Acronyms

3DES	AAA	ABAC	ACL	AD	AES	AES256	AH
AI	AIS	ALE	AP	API	APT	ARO	ARP
ASLR	ASP	ATT&CK	AUP	AV	BASH	BCP	BGP
BIA	BIOS	BPA	BPDU	BSSID	BYOD	CA	CAPTCHA
CAR	CASB	CBC	CASB	CBT	CCMP	CCTV	CERT
CFB	CHAP	CIO	CIRT	CIS	CMS	CN	COOP
COPE	CP	CRC	CRL	CSA	CSIRT	CSO	CSP
CSR	CSRF	CSU	CTM	CTO	CVE	CVSS	CYOD
DAC	DBA	DDoS	DEP	DER	DES	DHCP	DHE
DKIM	DLL	DLP	DMARC	DNT	DNS	DNSSEC	DoS
DPO	DRP	DSA	DSL	EAP	ECB	ECC	ECDHE
ECDSA	EDR	EFS	EIP	EOL	EOS	ERP	ESN
ESP	ESSID	FACL	FDE	FIM	FPGA	FRR	FTP
FTPS	GCM	GDPR	GPG	GPO	GPS	GPU	GRE
HA	HDD	HIDS	HIPS	HMAC	HOTP	HSM	HSMaaS
HTML	HTTP	HTTPS	HVAC	IaaS	IAM	ICMP	ICS
IDEA	IDF	IdP	IDS	IPS	IEEE	IKE	IM
IMAP4	IoC	IoT	IP	IPS	IPSec	IR	IRC
IRP	ISA	ISFW	ISO	ISP	ISSO	ITCP	IV
KDC	KEK	L2TP	LAN	LDAP	LEAP	MaaS	MAC
MAM	MAN	MBR	MD5	MDF	MDM	MFA	MFD
MFP	ML	MMS	MOA	MOU	MPLS	MSA	MS-CHAP
MSP	MSSP	MTBF	MTTF	MTTR	MTU	NAC	NAT
NDA	NFC	NFV	NGFW	NG-SWG	NIC	NIDS	NIPS
NIST	NOC	NTFS	NTLM	NTP	OCSP	OID	OS
OAI	OSINT	OSPF	OT	OTA	OTG	OVAL	OWASP
P12	P2P	PaaS	PAC	PAM	PAP	PAT	PBKDF2
PBX	PCAP	PCI DSS	PDU	PE	PEAP	PED	PEM
PFS	PGP	PHI	PII	PIN	PIV	PKCS	PKI
PoC	POP	POTS	PPP	PPTP	PSK	PTZ	PUP

Acronyms (cont)

QA	QoS	RA	RAD	RADIUS	RAID	RAM	RAS
RAT	RC4	RCS	RFC	RFID	RIPEMD	ROI	RPO
RSA	RTBH	RTO	RTOS	RTP	S/MIME	SaaS	SAE
SAML	SCADA	SCAP	SCEP	SDK	SDLC	SDLM	SDN
SDP	SDV	SED	SEH	SFTP	SHA	SIEM	SIM
SIP	SLA	SLE	SMB	SMS	SMTP/S	SNMP	SOAP
SOAR	SoC	SOC	SPF	SPIM	SQL	SQLi	SRTP
SSD	SSH	SSID	SSL	SSO	STIX	STP	SWG
TACACS+	TGT	TKIP	TLS	TOTP	TPM	TSIG	TTP
UAT	UDP	UEBA	UEFI	UEM	UPS	URI	URL
USB	USB OTG	UTM	UTP	VBA	VDE	VDI	VLAN
VLSM	VM	VoIP	VPC	VPN	VTC	WAF	WAP
WEP	WIDS	WIPS	WORM	WPA	WPS	XaaS	XSRF

POST EXAM BRAIN DUMP

PBQs

Know how to configure a RADIUS server, WiFi server, and a client machine with PKI, WPA2 and current best security practices

Be familiar with the linux kernel and how to identify how attacks are taken out on there

what security measures can be taken ons pecific network devices to enhance security

What tech can be applied to different network devices (web server, database, domain controller))

Review attack types and their indicators

General

Port numbers and their protocols, only common ones are mentioned and just review them. It can make some of the other questions easier as well.

different methods of "preventative" and the like, what physical security measures are the most effective

differences between SOAR and SIEM, Other acronyms to review: CVSS,LDAP, SPI, SoC, API

CASB, other cloud computing concepts (what it takes to move an organization to the cloud, availibility, BCP, edge and fog computing))

review linux kernel for directory traversals, CSFR,

POST EXAM BRAIN DUMP (cont)

Tip: when taking the exam, flag questions that are worded weirdly and go back to them later and try to rewrite the question yourself. This is what I had to do for like 8 questions

Best cryptography practices and types to use based on specific scenarios, understand how PKI and PSK works, Tokenization vs hashes

Tip: most "scenarios" seemed to start with "_____ works at _____ organization and is updating/removing/hardening", so familiarize yourself with business related terms

Review GDPR, ISO, NIST, the diamond intrustion analysis method, and Diffe

Best practices for implementing secure work from home networks and remote desktop accessing

My final score was 759 the second time I took it, 723 the first

DISCLAIMER: This is not a word for word description of the exam and every exam is different

Braindumps.com This website has some "very very similar" questions as to what I had on this exam

Exam Objectives

Attacks, Threats, and Vulnerabilities (24%)	1.1-1.8
Architechture (21%)	2.1-2.8
Implementation (25%)	3.1-3.9
Operations and Incident Response (16%)	4.1-4.5
Governance, Risk, and Compliance (14%)	5.1-5.6

36 Objective Tasks, each with various subsections.

1.1 SE Attacks

Phishing	a way to trick people into giving up sensitive info, usually through fake links. prevent with email
filtering	
Smishing	
Vishing	
Spam/SPIM	
Spear phishing	
Whaling	
Prepending	
Reconnaissance	
Watering Hole Attack	
Influence Campaigns	
Reasons of Effectiveness	authority, intimidation, consensus, scarcity, familiarity, trust, urgency

Terms without Definitions

dumpster diving, shoulder surfing, pharming, tailgating, eliciting information, identity fraud, invoice scams, credential harvesting, impersonation, hoax, typo squatting, pretexting,

1.2 Analyze Attack Indicators

Malware	Ransomware
	Trojan
	Worm
	PUPs
	Logic Bomb
	RAT
	Rootkit
	cryptomalware
Pass Attacks	spraying

1.2 Analyze Attack Indicators (cont)

	dictionary	
	brute force	online v offline
	Rainbow Table	
Physical	skimming	
AI	Training Data	
Cryptographic	birthday	
	collision	
	downgrade	
Cloud-based v. on prem		

Terms w/o Definitions

Malware: fileless virus, command and control, bots, spyware, keyloggers, backdoor

Password Attacks: plain text, unencrypted

Physical Attacks: USB, malicious flash drive, card cloning

1.3 Indicators of App Attacks

Privilege Escalation
XSS
Injections
Pointer/object Dereference
Buffer Overflows
Error Handling
Race Conditions
Imprope Input Handling
Replay Attack
Integer Overflow
Request Forgeries
API Attacks
SSL Stripping
Driver Manipulation
Pass the Hash

Terms w/o Definitions

resource exhaustion, memory leak

1.4 Network Attacks

Wireless	Evil Twin
	Rougue Access Point
	Bluesnarfing
	Bluejacking
	Disassociation
	RFID
	NFC
	IV
On-path	
Layer 2	ARP poisoning
	MAC poisoning
DNS Poisoning	
DDoS	OT, Network, App
Malicious Code	VBA
	PS, Python, Bash
	Macros

Terms w/o Definition

MAC cloning, domain hijacking, URL redirection, domain reputation

1.5 Threat Vectors

Actors and Threats	APT
	Auth Hackers
	Unauth Hackers
	Semi-auth
	Shadow IT
Attributes of Actors	Internal or external threats, level of experience/capability, resources, funding, intent

1.5 Threat Vectors (cont)

Vectors	Direct access, wireless, email, supply chain, social media, cloud, removable media
Threat Intel Sources	OSINT
	Proprietary
	CVE Databases
	AIS
Research Sources	Conferences, academic journals, RFC, local industry, social media, threat feeds
	TTP

Terms w/o Definitions

insider threats, state actors, hacktivists, script kiddies, criminal syndicates

dark web, IoC, sharing centers, predictive analysis, threat maps, code repos

1.6 Security Concerns

There are security concerns with each of the sections below. The concerns depend on industry, implementation, and time, along with other factors. The objective is to explain the security concerns associated with everything below

Cloud based v on prem	**Cloud**- can be hacked, default must be changed, availability **On-prem**- physical, can be stolen, human errors
General Concerns	open permissions, unsecure root accounts, errors, weak encryption, unsecure protocols, default settings, open ports and services

1.6 Security Concerns (cont)

Thirs Party Risks	vendor management, supply chain, outsourced code, data storage
Impacts of Bad Security	data loss/breaches/exfiltration, identity theft, financial, reputation, availability loss

Terms w/o Definition

zero-day, patch management, legacy platforms

1.7 Techniques

Threat Hunting	Intel fusion
	threat feeds
	manuever
Vulnerability Scans	non/credentialed
	non/intrusive
	application
	CVE
	Config review
SIEM	Security info and event management
	Packet Capture, review reports, data inputs
	User behavior analysis
	sentiment analysis
	security monitoring
	log collectors
SOAR	Security, orchestration, automation, and response

Terms w/o Definition

false positives/negatives, log reviews, web application, network

1.8 Pen Test Techniques

Passive/Active Recon	drones, war flying/driving, footprinting, OSINT
Exercise Types	red, blue, white, or purple team
Pen Testing	un/known environment, partially known environment, lateral movement, privilege escalation, cleanup, bug bounty, pivoting

2.1 Sec Conference

EXplain the importance of security concepts in an enterprise environment	
Config Management	diagrams, baseline
Data soverignty	
Data Protection	DLP, masking, encryption, at rest, in motion, in processing
	tokenization
Geography	
SSL transport	
API	
Site resiliency (hot, warm, cold))	
Honeypots/flies/nets	
DNS Sinkhole	
Fake telemetry	

2.2 Cloud Concepts

Acronyms to review: IaaS, PaaS, SaaS, XaaS, CSP, MSP/MSSP, API, SDN, SDV, VM, SIAM	
Fog computing	cloud that is close to IoT data, midpoint, distributed cloud architecture, extends the cloud, distribute data and processing
	no latency, no bandwidth reqs, miminzes security concerns
Edge computing	IoT systems, edge server, close to the use, process the data on the device, increased internet speed

2.2 Cloud Concepts (cont)

Thin client	basic app usage, runs on remote server, VDI, local device, minimal operating system on the client, big network requirement
Containers	Standardized, physical infrastructure with one OS with container software, isolated process, image, standardized and lightweight, secure
Monolithic	client database code, one big application, codebase is so large it is hard to do maintinence, not as fast
	Microservices and APIs are the more effecient version of monolithic
Microservices/APIs	API gateway manages communication through gateway to different microservices that leads to a data base, the API is the "glue", scalable, resilient, security and compliance
Serverless architechture	FaaS, applications are remote and autonomous, removes the OS, it is a stateless compute container, event triggered (available as needed), third party

2.2 Cloud Concepts (cont)

Transit Gateway	VPC, public cloud that has resources, VPC is controlled by the transit gateway aka "cloud router," connects through VPN to VPCs
Virtualization	one physical piece of hardware, runs different OSs on one deviceVm sprwal avoidance
	vm escape protection
Virtualization Security	avoid VM sprawl because noo one knows where VMs live, detail provisioning so everyone knows where it is (track), VM is self-contained
	VM escape attack type can control host
HaaS/IaaS	outsourcing equipment, must manage internally
SaaS	easier and on-demand
PaaS	middle ground, no HVAC, no maintenance team, no direct control, building blocks
Cloud Design	elasticity, on-demand, global access,
Data Protection	resource policies,
SIAM	most providers are different, SIAM integrates diverse providers for a unified view
IaaC	can be deployed at will, describes app instances in code,

2.2 Cloud Concepts (cont)

SDN	central mngmt, vendor neutral, no human intervention, Agile, directly programmable
	to secure, use Internal firewall to connect all servers, use an IPS between internet and internal net, devices are software based
SDV	must see traffic to secure data, monitoring, SIEM, firewalls are able to be implemented
	data is encapsulated and encrypted

Terms w/o Definitions:
public, community, hybrid, infrastructure as code, on prem v off prem, service integration, multisourcing, control pane (config), data plane (performing)

2.3 App Dev/Deploy

Must be able to summarize these concepts	
De/Provisioning	
QA	
Integrity Measurement	
Secure Coding	normalization, stored procedures
	obfuscation/camoflauge
Server v Client Side	
OWASP	
Compiler v Binary	
Elasticity	
Scalability	

Terms w/o Definitions:
memory management, version control,

2.4 Authen. and Author.

Authentication methods	directory services
	federation
	attestation
	TOTP, HOTP, SMS, token key, static codes, push notifications/phone calls
	smart cards
Biometrics	fingerprint, retina, iris, facial, voice, gait analysis, efficacy rates, fase acceptance/rejection, CER
MFA	Factors: something you know, have, or are
	Attributes: somewhere you are, something you can do or exhibit, someone you know
AAA	

2.5 Cybersecurity

Redundancy	RAID
	Load Balancers on a network
	UPS
Backup types	Full
	Incremental
	Snapshot
	Differential
	Tape

2.5 Cybersecurity (cont)

Non-persistence	revert to nkown state, last known good config, high availibility, restoration order
Diversity	tech, vendors, crypto, controls

Terms w/o Definitions:
generator, dual supply, managed power, PDUs, multipath, NIC, replication (SAN), disk, copy, NAS, cloud, image, online v offline, offsite storage

2.6 Sec Implications

Acronyms to Remember	***REVIEW THEIR IMPLICATIONS AND SCENARIOS*** SCADA, IoT, VoIP, HVAC, MFP, RTOS, SoC, SIM cards
Embedded systems	arduino, raspberry pi, FPGA
SCADA/ICS	facilities, industrial, manufacturing, energy, logistics
IoT	sensors, smart devices, wearables, facility automation, weak defaults
specialized systems	medical
	vehicles, aircraft
	Smart Meters
Constraints for embedded and specialized systems	power, compute, network, crypto, inabilities to patch, authentication, range, cost, implied trust

Terms w/o Definitions:
drones, surveillance systems, 5G, narrow band

2.7 Physical Sec

Air Gap	
Screened subnet (DMZ)	
Secure Areas	
Secure Data destruction	burning, shredding, pulping, pulverizing, degaussing, third-party
Faraday cages	
Sensors	motion, noise, proximity, moisture, cards, temp

Terms w/o Definitions:
bollards, AC vestibules, badges, alarms, signage, cameras, motion detection, CCTV, industrial camo, Personnel, Locks (biometric/physical), USB data blocker, fencing, lighting, fire suppression, drones, visitor logs

2.8 Cryptographic Concepts

Common Use Cases	Low Power devices
	low latency
	high resiliency
	supporting confidentiality
	supporting integrity
	obfusacation support
	non-repudation support
Blockchain	public ledgers
Limitations	speed, size, weak keys, time, longevity, predicability, reuse, resource and security constraints
	entropy
Modes of Operation	Unauthenticated
	Authenticated
	Counter

2.8 Cryptographic Concepts (cont)

Steganography	Audio
	Video
	Image
Quantum	communications
	computing
	Post-Quantum
Other Concepts	digital signatures
	key length
	salting
	hashing
	key exchange
	elliptic-curve
	perfect forward secrecy

3.1 Implement Secure Protocols

Imlement secure protocols based on a scenario

Protocol	Definition	Use Cases
DNSSEC	Secure DNS, validates info and integrity through public key cryptography	sign DNS certificate
SSH	Secure shell provides encypted client-server terminal, replaced telnet/FTP	secure terminal communication
S/MIME	Used with email, Secure/Multi-purpose Internet Mail Extensions, public/private key pair is required	PKI manages these keys
SRTP	Secure Real Time Protocol, keeps convos private, adds encryption, uses AES, uses Hash based message	ex: HMAC SHA1
LDAP	Lightweight Directory Access Protocol (X.500 written by International Telecommunications Union) protocol for read/writing dir over an IP network, uses TCP/IP	ex: LDAP can access active directory
LDAPS	uses SSL, secure LDAP	
SASL	provides authentication using client certifications	
FTPS	uses SSL for encryption over FTP client	NOT THE SAME AS SFTP
SFTP	SSH FTP, SSH used for encryption, can ls dir, manipulate files	
POP/IMAP	Used with email,	Use a STARTTLS exntension to encrypt POP3 with SSL or use IMAP w/SSL
NTP	no security, classic	used in DDoS as amplifiers
NTPSec	secure version of NTP	
SSL/TLS	Used with email,	always encypted with browser emails

3.1 Implement Secure Protocols (cont)

	SSL (Secure Sockets Layer), TLS (Transport layer security) is the newer version of SSL)	
HTTPS	private key used on server, symmetric session key transferred using asymmetric encryption	most common form uses public key encryption
		symmetric key gets used during communication
IPsec	OSI Layer 3, public internet, data IS encrypted, anti-replay with encryption	both tunnel ends are secure, very standardized
	AH provides integrity, ESP provides encryption	
Tunneling		
ESP		
SNMPv3	SSH encrypts tunnel communication, follows CIA	is asking routers/switches for info from web browser with HTTPS
DHCP	servers must be authorized in AD, no secure version of DHCP	routing/switching

3.1 Implement Secure Protocols (cont)

	DHCP snooping, MAC spoofing,no built in security, rogue DHCP servers are a security issue but can be minimized through trusted interfaces on switches and only allowing distribution from trusted interfaces
	prevent DHCP client DoS starvation attacks with a limited number of MAC addys per interface
Antivirus, Firewalls, animalware	auto updates, constant, always check for encryption/integrity checks to inform firewall configurations

Use cases can include, voice and video, time sync, email, file transfer, directory services, routing and switching, DNR(Domain Name Resolution), Net address allocation, and subscriptions

3.2 Host/App Sec

Implement these based on a scenario

Secure coding practices:

Type	Scenario	Solution
Endpoint Protection	trojans worms and viruses are stopped	Antivirus
	stops spyware/ransomware/fileless	Antimalware
	allows to detect a threat without or with signatures and can use behavioral analysis, can investigate and respond	EDR
	OSI app layer, can block/allow, examine encrypted data	NGFW
	HIDS uses log files to detect, HIPS can block known attacks and uses signatures, hashes, and behavioral analysis	HIPs/HIDS
	allow/block incoming or outgoing app traffic	Host-based firewall

3.2 Host/App Sec (cont)

Boot Integrity with Bootloader	BIOS, will use secure boot, protects the BIOS and public key to protect BIOS update with digital signature check, verifies boot laoder	UEFI
	device provides central management server with all bootloader info from chain of trust. The report will compare with trusted v not trusted	Attestation
Various Boot Levels (Chain of Trust)	not wanting to lose contact with a system, perfect to get in, rootkits work, UEFI	Secure Boot
	bootloader verifies signature of OS kernel	Trusted Boot
	allows us to measure if any changes occured, measurements stored in TPM as a hash from previous two processes	Measured Boot
Database	breaches can be expensive, compliance issues, continuity of business is important	

3.2 Host/App Sec (cont)

	replacing sensitive data like a SSN with a different, totally random number. ex: tap to pay, NOT HASHING OR ENCRYPTING	Tokenization
	adding random data to a hash to secure it further	Salting
	one way, ex: passwords, fixed length	Hashing
Application Security	occurs when info is going in, normalization	input validations
	info stored on computer from browsers, tracks temp info, personalization, session mangmt, sensitive info is NOT supposed to store info	cookies
	secure headers are added to web server configuration, restricts browsers, helps prevent XSS attacks	Headers

3.2 Host/App Sec (cont)

	app code is signed by developer, assymetric encryption, trusted CA signs developers public key	code signing
	SAST for static code analysis, can easily find vulnerabilities(can have false positives).	Static v Dynamic Code Analysis
	dynamic analysis, random data put into an app, time and CPU resource heavy, try CERTBFF, negative testing, attack type,	Fuzzing
Hardening	minimizing attack survace, removing all possible entry points, can be based on compliance, CIS, SANS, NIST	
	possible entry points, close all except required ports, used with NGFW, use nmap	Open Ports
	FDE, ex: Bitlocker,	Disk encryption

3.2 Host/App Sec (cont)

	system stability, security fixes, emergency used for zero day attacks	Patch management
TPM	trusted platform modules, used in junction with HSM	Secure Boot

Terms w/o Definitions:
allow/block list, sandboxing, FDE, SED, Hardware root of trust, registry, auto update, third party services

3.3 Secure Net Design

Implement secure network designs based on scenarios

Design Type	Terms	Definition	Scenarios
Load Balancing	active/active		
	passive/active		
	Virtual IP		
Segmentation	VLAN		
	DMZ		
	Extra or Intranet		
VPN	split tunnel v full tunnel		
	SSL/TLS		
	HTML5		
	L2TP		
DNS			
Port Security	snooping		
Network Appliances	jump servers		
	forward proxy		
	reverse proxy		
	NIDS/NIPS		
	HSM		
	Aggregators		
	Firewalls		
	ACL		
	App v host v virtual		
Port Scanning			

3.4 Wireless Security

Remember to review how to install and configure wireless security settings

Cryptographic Protocols	WPA2
	WPA3
	CCMP
	SAE
Authentication Tools	EAP
	PEAP
	EAP-FAST
	EAP-TLS
	EAP-TTLS
	IEEE 802.1x
	RADIUS
Methods	PSK, open, WPS, captive portals
Installations	site surveys, heat maps, WiFi analyzers, channel overlaps, WAP, ap security

3.5 Mobile Solutions

Connection Methods	cellular, wifi, bluetooth, infared, USB, PTP, GPS, RFID
	NFC
MDM	remote wipes, geofencing, geolocation, screen locks, push notifications, passowrds and pins
	application management
	content management
	Biometrics
	full device encryption
	containerization
	storage segmentation
Enforcement and monitoring...	monitor third parties
	rooting
	sideloading
	custom firmware
	OTA
	geotagging
	Hotspot
Deployment Models	BYOD, CYOD, COPE, VDI

Terms w/o Definitions:
context-aware authentication, carrier unlocking, UEM, MAM, Android, Camera use, SMS, external media, USB OTG, microphone, GPS

3.6 Cloud Cybersecurity

Controls	High availibility, resource policies, secrets management, auditing
Storage Controls	permissions, encryption, replication, high availibility
Network Controls	Virtual Networks
	Public/private subnets
	Segmentation
	API Inspection
Compute Controls	Sec groups, dynamic resource allocation, instance awareness, VPC endpoint, container security
Solutions	CASB, app security, SWG, Firewalls *consider for firewalls cost, segmentation*
	Third party

3.7 Account Management

Identity Tools	IdP, Attributes, Certificates, Tokens, SSH Keys, Smart Cards
Account Types	user, shared, generic, guest, service
Account Policies	Password complexity, history, and reuse prohibiting
	Network location, geofencing, geotagging
	access policies, time based logins, account audits, permissions, lockout, disablement

3.8 Authen/Author Solutions

Authentication management	keys, vaults
	TPM, HSM, knowledge-based
Authentication/-Authorization	EAP, SHAP, PAP, RADIUS, 802.1x, SSO, SAML, TACACS+
	Kerberos
Access Control Schemes	ABAC, MAC, DAC
	rule or role based, conditional, privilege access management

3.9 PKI

PKI Types	Definition	Certificate Types	Definition
Key Management		Wildcard	
CA, RA, CRL, OCSP, CSR, CN		Subject Alternative Names	
Expiration		Code Signing	
		Self Signed	
Concepts		Email, User, Root, Domain	
Online v Offline		DER Format	
Stapling		PEM Format	
Pinning		PFX Format	
Trust Model		P12	
Key Escrow		P7B	

Recommended Resources

Comptia Objectives List (Free)	Sec+ 691 Exam Cram (Book, $40)
Professor Messer(Free, Videos)	601 Get Certified Get Ahead (Book, $40)
LinkedIn Learning (1st Month Free)	Official Comptia Study Tools (Books, $50 USD)
Anki Learning Flashcards (Free)	Practice Tests!
see braindump	

4.1 ToolUse

Organizational Security

Commands	Function	Tools	Function
`tracert`		theHarvester	
`nslook up/dig`		sn1per	
`nmap`		Nessus	
`ipconfig/ ifconfig`		Cuckoo	
`hping`		FTK Imager	
`netstat`		Win Hex	
`netcat`		Autopsy	
`arp`		Wireshark	
`route`		Memdump	
`curl`		Powershell, Python, SSH	
`dnsenum`	last one used for recon	Tcpdump	
`head`	used for file manipulation (FM)	Tcpreplay	
`tail`	FM		
`cat`	FM		
`grep`	FM		
`chmod`	FM		
`logger`	FM		

Terms w/o Definitions:Data sanitization, dd, password crackers, indicent response, OpenSSL

4.2 PPP

Policies, Processes, and Procedures for IR

IR Process	Preperation
	Identification
	Containment
	Eradication
	Recovery
	Lessons Learned
Attack Frameworks	MITRE ATT&CK
	Cyber Kill Chain
Stakeholder Management	
Communication Plan	
DRP	
BCP	
COOP	
Retention	

Terms w/o Definitions:tabletop, walkthroughs, simulations, diamond model of intrusion analysis, irp

4.3 Data Support

Utilize appropriate data sources to support an investigation

SIEM Dashboards	sensors, sensitivity, trends, alerts, correlation
Log Files	Network, system, app, security, web, DNS, authentication, dump files, VoIP, SIP
`syslog`	
journalctl	
NXLog	
Bandwidth monitors	
Metadata	email, mobile, web, file
netflow	

4.3 Data Support (cont)

Protocol Analyzer	

4.4 Mitigation

Reconfiguring Endpoints	
Quarantine	
Configuration changes	alter firewall, MDM, DLP, content filter, cert updates
Isolation, Containment, Segmentation	
SOAR playbooks	

4.5 Digital Forensics

Documentation and Evidence	can include video, tags, reports, snapshots, time stamps, event logs, interviews, admissibility
	chain of custody
Acquisition	order of volatility
	use disks, RAM, OS, device type, firmware, snapshots, caches, networks, artifacts
Integrity	Hashing, checksums, and provenance
Preservation is crucial	
Non-repudiation	
Counterintelligence	

Terms w/o Definitions:
on prem v cloud, right to audi, data breaches

5.1 Types of Controls

Control Types	preventive, detective, corrective, deterrent, compensating, physical
Categories	manegerial, operational, technical

5.2 Regulations

Importance of applicaible regulations, standards, or frameworks that impact organizational security posture

Legislation	GDPR
	National/territory/state laws
	PCI DSS
	HIPAA
Frameworks	CIS
	NIST
	RMF/CSF
	ISO
	Cloud
	SSAE
Guides	OS
	Web server

5.3 Policies

Personnel	Abide by AUP, job rotations, mandatory vacations, sepereation of duties
	least privilege
	clean desk, background checks, NDAs, social media analysis, Onboarding, Offboarding, User Training/Role based training
Diverse Training	

5.3 Policies (cont)

Third Party Risk Management	vendors, supply chain, business partners, SLA, MOU, MSA, BPA, EOL, EOSL
Data	Classification
	Governance
	Retention
Credential Policies in reference to...	personnel, third party, devices, service accounts, admins
Organizational Policies	Change management and control
	Asset Management

5.4 Risk Management

Acronyms: RTO, RPO, MTTR, MTBF, DRP, SLE, ALE, IP, ARO

Risk types include...	external, internal, legacy systems, multiparty, IP theft, and software compliance
Risk Management Stategies	Acceptance, Avoidance, Transference, Mitigation
Risk Analysis	Control assessments
	inherent risk
	residual risk
	control risk
	Qualitative v Quantitative risk
	Likelihood of occurence
	Asset Values
	SLE, ALE, ARO
Business Impact Analysis	RTO, RPO, MTTR, MTBF, DRp
	site risk assessment

5.5 Data Security

Consequences to an org when data breaches occur	reputation is damaged, identity theft, fines, IP theft
Notifications	
Data Types	Public
	Private
	Sensitive
	Confidential
	Proprietary
	PII
	Health, Govt, Customer
	Financial
Privacy Enhancing Technologies	Data minimization
	Data masking
	tokenization
	anonyminity
Roles and their Responsibilities	Data owners
	Data controller
	DPO
Info Life Cycle	
Terms of Agreement	Privacy Notices

Network Design

Conduct a risk assessment: The first step in designing a secure network is to assess the risks to the network and the assets it protects. This includes identifying potential threats, vulnerabilities, and the impact of a security breach. Based on the risk assessment, the security requirements can be identified, and the security design can be developed.

Network Design (cont)

Use layered security: A layered security approach involves implementing multiple layers of defense to protect the network from different types of threats. This includes using firewalls, intrusion detection and prevention systems, antivirus software, encryption, and access controls.

Secure network infrastructure: The network infrastructure should be secured by implementing strong passwords, disabling unnecessary services, updating firmware and software, and restricting access to critical network devices. Network devices should also be physically secured to prevent unauthorized access.

Implement access controls: Access controls should be implemented to restrict access to sensitive information and resources. This includes user authentication, authorization, and accounting (AAA), role-based access control, and network segmentation.

Encrypt sensitive data: Sensitive data should be encrypted both in transit and at rest. This includes using secure protocols such as HTTPS, SSH, and VPNs for data transmission and encryption tools such as BitLocker, VeraCrypt, or LUKS for data storage.

Train employees: Security awareness training should be provided to all employees to educate them on security best practices and to reduce the risk of human error.

Monitor and test the network: Regular monitoring and testing should be conducted to identify and remediate security vulnerabilities. This includes using network monitoring tools, conducting penetration testing, and reviewing audit logs.

Encryption and Keys

Public vs Private Key

Encryption and Keys (cont)

Public Key: A public key is a part of the asymmetric encryption algorithm and is made available to anyone who wants to communicate with the owner of the key. It is used to encrypt data, digital signature verification, and establish secure communication channels. The public key can be freely distributed as it does not contain sensitive information. **Private Key**: A private key, on the other hand, is the other half of the asymmetric encryption algorithm and is kept secret by the owner of the key. It is used to decrypt data, generate digital signatures, and establish secure communication channels. The private key must be kept secure as it contains sensitive information that must not be disclosed to anyone else.

Asymmetric Keys vs Symmetric Keys

Symmetric Key: A symmetric key encryption system uses the same secret key to both encrypt and decrypt the data. The sender and receiver must have the same secret key to communicate securely. The symmetric key encryption system is faster than the asymmetric key encryption system, and it is typically used for bulk data encryption. **Asymmetric Key**: An asymmetric key encryption system uses two keys, a public key, and a private key. The public key is used to encrypt the data, and the private key is used to decrypt it. Anyone can have access to the public key, but the private key is kept secret by the owner. Asymmetric key encryption is slower than symmetric key encryption but provides better security and is typically used for digital signatures, secure key exchange, and establishing secure communication channels. **The main difference between symmetric and asymmetric key encryption is that symmetric key encryption uses the same key to encrypt and decrypt data, while asymmetric key encryption uses two different keys for encryption and decryption. The symmetric key encryption system is faster, while the asymmetric key encryption system is more secure.**

PBQ Notes from Youtube

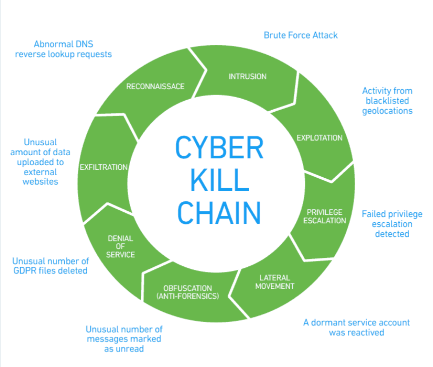
Firewalls and Proxy PBQ	allow web traffic, disallow all traffic from specific IP, ensure implicit deny, port 53 is DNS,
	IDS alert, supposed to be denied on ACL, given diagram. 443 default port for https, NAT, NAPT firewall in use
3.3 PBQ	tcp port 22, new inbound rule wizards, use custom, rule can be named SFTP, most groups use third party for FTP,
PBQ Vincent Humble	multifactor auth characteristis, payload, trojan with keylogger
	cryptographic scenario: RSA,
	hash → private key encryption → to create dig sig → alice then attatches DS to og message to deliver to bob (SHE FORGOT TO ENCRYPT THIS)→ bob then decrypts og message w/ DS using Alice's **public** key → resulting in the has of the og message → bob performs hash comparison → the hashes do not match → no trust
Other Vincent Humble Videos	601-P1: blowfish cipher, Bcrypt? can lengthen and strengthen keys, longer the key, the longer a file is confidential,

PBQ Notes from Youtube (cont)

601-P2: Sim cloning, elliptic curve cryptography, geo requirement for data centers 100 miles?, hybrid, DLP, GPS and WiFi, nonrep & accountibility,

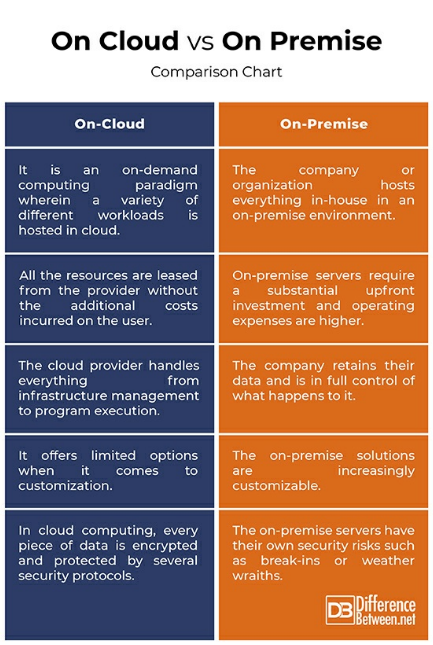
601-P3:

Cyber Kill Chain


CYBER KILL CHAIN
RECONNAISSACE
INTRUSION
EXPLOITATION
PRIVILEGE ESCALATION
LATERAL MOVEMENT
OBFUSCATION (ANTI-FORENSICS)
DENIAL OF SERVICE
EXFILTRATION
Brute Force Attack
Abnormal DNS reverse lookup requests
Activity from blacklisted geolocations
Unusual amount of data uploaded to external websites
Failed privilege escalation detected
Unusual number of GDPR files deleted
Unusual number of messages marked as unread
A dormant service account was reactived

Alt text: the cyber kil chain, 8 steps

Cloud vs On Premises



On Cloud vs **On Premise**

Comparison Chart

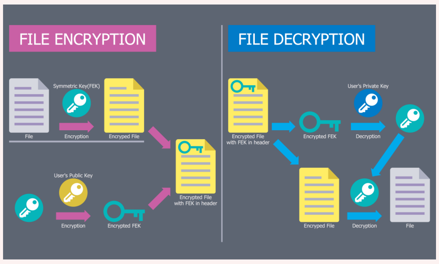
On-Cloud	On-Premise
It is an on-demand computing paradigm wherein a variety of different workloads is hosted in cloud.	The company or organization hosts everything in-house in an on-premise environment.
All the resources are leased from the provider without the additional costs incurred on the user.	On-premise servers require a substantial upfront investment and operating expenses are higher.
The cloud provider handles everything from infrastructure management to program execution.	The company retains their data and is in full control of what happens to it.
It offers limited options when it comes to customization.	The on-premise solutions are increasingly customizable.
In cloud computing, every piece of data is encrypted and protected by several security protocols.	The on-premise servers have their own security risks such as break-ins or weather wraiths.

DB Difference Between.net

Alt text: On cloud vs On premises

Note: This is a VERY strong theme throughout all of the objectives for this exam

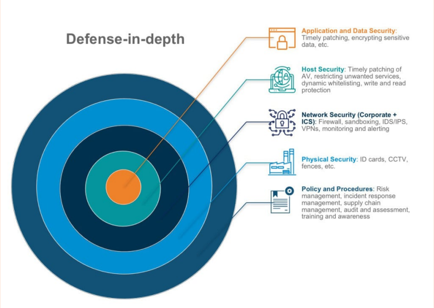
Encryption (Image)



Alt text: encryption process

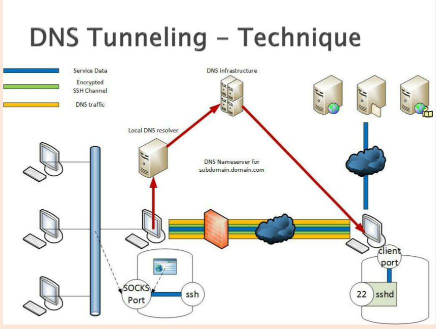
Data preparation, Key generation, Encryption algorithm, transmission of data, decryption

DiD


Defense-in-depth
Application and Data Security: Timely patching, encrypting sensitive data, etc.
Host Security: Timely patching of AV, restricting unwanted services, dynamic whitelisting, write and read protection
Network Security (Corporate + ICS): Firewall, sandboxing, IDS/IPS, VPNs, monitoring and alerting
Physical Security: ID cards, CCTV, fences, etc.
Policy and Procedures: Risk management, incident response management, supply chain management, audit and assessment, training and awareness

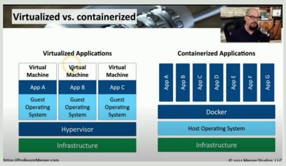
Alt Text: Defense in depth methods

DNS Tunneling



Alt Text: DNS tunneling techniques

Virtualization vs Containerization



Virtualized vs. containerized

Virtualized Applications

Virtual Machine	Virtual Machine	Virtual Machine
App A	App B	App C
Guest Operating System	Guest Operating System	Guest Operating System
Hypervisor		
Infrastructure		

Containerized Applications

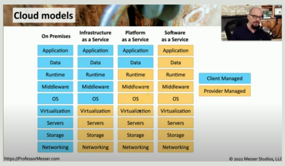
App A	App B	App C	App D	App E	App F	App G
Docker						
Host Operating System						
Infrastructure						

https://ProfessorMesser.com

© 2021 Messer Studios, LLC

Alt text: virtualization vs containerization screenshot from Professor Messer Video

"As a Service"



Cloud models

On Premises	Infrastructure as a Service	Platform as a Service	Software as a Service
🟦 Application	🟦 Application	🟦 Application	🟨 Application
🟦 Data	🟦 Data	🟦 Data	🟨 Data
🟦 Runtime	🟦 Runtime	🟨 Runtime	🟨 Runtime
🟦 Middleware	🟦 Middleware	🟨 Middleware	🟨 Middleware
🟦 OS	🟦 OS	🟨 OS	🟨 OS
🟦 Virtualization	🟨 Virtualization	🟨 Virtualization	🟨 Virtualization
🟦 Servers	🟨 Servers	🟨 Servers	🟨 Servers
🟦 Storage	🟨 Storage	🟨 Storage	🟨 Storage
🟦 Networking	🟨 Networking	🟨 Networking	🟨 Networking

🟦 Client Managed

🟨 Provider Managed

https://ProfessorMesser.com

© 2021 Messer Studios, LLC

Alt text: Cloud services and how they differ from one another