Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

- **DNS Cache Snooping:** DNS cache snooping is a DNS enumeration technique whereby an attacker queries the DNS server for a specific cached DNS record.
- **DNSSEC Zone Walking:** DNSSEC zone walking is a DNS enumeration technique where an attacker attempts to obtain internal records of the DNS server if the DNS zone is not properly configured.
- **Dictionary Attack:** In this type of attack, a dictionary file is loaded into a cracking application that runs against user accounts.
- **Distributed Network Attack:** A Distributed Network Attack (DNA) technique is used for recovering passwords from hashes or password-protected files using the unused processing power of machines across the network.
- **DCSync Attack:** In a DCSync attack, an attacker initially compromises and obtains privileged account access with domain replication rights and activates replication protocols to create a virtual domain controller (DC) similar to the original AD.
- **Document Steganography:** Document steganography is the technique of hiding secret messages transferred in the form of documents.
- **Domain Dominance:** Domain dominance is a process of taking control over critical assets such as domain controllers on a target system and gaining access to other networked resources.
- **Data Protection API (DPAPI):** DPAPI is a unified location in Windows environments where all the cryptographically secured files, passwords of browsers, and other critical data are stored.
- **Downloader:** A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system.
- **Dropper:** A type of Trojan that covertly installs other malware files on to the system.
- **Dynamic Malware Analysis:** It involves executing the malware code to know how it interacts with the host system and its impact on the system after infection.
- **DHCP Starvation Attack:** This is a denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope.
- **DNS Poisoning:** DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when it has not received any
- **DNS Cache Poisoning:** DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site.
- **Diversion Theft:** The attacker tricks a person responsible for making a genuine delivery into delivering the consignment to a location other than the intended location.
- **Deepfake Attack:** A deepfake attack is a type of phishing attack in which attackers create false media of a person they target using advanced technologies such as ML and AI.
- **DoS Attack:** Denial-of-Service (DoS) is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.
- **DDoS Attack:** Distributed denial-of-service (DDoS) is a coordinated attack that involves a multitude of compromised systems (Botnet) attacking a single target, thereby denying service to users of the targeted system.
- **Distributed Reflection Denial-of-Service (DRDoS) Attack:** A distributed reflected denial-of-service attack (DRDoS), also known as a spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.
- **DNS over HTTPS:** DNS over HTTPS (DoH) is an enhanced version of DNS protocol, which is used to prevent snooping of user's web activities or DNS queries during the DNS lookup process.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

DO NOT COPY
shikridat@gmail.com

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

- **Demilitarized Zone (DMZ):** The demilitarized zone (DMZ) is an area that hosts computer(s) or a small sub-network placed as a neutral zone between a particular company's internal network and an untrusted external network to prevent outsider access to a company's private data.
- **Database Honeypots:** Database honeypots employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration.
- **DNS Server Hijacking:** Attacker compromises the DNS server and changes the DNS settings so that all the requests coming towards the target web server are redirected to his/her own malicious server.
- **Directory Traversal:** Directory traversal allows attackers to access restricted directories, including application source code, configuration, and critical system files to execute commands outside the web server's root application directory.
- **DNS Rebinding Attack:** Attackers use the DNS rebinding technique to bypass the same-origin policy's security constraints, allowing the malicious web page to communicate with or make arbitrary requests to local domains.
- **Dynamic Application Security Testing (DAST):** It is also known as a black-box testing approach and is performed directly on running code to identify issues related to interfaces, requests/responses, sessions, scripts, authentication processes, code injections, etc.
- **Direct-Sequence Spread Spectrum (DSSS):** DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code.
- **Directional Antenna:** A directional antenna can broadcast and receive radio waves from a single direction.
- **Dipole Antenna:** A dipole antenna is a straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line.
- **Distributed Control System (DCS):** DCS is a highly engineered and large-scale control system that is often used to perform industry specific tasks.
- **Docker:** Docker is an open source technology used for developing, packaging, and running applications and all its dependencies in the form of containers, to ensure that the application works in a seamless environment.
- **Data Encryption Standard (DES):** DES is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 56-bit key.
- **DSA:** The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures.
- **Diffie–Hellman:** It is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel.
- **Digital Signature:** Digital signature uses asymmetric cryptography to simulate the security properties of a signature in digital rather than written form.
- **DUHK Attack:** DUHK (Don't Use Hard-Coded Keys) is a cryptographic vulnerability that allows an attacker to obtain encryption keys used to secure VPNs and web sessions.
- **DROWN Attack:** A DROWN attack is a cross-protocol weakness that can communicate and initiate an attack on servers that support recent SSLv3/TLS protocol suites.

E

- **Email Indicators:** Email indicators are used to send malicious data to the target organization or individual.
- **Ethical Hacking:** Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities and ensure system security.

DO NOT COPY
shikrirdat@gmail.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.