Domain 1

Social engineering – physical vs Virtual

Social Engineering – provide info or perform actions.

Phishing – give up personal information

Spear – specific group

Whaling – executives

Vishing – phone

Smishing – SMS

SPAM – email VS SPIM is SMS

Dumpster Diving – from trash

Tailgating – unauthorized following

Eliciting information – elicitation

Shoulder surfing – privacy filter

Pharming – drive traffic to another location

Identity theft

Prepending

Invoice Scams

Credential Harvest – get passwords

Reconnaissance – passive, semi-passive, and active

Hoaxes – falsehoods

Impersonation – fraud

Watering hole attack – malware on visit website

Typosquatting – URL hijacking

Drive-by-download

Pretext – story with character and plausible story

Hybrid warfare – unconventional such as social media

Principles of social engineering – authority, intimidation, consensus, scarcity, familiarity, trust, urgency

Rootkit – escalation of privilege for OS attack (EDR endpoint detection response\_

Backdoor – usually dev or debugging

Computer virus – malicious code designed to spread

Crypto-malware – extort money

Hoax – nuisance and wasted resource

Logic bomb – some trigger

Trojan Horse – hidden payload

Worm – copies itself without human

PUP – potentially unwanted program (spyware, adware, dialers)

Keylogger – log keystrokes

Spyware – obtain info

Fileless virus – executes in resident memory

C&C – controlled by attacker exfiltration

RAT – remote access

Ransomware – unable to access files

Counter with backups, cloud

Dictionary attacks – all words using standard word

Password spraying – many accounts to avoid lockouts, usually default passwords

Offline – discover DB or packet scan

Online – guess user like web and wi-fi

Plaintext is wireshark

Brute force – all possibilities

Rainbow tables – precomputed hashes

Salts – random data added when hashing which stops rainbow tables

MFA – know, have, are

Bots, bot herder, bot net. Usually DDoS

Malicious flash drive has trojan

Malicious USB cable (HID)

Card clone – using skimming like machines on gas pumps

Adversarial AI – poison data. Security of data sources.

AI – smart tasks

ML – improve automatically algorithms through data

Deep learning using neural networks

Supply Chain – upstream compromise vendors (island hopping)

Cloud vs On-Prem. Cloud more secure. No access to facility or audit access. Will list certification compliant. On-prem do not have shared responsibility, costs, full control.

Collision attack – two inputs have same hash (birthday attack is a collision attack)

Downgrade attack (ex with TLS)

Replay attack – reuse authentication like Kerberos

Privilege escalation

Malicious scripts – xss (stored vs reflected)

XSRF,CSRF – use authenticated session of user to then create requests to steal. Ensure request came from local site and use secure tokens

DLL – inject into memory

LDAP – active directory

XML (extensible markup language) – xpath similar to SQL

SQL injections – uses frontend to expose backend issue

Point dereference – denial of service by dereference null pointer

Directory traversal – command injection attack, access to root directory

Buffer overflow – too large input

Race condition – sequence or timing (time of check to time of use TICTOU)

Error handling

Session replay – steal valid session ID whereas replay is for authentication

Integer overflow – not enough allocated memory

API – gain resource or interrupt service

OAUTH – open authorization, usually with web apps, authorization request to user, user consent, access token, access resources. No sharing passwords

Resource exhaustion – hang/crash, memory leak

Memory leak – bad memory management in older languages

SSL Stripping – downgrade from HTTPS to HTTP, through on-path (MITM), also affects TLS

Driver manipulation – shim intercepts API calls, new library bypasses a driver. Refactoring evades detection.

Pass the hash – used with NTLM a legacy windows to grant authentication.

Pass the ticket – Kerberos with limited ticket expiration

Network attacks – on path MITM – sits between and captures traffic.

Mobile – bluejacking (unsolicited messages), bluesnarfing (theft), bluebugging (backdoor). Disable discovery mode.

Evil twin – copy access point like airport.

Disassociation – DoS breaking wireless connection to allow evil twin.

Jamming – prevents others from using channel

RFID – badges, NFC like credit cards

Initialization Vector – compute RC4 key for wireless (legacy)

DNS poison – alter domain to IP address. Redirect traffic.

DNS spoofing – attacker sends false replies beating the valid DNS server

Hyperlink spoofing

DoS – resource consumption

DDoS – multiple attacks from botnet. Disable echo replies

Network based DDos – UDP, ICMP, Syn flood)

Application – layer 7, open connections or transactions

OT (operation tech) – weakness in hardware and IoT

IDS/IPS/ rate limiting / firewall ingress/egress

Three way handshake – TCP/IP 1. Syn 2. Syn-ack 3. Ack

URL redirection – forces users to untrusted external site. Domain reputation suffers.

SPF – Secure policy framework – admin list DNS records for IP’s able to send email on behalf of domain

DMARC – domain based message authentication reporting and conformance – specify how receiving mail servers handle fail authentication checks along with reports.

DKIM – Domainkeys identified mail – digital signature using PKI. Public key is in domain’s DNS records.

Domain hijacking – changing domain registration info

MAC flooding – MAC table is flooded and works as unicast flooding

ARP poison – send ARP packet containing attacker’s MAC but target IP address (ARP spoofing)

MAC cloning – duplicate MAC address. Counter is Network access control (NAC)

Malicious code/Script – PS, python, bash, macros, VBA. Endpoint security reducing attack surface

APT – advanced persistent threat

Insider threats – colluding with outsiders

State actors – attack infrastructure

Hacktivists – some cause

Script kiddies

Criminal Syndicates – structured threats

Hackers – unauthorized, authorized, semi-authorized

Shadow IT – use tools without IT approval

Competitors

Collusion – agreement between multiple

Separation of duties – no one controls entire process

Job rotation – different tasks

Espionage – external

Sabotage – insider

Direct access – hardware, keylogger, flash drive

Wireless – rogue, evil

Email – spam, phishing, invoice

Supply chain – vendor screen

Social media – hybrid warfare – AUP

Cloud – unsecure apps, misconfigured, use CASB (cloud access security broker)

Open source intelligence OSINT

Closed/proprietary

Vulnerability DB – NIST CVE’s

Public/private sharing – CISA (cyber infra and Security agency)

Dark web – hacker groups

Indicators of compromise – log entries or malicious activity

AIS – automated indicator sharing – free from CISA

TAXII – trusted automated exchange intelligence information – the protocol from sharing messages of threats

Structured threat information expression – stix – defines language/API for describing threat information

STIX is the language while TAXII is the protocol. Both created by MITRE and maintained by OASIS

Predictive analysis – automation and human intelligence

Threat maps – real time map of security attacks

File/code repos – hackers use open source

Vendor websites – keep track of vulnerabilities

Vulnerability feeds into central management system

Conferences – network with experts and product teams

Academic journals are peer-reviewed

RFC – request for comments – internet engineering task force (IETF)

Local industry groups, social media, youtube

Threat feeds – automated delivers info to SIEM, firewall

TTP – threat actors use tactics, techniques, procedures

Untrained users are vulnerable everywhere. Misconfigurations but cloud has help with in-built tooling and alerts.

Disruptive attacks susceptible to disruptive attacks

Shared responsibility model – on-prem secure all. IaaS must secure OS, network, apps. PaaS takes care of OS. SaaS is always just the application.

Zero-day exploit – unknown vulnerability, user entity behavior analysis (UEBA!!!!!!!!!), zero trust security

Open permissions – fail to use least privilege. Use change and release management

Unsecure root account – use sudo

Errors – train employees

Open ports and service increase attack surface

Weak encryption – use stronger

Unsecure protocols – telnet, snmpv1 v2 FTP

Default settings – spray attacks

Lack of vendor support – security patches

Outsourced code development – secure code. Managed virtual desktop

Data storage – backup data

Supply chain – everyone including customers

Vendor management – reduce vendors – external audit because of island hopping

System integration – privileged remote or physical access, contractors

Firmware – embedded systems

Operation Systems – easy to patch

Legacy platforms – isolation, patching, sandboxing (isolate legacy!!!!!!!!!!!!!!) such as in VM

Impact – breach, loss, exfiltration, reputation damage

Availability loss – system is down

Identity theft – financial loss. IP theft.

Threat hunting – seek out threats in network.

Intelligence fusion – industry and government sharing threat information.

Threat feeds – indicators of compromise (IOC)

Advisories are government and bulletins are private companies

Maneuver – company to disguise system, harder to infiltrate!!!!!!!!!!!!!!

Vulnerability scans – credentialed (more powerful) vs non-credentialed (attacker)

False positive, false negative, true positive, log reviews

Non-intrusive scan will only report, intrusive scan will exploit (no prod)

Configuration review – no deviations in config

Network scans – on network, computers, devices

Application scans – regression testing

Web application scans – search engine, automated, XSS, SQL injection.

Static analysis secure testing – source code checked

Dynamic analysis security testing – running application tested

CVE – list of public vulnerabilities

CVSS – scoring system, overall score. Severity listed

NVD (national vulnerability database) – ties into the CVE with the CVSS

SIEM – security information event management – collects data, provides real time data, correlation, notification

SOAR – centralized alert and response automation with threat specific signature or indicators. Single click

Log collectors – built into SIEM can collect from syslog server and other servers. Agent used to collect logs, parse, and pass to SIEM

Log aggregation – correlate and aggregate events so that duplicates filtered and understand network events

Packet capture – real time capture and alert

Data inputs – IDM, MDM, CASB, XDR, IPS, IDS

**UEBA – user entity behavior analysis** – provides baseline of what is normal, tracks devices, and servers visited. 2-3 weeks.

Sentiment analysis – AI to identify attacks like on social media

Security monitor – real time and even monitor helps security team

Even reporting – dashboard, true positives vs false positives

SOAR – tooling define incident analysis and response. Log collection to SIEM to SOAR to SOC to log collection. Reduces (MTTD!!!!!!!!!!!) mean time to detection and accelerates response. Uses (Playbook!!!!!!!!!!!!) that define incident and action taken.

Known environment – full information, white box testing

Unknown environment – black box test, blind

Partial known – grey box test, limited info

Rules of engagement – define purpose and scope for those performing test, constraints

Lateral movement – movement to other devices

Privileged escalation – higher privilege, usually higher level but sometimes (horizontal privilege!!!!!!!!!!!!!!!! Like another user’s resources)

Persistence – achieve persistent presence in exploited system to gain access such as remote access

Cleanup – final stage all work is removed

Bug bounty – money reward for ethical hackers

Pivoting – island hopping – attack another system on same network

Reconnaissance – passive is war driving (wireless network), drones, war flying (SSID)

OSINT – data on open source

Active reconnaissance

Footprinting – ethical hacking to gather data about target. Ping sweep, tracert, nmap, DNS info. Passive is website, google, whois lookup

Red team – attackers, offense

Blue team – defenders

Purple – process improvement (both red and blue)

White team – oversees engagement

Domain 2