1. Denial of Service (DoS) and Network Attacks

- R-U-Dead-Yet? (RUDY) is a DoS tool used to attack target web applications by starving available sessions on the web server using never-ending POST transmissions and an arbitrarily large content-length header value.
- DoS/DDoS countermeasure for jamming: disabling TCP SYN cookies is *not* recommended.
- DHCP Starvation Attack: An attacker sends many fake DHCP requests to exhaust IP addresses, causing denial of service.
- VLAN Hopping: Jumping between VLANs to access unauthorized network segments.
- Rogue DHCP Server Attack: Setting up a fake DHCP server to assign malicious network settings.
- STP Attack: Manipulating Spanning Tree Protocol to disrupt network topology.

2. Scanning and Enumeration Tools

- User2Sid, Sid2User, DumpSec are used for enumeration of users.
- nslookup, dig, host, sam spade are used for zone transfers.
- Nmap with -sV flag is used for service version discovery.
- Faster network scan example: `nmap -T4 -F 10.10.0.0/24`
- hping2 command for ICMP ping: `hping2 -1 host.domain.com`
- Cronjob example to capture traffic on IP range using tshark:
  `sudo tshark -f "net 192.168.8.0/24"`
- Infoga: Tool to gather email information from public sources and check if emails were leaked using haveibeenpwned.com API.

3. Footprinting and Reconnaissance

- Google dorking example: using `filetype:` in footprinting to find files with specific extensions.
- ARIN tool for footprinting IP: <https://search.arin.net/rdap>
- Proxy activities: adversaries use the same host with different domains to hide.
- Covert channel: using a protocol in a way it was not intended to be used.
- WARDriving: Searching for Wi-Fi networks by moving around in a vehicle.

4. Cryptography and Hashing

- LM Hash uses the DES algorithm and is used in old Windows systems (Windows 2000).
- Twofish is a symmetric encryption algorithm with 128-bit block size and up to 256-bit keys.
- MD4 is used in NTLM hashes.
- WEP (Wired Equivalent Privacy) is a weak encryption protocol for wireless networks.

5. Authentication and Authorization

- Authentication bypass using SQL injection example: `Username: ' or 1=1 --`
- 2FA example: smart card + PIN (something you have and something you know).
- RADIUS protocol handles Authentication, Authorization, and Accounting.
- NTLM protocol can be used to secure an LDAP service against anonymous queries.
- LDAP is not relational and cannot easily handle many-to-one relationships.
- GINA: Graphical Identification and Authentication DLL in Windows.
- TPM (Trusted Platform Module): Hardware component storing encryption keys securely on the motherboard to protect encrypted data.
- TACACS+: Mainly used for device administration, not ISP user authentication.
- DIAMETER: Successor to RADIUS, mostly used in mobile/IP multimedia systems.
- Kerberos: Internal network authentication, especially in Windows domains.

6. DNS and Network Protocols

- DNS AAAA record is used to resolve IPv6 addresses.
- DNS Spoofing/Poisoning involves changing DNS records. The first step for a hacker conducting DNS cache poisoning is making a request to the DNS resolver.
- Pharming: Redirects user’s web traffic to a fraudulent website by modifying the local hosts file or exploiting vulnerabilities in DNS.
- Phishing involves spoofed or misspelled URLs.
- MX record priority does not increase as the number increases.
- SOA Record Format: `<primary-name-server>, <responsible-email>, (<serial-number>, <refresh>, <retry>, <expire>, <minimum-TTL>)`

7. Security Concepts and Miscellaneous

- False Positive example: admin working triggers IDS alert.
- Rootkit found in the system: recommended action is to reload OS from known good media.
- A firewall with 3 interfaces is considered multihomed minimum.
- SNMP uses UDP port 161; SNMPv3 is secure.
- VRFY command is used to validate users on mail servers.
- Social engineering manipulates human behavior to gain access.
- USB dumper tools are used to dump files from USB devices.
- Pipe to extract links example:

  ```
  wget https://site.com | grep "<a href=" | grep "site.com"
  ```

- File-less Malware: Operates entirely in-memory, does not write files to disk. Hard to detect by traditional antivirus tools.
- Multipartite Virus: Infects both boot sector and executable files. Spreads in multiple ways and activates from multiple infection points.
- Null User in Windows: A pseudo account that has no username and password.
- Rubber-Hose Attack: Extraction of cryptographic secrets through coercion or torture.
- Stateful Firewall: Tracks the state of active connections and makes decisions based on the context of the traffic, allowing or blocking packets accordingly.
- Stateless Firewall: Treats each packet independently, filtering based on predefined rules without considering the context or connection state.
- Main Security Service of Cryptographic Hash: Provides Integrity and computational infeasibility.
- Digital Signature Process: Sender uses their private key to sign the message or its hash; receiver uses sender’s public key to verify authenticity, confirming integrity and authentication.
- Session Donation Attack: Attacker donates their own valid session ID to a victim, linking victim’s input data to attacker’s account without the victim's knowledge.
- Spimming: Sending spam messages over instant messaging platforms.
- Bluesnarfing: Unauthorized access of information from a Bluetooth device.
- Bluejacking: Sending unsolicited messages over Bluetooth without user consent.

- WS-Addressing enables asynchronous SOAP message routing; WS-Address spoofing modifies SOAP headers to redirect responses or hijack sessions.
- Internal Monologue Attack: Attacking based on internal system observations or theoretical weaknesses rather than external breaches.
- Combinator Attack: Combining multiple attack vectors or weaknesses to gain access.
- Rainbow Table Attack: Using precomputed hash tables to reverse cryptographic hashes and crack passwords faster.
- Dictionary Attack: Guessing passwords by systematically trying words from a prearranged list.
- Skimming: Stealing credit card information using a physical device.
- Promiscuous Mode: NIC mode that processes all network frames, used for packet sniffing and monitoring.

8. TTL Values for OS Identification

- Windows TTL: 128
- Linux TTL: 64
- OpenBSD TTL: 255

9. Healthcare and Compliance

- HIPAA/PHL regulations apply to the healthcare industry.

10. IoT Security

- First port to block on IoT devices after compromise: 48101.
- Mirai malware targets IoT devices to create a DDoS botnet.

11. NetBIOS Security

- NetBIOS ports to block: 135, 139, 445.

12. Threat Intelligence Types

Type	Level	Description	Example Info
Strategic	High-level	Non-technical for decision-makers	Trends, risks

Tactical	Short-term	Tactics, Techniques, Procedures (TTPs)	MITRE ATT&CK usage
Operational	Mid-term	Contextual, real-time info about attacks	Attack plans, motivations
Technical	Real-time	Indicators of Compromise (IOCs)	IPs, URLs, malware hashes

13. MIBs for Network Monitoring

- DHCP.MIB: Monitors DHCP traffic.
- HOSTMIB.MIB: Manages host resources.
- LNMIB2.MIB: Workstation and server services.
- MIBJI.MIB: TCP/IP internet management.
- WINS.MIB: Windows Internet Name Service.

14. Password Cracking Tools

- L0phtcrack and John The Ripper are well-known password-cracking programs.

15. SQL Injection

- Out-of-band SQL Injection (SQLi) occurs when an attacker uses the database server's ability to make DNS or HTTP requests to deliver data to the attacker.
- SQL Injection Vulnerability: `Username: ' or 1=1 --`

16. Attacks & Techniques

- Hybrid Attack: Combining both brute force and dictionary methods to have a variation of words.
- ACK Scan (-sA): Used to identify firewall type:
  RST responses → stateless firewall; No response or ICMP unreachable → stateful firewall

17. Network Concepts & Tools

- Packet Sniffers: Operate primarily at OSI Layer 2 (Data Link Layer).

18. Wireless Security

- An old encryption protocol designed to mimic wired encryption is WEP (Wired Equivalent Privacy).

19. Vulnerabilities & Exploits

- If the authentication mechanism exploits design flaws in the password reset mechanism, then it may lead to social engineering.

⁂