Chapter 1

Wednesday, July 26, 2023 11:17 AM

Solid understanding of security goals, basic risk concepts

- security controls
- Windows/Linux cli tools
- logs and logging tools

Understanding core security Goals

security has several principles that orgs include as goals drive security decisions

CIA

What is a use case?

CompTIA uses term use case in many objectives

use case - a goal that an org wants to achieve

ex: use to identify/clarify goal

verb-noun format

"Place Order" use case in ecommerce site

"Place Order" use case in ecommerce site

Actors - customers, registered users, or the billing system

precondition - must occur before process can start
need to select item before purchase

trigger - starts use case
click on shopping cart

postcondition - after actor triggers process
order is placed in system after purchase

normal flow - use case lists steps in specific order

alternate flow - not all scenarios will be same

(not all elements of a use case security+ only requires to be familiar w/ use cases

Ensure confidentiality

confidentiality - prevents unauthorized

Ensure [illegible]

confidentiality - prevents unauthorized disclosure of data

Encryption

encryption - scrambles data to make it unreadable by unauthorized parties

only parties can decrypt

algorithms like Advanced Encryption Standard AES

EX: need to transmit PII

encrypt email to protect confidentiality

Access Controls

identification, authorization, and authentication provide access controls and help ensure authorized personnel view data

identification - user claim identity with a username

authentication - users prove identity with authentication, like a password

authorization - grant or restrict access [illegible] with authorization like

authorization - G...
to resources with authorization
permissions

Remember

confidentiality ensures data is only visible to authorized users

best way to protect confidentiality is with encryption

access controls help protect conf by restricting access

Provide Integrity

integrity - provides assurance that data has not changed
no unwanted mods, tamper, or delete
only auth user can modify

hashing techniques can enforce integrity

secure hashing algorithm SHA
creates fixed length irreversible output, given data
... in data will have

output, or

any changes in data will have different hash

variation in hashes tells you that it has been changed but not how

can also be used to verify integrity when downloading files

ex: verify that not a single bit of program was lost during download

Remember

integrity verifies that data has not been modified

hashing verifies integrity

Increase Availability

availability - data and services are available when needed

can be as simple as needed during 9a - 5p, M-F

and

can be
QA - SP, MI - F

orgs implement redundancy and fault tolerant methods

also ensure systems are patched with latest updates to avoid crashes due to bugs

remember

availability ensures systems are up and operational when needed

addresses single points of failure

add fault tolerance and redundancies

RAID, failover clusters, backups, generators

Redundancy and Fault Tolerance

redundancy - adds duplication to crit systems and provides fault tolerance

allows service to continue without interruption

common goal of redundancy and fault tolerance is to remove single points of failure SPOF - if it

single system does

points of

fails, whole system does

common examples

disk redundancies - fault tolerant disks

RAID-2 mirroring

RAID-5 striping with parity

RAID-10 striping with mirror

continue to operate even when disk fails

server redundancies - failover clusters include redundant servers, operate even if server fails

failover cluster - switch from failed server to operational server in same cluster

virtualization can help too

network redundancies

load balancing - use multiple servers to support single service like high volume website

Network interface card NIC

teaming - provides redundancy and increased bandwidth

and increased

power redundancies - uninterruptible power supplies UPS, and power generators provide power to key systems

Scalability and Elasticity

scale up by adding additional hardware resources (like mem, power, bandwidth, drive space

scale out by adding additional nodes or servers

can also scale down or in

static - scale up/out manually

dynamic - auto

Remember

redundancy and fault tolerance increase availability

scalability manually adding ... resources to systems

scalability manual
or removing resources to systems
to scale up or out
elasticity is dynamically
adding or removing resources
to system to scale if

scalability - systems ability to
handle increased workload
by scaling up or out

manual

elasticity - ability of system to
handle increased workload
by dynamically scaling up
or out

Cloud resources

Patching

patching systems through patch
management systems help

management system
availability

Understanding Resiliency

current trend is resiliency over high availability

99.999% (five 9) uptime is possible but requires removing all SPOF and multiple redundancies

high cost or total cost of ownership TCO

resilience methods - help systems heal and recover with min downtime

- backups
- power sources
- NIC teaming
- RAID

also expect components to retry failed processes

Resource versus Security Constraints

Resource versus Security Constraints

orgs need to balance resource availability with security constraints

Ex: why not encrypt all data?
encryption consumes resources
encrypting data typically increases size by 40%

Introducing Basic Risk Concepts

reducing risk is basic goal of implementing IT security

risk - possibility or likelihood of threat exploiting a vulnerability, resulting in loss

threat - any circumstance or event that can compromise CIA

vulnerability - weakness that threat can exploit

i.e. - threat exploits a vulnerability

if a threat exploits a vulnerability it can result in a security incident - adverse event that can impact CIA

threats can be
- inside org (employee)
- outside org (attacker)
- natural disaster
- human made malware
- intentional
- accidental

risk mitigation - reduces chance of threat exploiting vulnerability
reduce risk by implementing controls

Remember
Risk is likelihood that threat will exploit vulnerability
risk management reduces ...ances of threat exploiting ...es impact

risk management

chances of threat exploiting vulnerability, or reduces impact of risk with controls

Understanding security controls

need to know control types and categories

Control categories

managerial controls - primarily administrative in function typically documented in security policy and focus on managing risk

operational controls - help ensure day-to-day operations of organization comply with security policy. People implement

technical controls - use tech like hardware, software, firmware to reduce vulnerabilities

control types

[illegible] controls - occurring

control types

preventative controls
prevent incident from occuring

detective controls
detect incidents before they occur

corrective controls
reverse impact of incident

deterrent controls
discourage individuals from causing incident

compensating controls
alt controls used when primary control not feasible

physical controls
controls you can physically touch

Managerial controls

administrative function and documented in security policy

planning and assessment methods to provide ongoing review of risks to reduce and

to provide [illegible] org's ability to reduce and manage risk

Vulnerability assessments attempts to discover current vulnerabilities

if necessary add more controls

Risk assessment - quantify and qualify risks within an org to focus on serious risks

quantitative - cost and asset values to quantify risks

qualitative - uses judgements to categorize risks based on probability and impact

Remember

Managerial controls are admin and documented in security policy

Operational controls are implement [illegible] who perform day [illegible]

Operational
by people who perform
to day operations to comply
with security policy

Operational controls
implemented by people
ensure day to day ops comply
with security plan

NIST and SP 800 Documents
National institute of standards
and technology NIST
part of US commerce dep
computer security division hosting
information technology lab
ITL

ITL posts special publications
SPs 800 series important
for security
use docs to design secure
systems and networks

use docs to verify IT systems and networks

SP 800-53 rev. 5
security and privacy controls
security controls grouped into families
ex: Access control family
AC-1 – AC-25

Operational control families

- Awareness and training
  - pword making
  - clean desk policy
  - phishing and malware awareness
- configuration management
  - use baselines to ensure systems start in secure, hardened state
  - change management - ensure changes don't result in config errors

changes don't ... unintended config errors

- media protection
  physical media
- physical and environmental protection
  physical controls like cameras, doors, locks
  environmental controls like heating/vent

Remember
Managerial - documented in written policies
Operational - day to day ops
Technical - implemented with tech

Technical controls
... tech like hardware, software,

Technical

use tech like hardware, software and firmware

admin installs and configures tech controls then they protect auto

technical controls examples

- encryption - strong control for confidentiality
- antivirus - provides protection against malware
- IDS/IPS - monitor networks for protection from ongoing threats
- firewall - network files filter traffic going in/out
- least privilege - least privilege needed to do job

Control types

n to perform

Control types

Controls designed to perform specific functions in relation to security incidents

Preventative Controls

prevent security incidents

Hardening - making a system or app more secure than its default state

defense in depth or layered

- disabling ports
- secure protocols
- patches
- Strong pword
- disable accounts

training - ensure users aware of vulnerabilities and threats

security guards - prevent access into secure areas

into secure areas

Change management - changes dont result in unintended outages

account disablement policy - disable accounts when employees leave

IPS - block malicious traffic before reach network

Remember

preventative controls try to prevent incident from happening

- hardening
- guards
- change management
- account disablement

Detective controls

detect when vulnerabilities have exploited

detect when ...
been exploited

discover event after it has occurred

log monitoring - logs record system and network activity some can auto detect incidents

SIEM - monitor logs, detect trends, and raise alerts

security audit - examine security posture of org determine if policies implemented correctly

video surveillance - closed-circuit TV (CCTV)
also works as deterrent

motion detection in alarm systems

... detect malicious traffic

IDS to detect malicious traffic

Corrective and recovery controls

corrective and recovery try to reverse the impact of an incident

backups and system recovery

backups ensure data can be recovered

System recovery recovers the system itself

incident handling process

define steps to take response to security incidents

Start with incident response policy and plan

Physical controls

any controls you can physically touch

- Hard/ barricades

- bollard/ barricades
- access control vestibules
- lighting
- signs
- fences

lots of overlap with other control type/

Deterrent controls

attempt to discourage a threat

discourage potential attackers

or

discourage employees from breaking policy

very similar to preventative

ex: security guard

discourages people from entering

& the deterrence prevents people from entering

Cable locks - secure laptops to furniture

physical locks

Compensating controls

alternative controls used when primary control is unavailable

ex: org might require smart cards but might take time to setup for new employees

to allow new employees access, use Time-based one-time password TOTP

Response controls

incident response controls prepare for security incident and respond when they occur

security policies

- Create security policies
  incident response policies
- train personnel on how to respond to incidents

Combining control categories and types

controls can be both a cat and type, and can be multiple of each

ex: encryption is a preventative technical control

or fire suppression system is physical technical control

Using command line tools

will need to know best tool out of answers

Network reconnaissance and discovery

traps devices

Network reconnaissance

network discovery - allows devices on network discover other devices on same network

network reconnaissance - learn additional details about network and devices

Ping

ping tests connectivity for remote systems

can also use to verify system can resolve hostnames to IP, test NIC, and assess org security

works by sending Internet control message protocol ICMP echo request packets

respond with ICMP echo

respond with [illegible]
reply packets

Windows sends out 4 requests
but linux sends until you
stop it

-t in windows mimics linux

-c in linux mimics windows
need to specify #

-c 4

Using Ping to check Name Resolution

name resolution resolves hostname
google.com to IP address

several elements to name resolution
typically pc queries DNS
with hostname and gets IP

some malware tries to disrupt
name resolution for hosts
[illegible] pcs get updates
[illegible]

name resolution

ex: windows pcs get updates from windows update server malware changes process so it won't be able to

can ping a hostname to verify resolution

Beware of firewalls

if you receive replies from system, it verifies other system is operational and reachable

if ping fails, doesn't always mean its not operational might show "reply timed out" even if operational

Many DoS attacks use ICMP flood or Ping

firewalls block ICMP

flood

many firewalls block ICMP or ICMP echo requests

Using ping to assess organizational security

ex: verify firewalls block traffic by pinging

Remember

admins use ping to check connectivity of remote systems and verify name resolution

also verify firewalls, IDS/IPS, and routers block ICMP traffic

hping

hping - similar to ping but sends pings using TCP,

hping - [illegible]

can send pings using TCP, UDP, and ICMP

useful when verifying if ICMP is blocked on linux-like systems

other capabilities like scan for open ports

Ipconfig and ifconfig

ipconfig - internet protocol config

shows transmission control protocol (TCP)/IP config info for a Windows system

- pc IP address
- subnet mask
- default gateway
- MAC address
- address of DNS

[illegible] all network

. addr...

shows config info for all network interface cards (NIC) on a system

wired and wireless

ipconfig typically first step in network issues troubleshooting

ifconfig - interface config

linux systems

more capabilities than ipconfig

allows to config NIC and list properties of NIC

common command usage

ipconfig - basic info about NIC

ipconfig /all or ifconfig -a

comprehensive list of TCP/IP configs for each NIC

configs for each

MAC Address

assigned DNS addresses

Dynamic host config protocol

DHCP server if system is a DHCP client

ipconfig /displaydns

each time system queries DNS to resolve IP address it stores result in DNS cache

this command displays DNS cache

also shows any hostname to IP mappings in hosts file

ipconfig /flushdns

erase contents of dns cache

use if cache has incorrect info or want to ensure latest is used

or ...
info is used

ifconfig eth0 - shows configuration of first ethernet NIC
if there are multiple you can do eth1, eth2, ...
wlan0 for wireless NIC

ifconfig eth0 promisc enables promiscuous mode to listen for all network traffic the NIC processes, instead of only traffic addressed to it
can disable with ifconfig eth0 -promisc

ifconfig eth0 allmulti - enables multicast mode on NIC
process all multicast received by NIC instead of only ... for groups it is in

by [illegible]
traffic for groups it [illegible]

can disable with ifconfig eth0
-allmulti

Remember
ipconfig for windows
ifconfig for linux

if allows change NIC settings
like promisc mode

ip better for viewing NIC
configs and changing

many linux distros deprecated
ifconfig ; typically recommend

ip

but ip doesnt have commands
like change promisc

ip commands

- show - shows interfaces

ip commands

ip link show - shows info about them and some details about them

ip link set eth0 up - enables a network interface

ip -s link - shows stats on Network interfaces

Netstat

netstat - network statistics

View stats for TCP/IP protocols on a system

Many attacks establish connections from infected pc to remote pc

Common commands

netstat - displays list of all open TCP connections

netstat -a - displays all TCP and User datagram protocol UDP ports that system is listening in on and all connections

listening in on
open connections

displays sockets (IP:port#)
can use port # to tell type
of traffic
ex: :80 = HTTP

netstat -r - routing table

netstat -e - details on network
stats like how many bytes
system sent and received

netstat -s - statistics of packets
sent or received for specific
protocols such as IP, ICMP, TCP
and UDP

netstat -n - addresses and port
numbers in numerical order

netstat -p protocol - stats on
specific protocol
netstat -p tcp

can combine many options
ex: show all ports (-a) in
numerical order (-n) for
only tcp (-p tcp)

State of connection

ESTABLISHED - normal state
of data transfer phase
active open connection

LISTEN - waiting for a connection
request

CLOSE_WAIT - waiting for
connection termination

TIME_WAIT - system waiting
for enough time to pass
to be sure remote system
received TCP ack of connection

SYN_SENT - system sent SYN
packet and is waiting for

packet

SYN-ACK

SYN_RECEIVED - system sent a syn-ack packet after receiving SYN packet waiting for ack packet

Excessive SYN_RECEIVED means syn flood

Tracert and traceroute

tracert - lists all routers between two systems

each router referred to as "hop"

identifies IP and sometimes hostname of each hop with round trip time RTT for each hop

traceroute

for linux

for linux

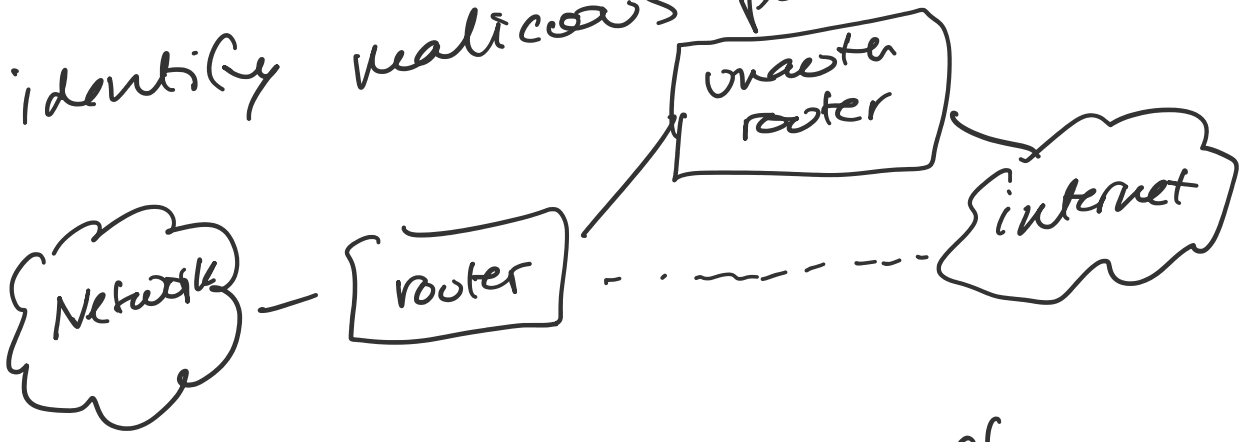
network admins use to find faulty routers

can use ping to verify connection to remote

but if ping fails you can use tracert to identify where the connection breaker

can see where packets are lost or where RTTs increase

identify malicious path:



what if normally connect from NY to NY and random hops to foreign

from ... see random hops to ... country

tracert -d google.com doesn't resolve IPs to hostnames

traceroute -n same as -d

Pathping

pathping - combines ping and tracert commands

tracert finds all hops
ping sends pings to each hop

shows stats of how many pings and responses

-n to not resolve hostnames

if you see 100% packet loss on a hop but still continue to get hops, means that ... kind ICMP

to vet loops, me...
router is blocking ICMP traffic

mtr for linux but not on security+

ARP

arp -cli tool related to address resolution protocol ARP

ARP resolves IP addresses to MAC addresses

arp command to view and manipulate ARP cache

arp - shows help on windows, ARP cache on linux

arp -a - shows ARP cache on windows

arp -a 142.168.1.1 - shows ARP cache ... specified IP

arp -a 192.168.[illegible]
entry for specified IP

can use to identify MAC addresses on local network

ex: Want to know MAC address of server1

. ping server1
. ARP identifies IP
. view arp -a —

Linux and LAMP

many orgs host web servers using LAMP stack

Linux - OS
Apache - web server app
MySQL - db management
PHP/Perl/Python - web pages

cat command

cat - concatenate show contents of files

vs of files

of files

make copies of files

merge multiple files

sudo cat /var/log/auth.log

view all authentication events on linux system

sudo cat /var/log/auth.log | more

more displays one page at a time

grep command

grep = globally search a regular expression and print

search for string or pattern in a file

sudo grep "authentication failure" /var/log/auth.log

can combine cat and grep

sudo cat /var/log/auth.log | [illegible] failure"

sudo cat /var/log/auth.log | grep "authentication failure"

head Command

head - show beginning of file 10 lines

logrotate.service copies syslog file to syslog.7 file then erases syslog and new events are written one of first events shows logrotate.service executed

sudo head /var/log/syslog

tail Command

tail - last 10 lines of file

sudo tail -n 15 /var/log/messages

logger Command

logger - adds to the /var/log/syslog

logger - adds to file

can use before an operation

logger Backup started

journalctl Command

journalctl - queries linux system logging utility (journald) and displays log entries from different sources

journald is in binary so journalctl lets you view it

by itself shows all logs which can be a lot

journalctl --since "1 hour ago"

limits logs to last hour

can use to show errors from previous boots

journalctl --list-boots

last logs

journalctl --list-boots
show boot logs

journalctl -1
show boot log with number
-1

can write to file
journalctl --since "1 hour ago" > journal.txt

Chmod command
chmod - change mode, change permissions of file or folder
read, write, execute permissions

3 groups
. owner of file
. owner group
. other

Read = 4
Write = 2
Execute = 1

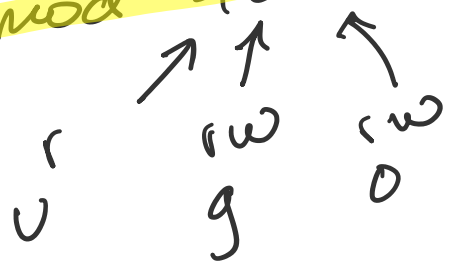
Write

Execute = 1

all permissions = 7

none = 0

`chmod 466 test.txt`



can use text as well

`chmod g=r filename`

set perms as is

`chmod g+r filename`

adds read to group

`chmod u-w`

removes write from user

Understanding Logs

expected to look at logs and interpret

what event happened

intell

what, when, where event happened
who/what did it

Windows logs

View logs with Windows event viewer

Security log - security log, audit log, and access log
auditable events like successes and failures

success
- login
- delete file

fail
- login fail
- permission error on file delete

System - record events related to OS
- when it starts
- shut down

- when it starts
- when shut down
- services start/stop
- drivers loading or fail

Application log - events sent to it by apps or programs

any app can write warnings, errors, and routine messages

Network logs

record traffic on network

on lots of devices

- routers
- firewalls
- web servers
- network IDS/IPS

info on where packets come from, where its going, IP, MAC, ports

web servers log requests for pages

common log format from W3C

common log

- host - IP
- user-identifier - name of user requesting
- authuser - logon name of user requested in the page if logged in
- date - date and time
- request - actual request line sent by client
- statur - HTTP status code
- bytes - byte length of reply

Centralized logging methods

two common ways to centralize all logs are SIEM and syslog protocol

SIEM systems

Security info and event management

SIEM centralizes solution for collecting, analyzing, and managing data from different sources

Security event management SEM

real time monitoring of security

real time monitoring
events

+

security information management SIEM
long time storage of data
with analysis methods

Common SIEM capabilities

log collectors - collects logs from devices in org and aggregates them

data inputs - come from any sources in org firewalls, IPS, routers, web servers, proxies

log aggregation - combines dissimilar items and puts up in similar format

correlation engine - software component used to collect and analyze event log data

aggregates based on common attributes

uses analytic tools to detect and raise alerts

uses analytic tools
patterns and raise alerts

reports - multiple built-in reports
categories like network traffic,
device events, threat events,
login ...

packet capture - many include
packet sniffers

user behavior analysis UBA - what
users are doing
what apps they use and network
activity
watch critical files for activity
some data loss prevention DLP
devices have this

sentiment analysis - analyze text
to detect opinion or emotion
using UBA to observe user behavior
for unwanted behavior

for unwanted

security monitoring - predefined alerts which can provide monitoring

custom alerts too

automated triggers - cause an action in response to predefined # of events

ex: failed logins

time synchronization - all servers sending data will have timestamps

different timezones

might convert to local or GMT time

event deduplication - removing duplicate entries

keep single copy of duplicates but associates will all sources

from

sources

logs / WORM - prevent anyone from modifying logs

write once read many WORM

common to put SIEM on private network even if it reads data from screened subnet

aggregation and correlation engine are intense processes that get offloaded to separate servers

primary SIEM focus on alerts and triggers

Dashboards provide admins view of meaningful activity

network operations center NOC might have huge dashboard

elements

might

Common dashboard elements

Sensors - use agents to collect logs from devices and send to SIEMs

dashboards display info

alerts - after events

sensitivity - sensitivity levels to detect triggers and alerts between 1-100

correlation - correlate and analyze data

trends - display trends in graphs

Syslog

syslog protocol - specifies general log entry format and details how to transport log entries

log server to

how to ...

centralized syslog server to collect entries similar to SIEM

Originators - systems sending logs

collectors - collects logs (syslog server)

does not define how syslog server handles syslog messages

collects entries and processes them according to /etc/syslog.conf file

syslog messages sent to /var/syslog

used to use UDP on port 514

now use TCP on port 6514 with transport layer security TLS and ensure packets arrive and have encryption

and
have encryption

Syslog-ng and Rsyslog

two open source alts to syslog
for linux
based on syslogd

Syslog-ng - extends syslogd allowing
log collection from any source
correlation and routing to route
logs to any log analysis
tool
rich filtering, content based
filter, and can be
extended w/ other langs
TCP and TLS

Rsyslog - improvement to syslog-ng
, logs to dbs

rsyslog

can send logs to dbs

NXlog

another log management tool
similar to syslog-ng and
rsyslog
supports log formats for windows
can work on linux and windows
integrate with SIEM

- NXlog community edition
- NXlog enterprise - adds event correlation and remote admin

Linux logs

located in /var/log directory
view logs with System Log Viewer
or with cat
ex: cat /var/log/auth.log

/var/log/syslog - all system activity including startup activity not syslog protocol

/var/log/messages - general system messages
startup, mail, kernel, auth

/var/log/boot.log - entries created when system boots

/var/log/auth.log - info about success and fail logins

/var/log/faillog - failed login attempts
faillog command

/var/log/kern.log - info logged by kernel

/var/log/httpd - if system setup as ... you can

/var/log/httpd - it sys...
apache web server, you can
view access and error logs

Assessment notes

1. Confidentiality = encryption

2. Integrity = hashing

3. which of the following is a cryptographic algorithm that creates fixed-length output from file that can be used to reproduce input?

   (A.) MD5
   B. AES
   C. IDS
   D. SIEM

Message digest 5 MD5 - hashing algorithm that creates irreversible

algorithm
fixed length, irreversible
output

4. Org hosts ecommerce site. Server randomly experiences high volume and spikes of resource usage. Which will prevent?

(A.) Elasticity
B. Scalability
C. Normalization
D. Stored procedures

elasticity = dynamically scale up/out depending on usage

normalization - organizing db columns to reduce redundant data

stored procedures - group of

Stored procedures - group of SQL statements that execute as a whole to prevent SQL injection

5. IDS = defective control

6. Monitor security logs, analyze SIEM trends, validate alerts = Defective

7. Server attacked by IP, want to know if connection still open.

netstat = view all open connections

8. tracert = verify that network isn't being rerouted to rouge router

Quanta Router

4. Using pathping to view connections and packet loss in hops

1 45ms 0/100 = 0% 0/100 = 0% IP1
14/100 = 14%

2 25ms 15/100 = 15% 0/100 = 0% IP2

Remember

the pipe between IPs is a segment packet loss here is usually the problem

packet loss on the following IP is the result of this too

10. Ping can be used in place

10. hping can be used instead of ping if ICMP requests are blocked because it can use TCP

11. grep = search through logfile

12. syslog file rotate will put message at top of file so use head

13. Want to ensure backup script records when it starts and ends

use logger

14. chmod to change perms

15. syslog = proper format of log entries for Linux

log entries