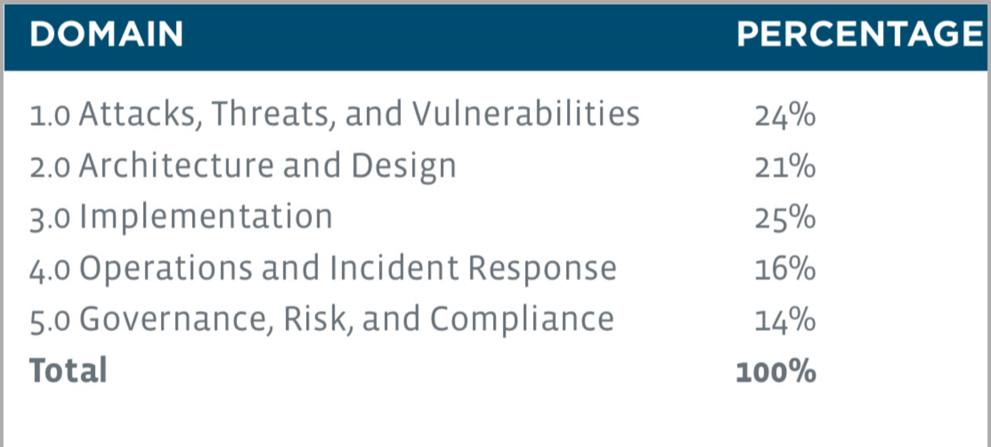
Security + 601 Notes



DOMAIN	PERCENTAGE
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%
Total	**100%**

1.0 Threats, Attacks, and Vulnerabilities

1.1 COMPARE AND CONTRAST DIFFERENT TYPES OF SOCIAL ENGINEERING TECHNIQUES.

Phishing is an example of social engineering techniques used to deceive users. Users are lured by communications purporting to be from trusted parties. Phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site

Smishing or SMS phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information. Smishing attacks typically invite the user to click a link, call a phone number, or contact an email address provided by the attacker via SMS message.

Vishing Voice phishing is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information for the purpose of financial reward. Vishing fraudsters often use modern Voice over IP (VoIP) features such as caller ID spoofing and automated systems (IVR) to make it difficult for legal authorities to monitor, trace or block.

Spam is the use of messaging systems to send an unsolicited message (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, or for any prohibited purpose (especially the fraudulent purpose of phishing). While the most widely recognized form of spam is email spam

Spam over Internet messaging (SPIM)

Messaging spam, sometimes called SPIM, is a type of spam targeting users of instant messaging (IM) services, SMS, or private messages within websites

Spear phishing attempts directed at specific individuals or companies is known as spear phishing. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success.

Dumpster diving The term "binner" is often used to describe individuals who collect recyclable materials for their deposit value.

Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder, either from keystrokes on a device or sensitive information being spoken and heard, also known as eavesdropping

Pharming is a cyberattack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned".

Tailgating guards, Network operations center (NOC) Services and technical team Anti-tailgating/Anti-pass-back turnstile gate. Only permits one person to pass through

Eliciting information present overtones of familiarity and trustworthiness to elicit confidential or personal information. Social hacking is most commonly associated as a component

Whaling The term whaling refers to spear phishing attacks directed specifically at senior executives

Prepending the internet is made up of distinct networks called autonomous systems (AS), which communicate with each other by utilizing the Border Gateway Protocol (BGP).

Identity fraud is the act of using a stolen identity to obtain goods or services by deception. This usually involves the use of stolen, forged or counterfeit documents such as a passport or driving licence.

Invoice scams Phishers believe that you would have a hard time spotting fake bills, which is why they’re increasingly using them as part of their mass mailings.

Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.

Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible

Hoax These can take the form of false virus alerts (such as the "Good Times" hoax), chain letters, or attempts to spread false information about some issue

Impersonation is one of several social engineering tools used to gain access to a system or network in order to commit fraud, industrial espionage or identity theft.

Watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

Typosquatting attempts to take advantage of typographical errors introduced by users when URLs are typed directly into the address bar. Similarly, malicious actors may seek to trick users taking a quick glance at a URL into opening a visually similar, yet malicious link.

Pretexting is form of social engineering in which an attacker tries to convince a victim to give up valuable information or access to a service or system. The distinguishing feature of this kind of attack is that the scam artists comes up with a story â€” or pretext â€” in order to fool the victim.

- Influence campaigns

- Hybrid warfare
- Social media

- **Principles (reasons for effectiveness)**

- Authority

-Intimidation

- Consensus

- Scarcity

- Familiarity

- Trust

- Urgency

1.2 GIVEN A SCENARIO, ANALYZE POTENTIAL INDICATORS TO DETERMINE THE TYPE OF ATTACK

- Malware

- Ransomware
- Trojans
- Worms
- Potentially unwanted programs (PUPs)
- Fileless virus
- Command and control
- Bots
- Cryptomalware
- Logic bombs
- Spyware
- Keyloggers
- Remote access Trojan (RAT)
- Rootkit
- Backdoor

• Password attacks

- Spraying

- Dictionary

- Brute force

- Offline

-Online

- Rainbow tables

- Plaintext/unencrypted

• Physical attacks

- Malicious universal serial bus (USB) cable

- Malicious flash drive

- Card cloning

-Skimming

- **Adversarial artificial intelligence (AI)**

- Tainted training data for machine learning

- Security of machine learning algorithms

- Supply-chain attacks
- Cloud-based vs. on-premises attacks
- Cryptographic attacks

- Birthday

- Collision

- Downgrade1.0 Threats, Attacks, and VulnerabilitiesCompare and contrast different types of social engineering techniques.

1.3 GIVEN A SCENARIO, ANALYZE POTENTIAL INDICATORS ASSOCIATED WITH APPLICATION ATTACKS

- Privilege escalation
- Cross-site scripting
- Injections

- Structured query language (SQL)

-Dynamic link library (DLL)

- Lightweight directory access protocol (LDAP)

- Extensible markup language (XML)

- Pointer/object dereference
- Directory traversal
- Buffer overflows
- Race conditions

- **Time of check/time of use**
-

- Error handling
- Improper input handling
- Replay attack- Session replays
- Integer overflow
- Request forgeries
-

- **Server-side**
- **Client-side**
- **Cross-site**

- Application programming interface (API) attacks
- Resource exhaustion
- Memory leak
- Secure sockets layer (SSL) stripping

- Driver manipulation

- Shimming

- Refactoring

- Pass the hash

1.4 GIVEN A SCENARIO, ANALYZE POTENTIAL INDICATORS ASSOCIATED WITH NETWORK ATTACKS.

-Wireless

- Evil twin

- Rogue access point

- Bluesnarfing

- Bluejacking

- Disassociation

- Jamming

- Radio frequency identifier (RFID)

- Near-field communication (NFC)

- Initialization vector (IV)

-

- Man-in-the-middle
- Man-in-the-browser
- Layer 2 attacks

- Address resolution protocol (ARP) poisoning

- Media access control (MAC) flooding

- MAC cloning

- Domain name system (DNS)

- Domain hijacking

- DNS poisoning

- Universal resource locator (URL) redirection

- Domain reputation

- Distributed denial-of-service (DDoS)

- Network

- Application

- Operational technology (OT)

- Malicious code or script execution

- PowerShell

- **Python**
- **Bash**
- **Macros**
- **Virtual Basic for Applications (VBA)**

1.5 EXPLAIN DIFFERENT THREAT ACTORS, VECTORS, AND INTELLIGENCE SOURCES

- Actors and threats

- Advanced persistent threat (APT)
- Insider threats
- State actors
- Hacktivists
- Script kiddies
- Criminal syndicates
- Hackers
- White hat
-Black hat
- Gray hat
- Shadow IT
- Competitors

- Attributes of actors

- Internal / external
- Level of sophistication / capability
- Resources / funding
- Intent / motivation

- Vectors

- Direct access
- Wireless
- Email
- Supply chain
- Social media
- Removable media
- Cloud

- Threat intelligence sources

- Open source intelligence (OSINT)
- Closed/proprietary
- Vulnerability databases

- Public/private information

- sharing centers

- Dark web

- Indicators of compromise

- Automated indicator sharing (AIS)

- Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII)

- Predictive analysis

- Threat maps

- File/code repositories

- Research sources

- Vendor websites

- Vulnerability feeds

- Conferences

- Academic journals

- Request for comments (RFC)

- Local industry groups

- Social media

- Threat feeds-Adversary tactics, techniques, and procedures (TTP)

1.6 EXPLAIN THE SECURITY CONCERNS ASSOCIATED WITH VARIOUS TYPES OF VULNERABILITIES

- Cloud-based vs. on-premises vulnerabilities
- Zero-day
- Weak configurations

-Open permissions

-Unsecure root accounts

-Errors

-Weak encryption

-Unsecure protocols

-Default settings

-Open ports and services

◦ Third-party risks

-Vendor management

-System integration

-Lack of vendor support

-Supply chain

-Outsourced code development

-Data storage

- Improper or weak patch management

-Firmware

-Operating system (OS)

-Applications

- Legacy platforms
- Impacts

-Data loss

-Data breaches

-Data exfiltration

-Identity theft

-Financial

-Reputation

-Availability loss

1.7 SUMMARIZE THE TECHNIQUES USED IN SECURITY ASSESSMENTS.

- Threat hunting

-Intelligence fusion

-Threat feeds

-Advisories and bulletins

-Maneuver

- Vulnerability scans

-False positives

-False negatives

-Log reviews

-Credentialed vs. non-credentialed

-Intrusive vs. non-intrusive

-Application

-Web application

-Network

-Common Vulnerabilities and Exposures (CVE)/ Common Vulnerability Scoring System (CVSS)

-Configuration review

- Syslog/Security information and event management (SIEM)

-Review reports

-Packet capture

-Data inputs

-User behavior analysis

-Sentiment analysis

-Security monitoring

-Log aggregation

-Log collectors

- Security orchestration, automation, and response (SOAR)Explain the techniques used in penetration testing

1.8 EXPLAIN THE TECHNIQUES USED IN PENETRATION TESTING.

- Penetration testing

-White-box

-Black-box

-Gray-box

-Rules of engagement

-Lateral movement

-Privilege escalation

-Persistence

-Cleanup

-Bug bounty

-Pivoting

- Passive and active reconnaissance

- Drones/ unmanned aerial vehicle (UAV)

-War flying

-War driving

-Footprinting

-OSINT

○

○

Exercise types

-Red-team

-Blue-team

-White-team

-Purple-team