 → 16 Stgs involving PAM for RHEL 9

1. What are the mechanism & how do the affect PAM functions

auth AUTHENTICATION (with a password by db or authserver; setting)

account AUTHORIZATION, ACCOUNT MANAGEMENT (time restrictions)

session relates to setup (logging) & termination

password UPDATE OF CREDENTIALS (auth token expiration or change)

a. Review /etc/pam.d/sshd; what is happening in that file?

2. What are the common PAM modules?

pam_unix - standard (authentication w/ getpwd) function

pam_

pam_

pam_ nologin

pam_ limits

extra: What are the control flags (these are success checks)

required IF SUCCESS THEN CONTINUE & ALLOW. IF FAIL THEN REJECT AFTER ALL

requisite IF SUCCESS THEN CONTINUE TO NEXT. IF FAIL THEN REJECT ASAP

sufficient IF SUCCESS THEN IMMEDIATELY ALLOW & SKIP THE REST OF CHECKS

optional THE RESULT IS IGNORED

include THIS JUST INCLUDES CONFIG FILE ENTRIES

substack THIS INCLUDES " " " "

3. Look for a blog/article discussing PAM

V3P2 Read about AD (active directory)
LDAP (lightweight directory access protocol)

1. Why do we want more than just local authentication

2. There are 4 SSSD strgs
   a. What are they? what do the do ltx

V-258123 • RHEL-09-611170 - cert status checking
V-258131 • RHEL-09-631010 - validate via certification path to trust
V-258132 • RHEL-09-631015 - map identity to usr/grp acct
V-258133 • RHEL-09-631020 - reset cached auth. each day

This is the wrong set

Minute 13 ⇒ COURSE FINAL PROJECT HINTS & NOTES
↳ SLIDESHOW of 20 pages

V-258019 • RHEL-09-271045 - ability to initiate a session lock
V-258122 • RHEL-09-611165 - enable cert based smartcard auth MFA
V-258123 • RHEL-09-611170 - implement cert. status checking via hardware token
V-258133 • RHEL-09-631020 - reset all cached authenticators each day

LSE

UNIT 4

Last week Topic1 PAM Topic 2 SSD & AD
Identity and Access Management

This Week
Air gap - ① Some way to get in there ② Ingress & Egress via Bastion
↳ still have to have a way
Talking Users -

Bastion hosts -

& THIS WEEK'S LAB USES KILLER CODA

What is an AIR GAPPED SYSTEM
- Really Secure

What is a bastion system
It's the way that we let everybody into our network

What is a jailed process?
- Via a chroot environ.

— X —

10GB vs 100GB vs 400GB (INFINIBAND)

Air gapped system benefits

- ENHANCED SECURITY
- PROTECTION AGAINST REMOTE ATTACKS ! MAJOR BENEFIT!
- MALWARE PROTECTION ?
- DATA EXFIL PREVENTION ! MAJOR BENEFIT!
- DATA INTEGRITY
- REGULATORY COMPLIANCE
- LAST LINE OF DEFENCE

JAILING IN LINUX

- CHROOT JAIL - SYSTEM SEES A FAKE (GOLD) ROOT FILESYSTEM
- LINUX CONTAINERS - LEVERAGE Cgroups & NAMESPACES for ISOLATION
  - ↳ NAMESPACES : Virtualize various system resources
  - ↳ Cgroups

Outside System → SSH → Bastion System → Backend system
Jailed user ⇢ Unjailed user

LSE

UNIT 3 Recatch

LAST WEEK

TOPIC 1: STIGs & focus on networking
TOPIC 2: DNS & name resolution

THIS WEEK

TOPIC 1: PAM
TOPIC 2: SSSD & Active Directory (trust outside of Linux for centralized auth)

OVERVIEW
HOW DO WE SECURE OUR NETWORK RELEVANT STIGs & TOOLS
CONNECTING TO OPENLDAP via SSSD

U3 DP1 - PAM (1) MECHANISMS: ① AUTH ② ACCOUNT ③ SESSION ④ PASSWD
(2) Various/Many different PAM modules
(3) BLOG POST - *I NEED TO EDIT & SUMMARIZE ** EDIT DISCORD
U3DP2 - AD with SSSD
FINAL PROJECT - HIPAA "How your systems handle data
2. WE ARE BUILDING DOCUMENTATION ABOUT RISK ANALYS & MGMT
*WE ARE GOING TO KEEP TRACK OF RISK IN OUR SYSTEMS
*) BY HARDENING THE SYSTEMS & HAVE A VULNERABILITY MGMT PROGRAM
SAFEGUARDS - On the Linux side what are we doing "Administrative i. Physical ii. Technical
Admin - managerial & operational */. Physical - how do we physically stop things
Technical - how do we technically stop things
BUSINESS ASSOCIATE AGREEMENTS - understand that we need a reciprocal agreement before we send data anywhere that & assurance that the other side will do the
- MINIMUM OF 5 FIVE POLICIES
- PROCEDURE
- UPDATE & REVIEW CADENCE

LAB - OpenLDAP Setup

1. Stop the warewulf client for this lab because I'll use
   #systemctl stop wwclient
2. Edit /etc/hosts & append to name of this specific host
   ↳ "ldap.prolug.lan ldap" (& note) "ldap.ldap.lan" mistake in later step
3. Setup dnf repo
   #dnf config-manager --set-enabled plus
   #dnf repolist
   #dnf -y install openldap-servers openldap-clients openldap
4. Start slapd
   #ss -ntulp ; #systemctl start slapd ; #ss -ntulp
   ↳ now you see processes listening to ports 389 & 636
5. Allow ldap through the firewall
   #firewall-cmd --add-service={ldap,ldaps} --permanent
   #firewall-cmd --reload
   #firewall-cmd --list-all
   #ls -l /usr/lib/firewalld/services/ldap*.xml
6. Generate a password e.g. "testpassword"
   #slappassword => enter "testpassword" twice
   ↳ Copy the output {SSHA}.....
6. Change the password by editing changerootpass.ldif
   #vi changerootpass.ldif
   ↳ dn: olcDatabase={0}config,cn=config
   changetype: modify
   replace: olcRootPW
   olcRootPW: {SSHA}.....

6. Change the password continued

```
#ldapadd -Y EXTERNAL -H ldapi:/// -f changerootpass.ldif
```

*see files /lab_work/identity_and_access_management.tar.gz

7. Generate the basic schema

```
#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

8. Setup the domain use the earlier password {SSHA}.....

```
#vi setdomain.ldif
```

↳ dn: olcDatabase={1}monitor, cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by
dn.base="gidNumber=0+.....
read by dn.base="cn=Manager, dc=prdug, dc=lan" read by * none
:
dn: olcDatabase={2}mdb, cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}.....
:
olcAccess: {2}to * by dn="cn=Manager, dc=prdug, dc=lan" write by * read

```
#ldapmodify -Y EXTERNAL -H ldapi:/// -f setdomain.ldif
```

↳ see output

```
#ldapsearch -H ldapi:// -x -s base -b "" -LLL "namingContexts"
```

9. Add the base group and organization

#vi addou.ldif

↳ dn: dc=prolug,dc=lan

⋮

ou:Group

#ldapadd -x D cn=Manager,dc=prolug,dc=lan -W -f addou.ldif

↳ enter the password

↳ see output

#ldapsearch -H ldap:// -x -s base -b "" -LLL "+"

#ldapsearch -x -b "dc=prolug,dc=lan" ou

↳ see output

10. Add a user

#ldappasswd

↳ enter password e.g. test1234

↳ save output of hashed string {SSHA}.....

Edit file

#vi adduser.ldif

↳ dn: uid=testuser,ou=People,dc=prolug,dc=lan

⋮

userPassword:{SSHA}.....

⋮

memberUid: testuser

#ldapadd -x -D cn=Manager,dc=prolug,dc=lan -W -f adduser.ldif

↳ enter main password

#ldapsearch -x -b "ou=People,dc=prolug,dc=lan"

↳ see output

11. Secure the system with TLS *accept all the defaults / hit enter*

```
#openssl req -x509 -nodes -days 365 -newkey rsa:2048
  -keyout /etc/pki/tls/ldapserver.key
  -out /etc/pki/tls/ldapserver.crt
```

↳ accept all defaults by adding enter or INPUT CORRECT INFO
↳ #this creates a self signed cert*

```
#chown ldap:ldap /etc/pki/tls/ldapserver.crt
#chown                          /ldapserver.key
#ls -l /etc/pki/tls/ldap*
```

↳ ldapserver.crt is a public file & ldapserver.key is the private key for ldapsrv

```
#vi tls.ldif
```

↳ dn: cn=config
⋮
olcTLSCACertificateFile: /etc/pki/tls/ldapserver.crt
⋮
olcTLSCertificateKeyFile: /etc/pki/tls/ldapserver.key
⋮
olcTLSCertificateFile: /etc/pki/tls/ldapserver.crt

```
#ldap -Y EXTERNAL -H ldapi:/// -f tls.ldif
```

12. Fix the /etc/openldap/ldap.conf to allow for certs

```
#vi /etc/openldap/ldap.conf
```

↳ TLS_CACERT /etc/pki/tls/ldapserver.crt
↳ TLS_REQCERT never
↳ BASE dc=prolug,dc=lan
↳ URI ldap://ldap.prolug.lan/
? evtlc or ldap ?

17. Restart
#systemctl restart slapd

SSSD Configuration and Realmd join to LDAP

18. Install sssd, configure & validate that the user is seen by system
#dnf install openldap-clients sssd sssd-ldap
#dnf install oddjob-mkhomedir authselect
#authselect select sssd with-mkhomedir --force
#systemctl enable --now oddjobd.service
#systemctl restart oddjobd.service
#systemctl status oddjobd.service
19. vi /etc/sssd/sssd.conf
↳ id_provider = ldap *or AD *since AD is prevalent
⋮
homedir_substring = /home
#chmod 0600 /etc/sssd/sssd.conf
#systemctl start sssd
#systemctl status sssd
20. Validate that the user can be seen
#id testuser
↳ see output

LSE

UNIT 4 FIRST YOUTUBE RECORDING

LAST WEEK

TOPIC 1 : PAM.

TOPIC 2 : LDAP, SSSD & ~~Active~~ Directory

THIS WEEK

TOPIC 1 : AIR GAPPED SYSTEMS ; BASTION HOSTS entry to air gapped

TOPIC 2 : JAILING USERS

WHAT IS AN AIRGAPPED SYSTEM

↳ A system that is completely separated/away from other systems

↳ so that the person inside cannot cause damage

↳ we put it in it's own network & limit ingress & egress

BENEFITS OF AIRGAPPED

Allows us to slow down our patching timeline / slow upgrades

TECHNICAL + PREVENTATIVE CONTROL -

↳ It forces users to come in only by our predefined method

* A good bastion means we don't need a zero trust

NOTE! ZERO-TRUST IS considered A GOOD THING (put on resume)

WHAT IS A BASTION SYSTEM

A BASTION SYSTEM IS THE ROUTE WE ALLOW USERS TO COME IN

IT'S THE ONE SECURE INGRESS & EGRESS

IT'S AN AREA WE CAN EASILY DEFEND. IT'S A PLACE WE CAN LOCK DOWN.

WHAT IS A JAILED PROCESS

WE USE CHROOT TO JAIL PROCESSES SO THEY CAN'T ACCESS FULL SYSTEM

USERS OF THE JAIL CAN'T ACCESS NORMAL COMMANDS NOR FILESYSTEM

* SO WE need to provide the necessary files, binaries, etc.

NO real world SYSTEM IS FULLY AIRGAPPED → they have some access to other machine

AN AIRGAPPED SYSTEM IS A COMPUTER NETWORK OR SINGLE COMPUTER, THAT IS PHYSICALLY ISOLATED, FROM ALL OTHER NETWORKS, INCLUDING THE INTERNET AND ANY LOCAL AREA NETWORKS.

THIS ISOLATION IS ACHIEVED BY *ONLY ALLOWING TRAFFIC IN AND OUT VIA INGRESS/EGRESS POINTS THAT WE DEFINE.

(BUT PEOPLE OFTEN SAY - AIR GAP HAS NO NETWORK INTERFACES CONNECTED)

IT'S LIKE A CHOKE POINT A SINGLE POINT OF ENTRY/EXIT

BENEFITS

- ENHANCED SECURITY - KEEP SYS ON OLDER STABLE RELEASE
- PROTECTION AGAINST REMOTE ATTACKS - SINGLE POINT OF ENTRY
- MALWARE PREVENTION - MALWARE CANT COMMUNICATE TO EXTRANET
- DATA EXFILTRATION PREVENTION - MALWARE CANT EXFIL DATA
- DATA INTEGRITY
- REGULATORY COMPLIANCE - REASON TO PROVE COMPLIANCE
- LAST LINE OF DEFENSE - CUT THE BASTION FROM REAL AIRGAP TO STOP BACKFLOW (PULL UP THE DRAW BRIDGE)

JAILING

TECHNIQUES TO ISOLATE A SET OF PROCESSES FROM THE REST OF THE SYSTM

CHROOT JAIL: system sees the root filesystem but is actually an inner directory

SSHD supports this natively e.g. /var/chroot

LINUX CONTAINERS: MORE ADVANCED THAN SIMPLE JAILING

LEVERAGES cgroups & namespaces for isolation

NAMESPACES: VIRTUALIZE VARIOUS SYSTEM RESOURCES

ISOLATE VARIOUS SYSTEM PROCESSES

cgroups (CONTROL GROUPS): LIMIT CPU, I/O, MEMORY OF A GRP OF PROCESSES

LSE

PRE DEPLOY STEPS

Write a bastion.sh script

FULL BASTION DEPLOY STEPS

1. CREATE USER/USERS TO JAIL
2. CREATE A LINE IN /etc/ssh/ssh_config for the jailed user(s)
3. SET THE USER TO HAVE THE BASTION.SH SHELL AS THEIR HOME
4. CREATE THE JAIL IN /var/chroot
   a. FIVE DIRECTORIES - Create these 5
      /var/chroot/bin /var/chroot/lib64 /var/chroot/dev
      /var/chroot/etc /var/chroot/home /var/chroot/usr/bin
   b. COPY IN THE CORRECT EXECUTABLE FILES
      BASH SSH CURL
   c. COPY OVER THE LIBRARY FILES FOR THE ABOVE EXECUTABLES
      #ldd /usr/bin/bash → to see the needed library files
   d. MAKE THE DEV DEVICES SO THE USER ENVIRON WORKS
      /var/chroot/
      ↳ dev/null ↳ dev/tty ↳ dev/zero
      ↳ dev/random ↳ dev/urandom

V4DP1

Review 2 blogs about air

① WHAT SEEMS TO BE THE THEME OF AIR-GAPPED SYSTEMS

② WHAT SEEMS TO BE THEIR PURPOSE

③ WHAT DOES GOOGLE SAY ARE COMMON THEMES

V4DP2

SEARCH GOOGLE TOPICS around JAILING A USER OR PROCESSES

① CAN YOU LIST/ENUMERATE THE METHODS OF JAILING USERS

② CAN YOU THINK OF THE USEFUL WAYS TO USE A JAIL

LSE

UNIT 5

TOPIC 1 - BUILD REPOS
TOPIC 2 - ENTERPRISE PATCHING
LAB - REPOS & PATCHING • WORKSHEET

WHAT IS CONTROL ① HOW SOFTWARE GETS ONTO OUR SYSTEMS
② HOW WE CONTROL THE SOURCE OF SOFTWARE
* We offer control over the stability of our systems

WHAT IS FIT FOR USE ① THE CHECKBOXES WE MAKE AS ENGINEERS
e.g. ☐ APACHE vs ☑ HTTD • PORT ☐ 80 ☑ 443
* We go through all the options & make choices ("check boxes")

WHAT IS FIT FOR WARRANTY ① DO I BET MY WEEKEND EVERYTHING IS OK
IS EVERYTHING WORKING & WILL IT CONTINUE RUNNING

WHY DO WE CREATE LOCAL REPO'S ① TO CONTROL SOFTWARE INSTALLED
② CONTROL THE CONTENT & WHO HAS ACCESS TO SOFTWARE INSTALLED

HOW DOES ENTERPRISE PATCHING DIFFER FROM ONE-OFF PATCHING
?? ONE OFF IS EASY 1 time vs ENTERPRISE PATCHING DEV-INT-QA-PROD

LIFECYCLE ENGINEERING ⇒ PATCHING LIFECYCLE
① SHORT LIVED vs ② ??

REPOSITORIES ⇒ WE HOST .ISO OR RPM
* We can mount .ISO over IPMI devices, NFS shares
* We can create the xml files "createrepo" to turn rpms into a repo
repomd.xml ⇒ dnf or yum

Satellite
↳ Pulp - patch & content management
↳ Candlepin - subscription & entitlement management
↳ katello - unified workflow & web UI (Pulp + Candlepin)
↳ Foreman - provisioning & configuration management

PATCHING CYCLE

PATCHING THE ENTERPRISE (multiple challenges)

- Incomplete Inventory - we need to know all our machines & have access to them
- multiple machines of unknown states - we need to keep them up during patch
- point to a controlled repo - if we don't control the repo, dev vs prod will become out of sync
- patch dev & uat before prod - DEV → TEST → QA → PROD, PROD is customer facing

PATCHING THE ENTERPRISE

① We download Vendor Patches to our servers
↳ Download into Satellite & call it Lifecycle May2025
↳ CVE, Bugfix, Grata, Security Updates; Kernel patches
↳ So we download, EVERYTHING, on a specific date to our local REPO

② We release/apply those patches into a dev environment
↳ "Smoke test" - see if these patches break anything
*this is backwards in my opinion (uat/test is better)
↳ Have stakeholders test & validate the patches/updates

③ Release/apply to QA / Test environments
↳ Staging, UAT (Testing, Validation - Change Management/CAB approval)

④ Deploy/release/apply to PROD
Apply Patches, Monitoring
Load & actual user testing of PROD
Rollback change if not validated

CIA triad - keep servers up.