**1 )  
Unsecure protocol allows sniffing and discovery of data (credentials)**

http port 80 - for web sites  
ftp port 21 - file transfers  
telnet port 23 – admin of systems

1433 – MS sql - allows queries to be run remote

**Encryption protocols –**

https port 443 – for web sites  
SFTP/FTPS/SCP - for file transfer  
SSH - encrypted channel for admin or other features

**2)  
Windows VULN !! to the windows netbios servers and default shares**

SMB server message block  
Ports 445/139

3)

**In screen shots --  
PORT STATE**

**Open** means the port will connect  
**Closed** means the port has a hard reset RST flag in TCP  
**Filtered** means the port is probably filtered by ip range or address – **not accessible**

4)   
Linux Commands –

**chmod** allows to permission the file rwx – rwx – rwx  
 421 421 421  
Full control as example :: chmod 777 file.txt

**grep** allows to query strings  
**head** allows to query first 10 lines  
**tail** allows to query last 10 lines

**cat** – allows you to display the file on terminal  
**|** - pipe allows you to pass info to the next command

Example ::: cat FILE | grep “string”

**Hacks –**

**Pharm –** redirected to a fake web site (mostly with clicks ! )

**Waterhole** - infected web site code that attacks usually the browser  
**XSS** - the web site is infected through an attacker submitting code to be apart of website (FACEBOOK)  
 usually the code in in an <iframe> which you can not visually see but the browser reads the code   
 and executes the code   
**“CSRF” >= “XSRF”** - receive and email and CLICK !! code runs but you do not know results -  
usually seen in bank examples – in real world – used usually to steal cookies ( Simulation on test)

Frameworks :

**NIST** – federal government (6 step approach)  
**ISO 27701** – privacy   
**GDPR** – Euro standard for privacy   
  
data controller (owner)  
data processes on behalf of data controller   
data steward -- data quality,privacy - compliance

NIST  
Data Owner  
Data Custodian

**Diamond Model** – capabilities to track an APT group  
**MITRE** – Techniques/Tactics

Concept protecting data :  
**AT REST MOBILE** - Full Disk Encyrption (FDE) / Remote wipe [answering you will need one or both]  
**- scenario** : data is encrypted to a file server [ no sniffing ] – data protected  
data ON THE LOCAL DISK is ripped – protection is FDE

**Perfect Forward Secrecy (PFS), also called forward secrecy (FS)**, refers to an encryption system that changes the keys used to encrypt and decrypt information frequently and automatically. This ongoing process ensures that even if the most recent key is hacked, a minimal amount of sensitive data is exposed.  
**Use: PKI suite --**  
ECDHE or DHE to achieve perfect forward secrecy  
also note that it is a standard with TLS1.3

**HSM-as-a-service** (HSMaaS) is new approach that makes it easy to adopt an encryption strategy with VMs while mitigating the shortcomings found with traditional HSMs in virtual environments. While HSMaaS has long been a desirable goal, the fundamental building blocks were not easily available  
Virtual Env – AKA cloud

AV alerts indicating **Mimikatz** attempted to run  
mimkatz is used to collect passwords that are in clear text in memory on widows systems..

**Threat Feeds: IOCs**

TAXII client/server architecture  
STIX data format

Graphical user interface, application

Description automatically generated screened – subnet AKA DMZ

**Fog computing** is a decentralized computing infrastructure in which data, compute, storage and applications are located somewhere between the data source and the cloud. Like edge computing, fog computing brings the advantages and power of the cloud closer to where data is created and acted upon.

**Why ISO 27000 Certify ?? It** assures customers that the organization meets security standards

Supply Chain Attack –  
Public libraries – GIT downloads – updates like solarwinds hack

**TOR** network tool can access the Dark Web/net

A **secure web gateway** is a cyberbarrier or checkpoint that keeps unauthorized traffic from entering an organization's network. The traffic that a secure web gateway governs is all inline—the gateway stands between all incoming and outgoing data. Enforce AUP

**BCP – business continuity is** to continue and run when primary site fails / business processes fail  
**BIA business impact analysis** studies how the company functions and process function

**MTTR** **mean time to repair** is for recovery time on server and like devices

**RTO – recovery time objective** is when the business functions recover to functional

**Detective Controls** : cameras – SIEM

**Linux SUID**

ow to configure SUID in Linux?

Configuring SUID on your required files/script is a single CHMOD command away.

|  |  |
| --- | --- |
| 1 | [sarath@localhost ~]$ chmod u+s /path/to/file/or/executable |

**THE !! EVIL TWIN**

**DIGITAL SIGNATURE**

**DEFAULT Settings on devices –** default logins are documented on the web – some devices hardcoded with passwords

Routers **ACL ( access control list)** controls the flow of traffic from segments to segments

**Application whitelisting** : stops installs that are not authorized / stops execution of apps

**Credential stuffing** – hack reveals a username and password – it is used to launch an attack on another app or web site to login

**Email systems usually use TLS** to encrypt emails system to system and from client to system

**DR disaster recovery** restoration of data to systems

**BCP** business continuity program =survive the business FUNCTION ----------

When you go to a recovery site -- now in BCP

**BIA** business impact analysis =is where you document Business FUNCTIONS

SIMS: 4

**Legal Hold** – can not delete legal requested digital data - law enforcement requests why ? Legal Hold

Framework Regulation for Federal Systems with Controls **NIST -800-53**

You have to review code – NOT RUNNING – **Static Code Analysis**

Faster restore is a **FULL** backup – one restore

Send 2two factor auth (which is TIME Sensitive) **TOTP** (Timebased One Time Password) (ex RSA KEY)

Automation of playbook is **SOAR**

If you shared your Threat Intel with others you would send (format) **STIX**

**Geolocation** – authentication on where you are

Web servers respond to a request – 2 are present only one runs for requests – if one fails  
the 2nd server come live – model **ACTIVE-PASSIVE**

Attacked – systems communicate to remote C2 2am-4am - **RAT** remote access trojan

Need to remediate low level security incidents . SOAR spelled out:  
**Security Orchestration Automation Response**

Users need SEAMLESS access to Applications **SSO** (single sign on)

Containers are put into place and they have a root kit – best practice is to download and  
 **install from a trusted source**

**SNAPSHOT** – Vms : resiliency / backup / image – recovery

A detective control is an **ALARM**

Can gather credit cards numbers through **SKIMMING** – the device is attached to an ATM

Separation of duties also creates **LEAST PRIVILIG**E

I am listing 6 things that a frames work can do – **NIST RMF** (risk mgt framework)

Private key may have been compromised – You should **REVOKE** the certificate

Something – equipment or process – is scheduled by budgets and patchers , etc  
this is achieved by **MTBF** - mean time between failure

You are attacked by 100’s separate IPs from an internet address network – the defense would be to use a **FIREWALL** to block

Developer uploads a code-signing cert to the internet by accident – remediation – **revoke** the cs-certificate

Brute force of logins is successful – then you are experiencing logins from unusual locations  
you use **USER- BEHAVOIR ANALYTICS** to do research

Pick 3 for to produce data-center resiliency : that is hardware   
use the points to assign a solution   
ex. A percent of hard drive can fail **= RAID**   
system will shut down gracefully = **UPS**  //   
natural disaster – stay up and running = **GENERATOR**

Incident – SIEM detects malware on a host but the malware is not deleted – would is BEST solution  
**Quarantine the system from the network**

Access is needed to a database – it communicates with many applications – grant access with a  
**SERVICE** account ( service accounts login for the app to access database )

Notified of a wireless device signal – it is a Rasberry – PI (IoT device) – it is connected to a switch  
This device would be a **ROUGE ACCESS POINT** example

Several lines of code -- ??? they are scripts = **MALICIUOS SCRIPTS**

BYOD devices need access – they are not configured for the domain – To allow them access :  
**Use a new RADIUS server** - - **use the existing infrastructure to access the internal network**

An analyst needs to reduce the data center and create virtual networks , etc through automation:  
this is an example of **: IaC** ( infrastructure as code)

Companies check for credit card theft and monitor **DARK WEB** so they can alert you

Cloud is overwhelmed with service calls – in a DOS – solution is **ORCHESTRATION** (resiliency)

Hack on browser is PUP – browser at 99%

Backup question – down 72 hours – Differential (since last full) best restore