Create by: Ron Sharon
https://www.linkedin.com/in/ron-sharon/

200 Terms & 50 Windows Commend Shells Every SOC Analyst Should Know

Terms & commends	Explanation
IP Address	Identifies devices on a network; crucial for network traffic analysis and identifying sources of threats.
Subnet	Divides networks into smaller parts; important for organizing and securing network segments.
Firewall	Filters incoming and outgoing network traffic; essential for defending against unauthorized access.
VPN (Virtual Private Network)	Secures remote network access; critical for protecting data in transit.
TCP/IP (Transmission Control Protocol/Internet Protocol)	Fundamental protocols for data transmission; understanding these is key to analyzing network traffic.
DNS (Domain Name System)	Translates domain names to IP addresses; vital for understanding web traffic and detecting malicious domains.
DHCP (Dynamic Host Configuration Protocol)	Assigns IP addresses dynamically; important for managing network resources.
SSL/TLS (Secure Sockets Layer/Transport Layer Security)	Protocols for secure communication; essential for ensuring data confidentiality and integrity.
Port	Virtual communication endpoint; understanding ports is critical for network traffic analysis and intrusion detection.
NAT (Network Address Translation)	Maps private IP addresses to public ones; key for network security and resource management.
Intrusion Detection System (IDS)	Monitors network for suspicious activity; crucial for early threat detection.
Intrusion Prevention System (IPS)	Actively blocks threats; important for proactive network defense.
SIEM (Security Information and Event Management)	Aggregates and analyzes security data; essential for SOC analysts to monitor network health.
Packet	Basic unit of data in networks; understanding packet structure is fundamental for traffic analysis.
Protocol	Set of rules for data transmission; knowledge of various protocols (like HTTP, FTP) is crucial for understanding network communications.
Encryption	Secures data by encoding it; vital for protecting sensitive information.
Decryption	Converts encrypted data back to original form; necessary for data analysis and forensics.
VLAN (Virtual Local Area Network)	Segregates network logically; important for enhancing security and reducing broadcast domains.
DMZ (Demilitarized Zone)	Separates internal network from public internet; crucial for extra security layer around external-facing services.
Phishing	Deceptive attempt to obtain sensitive information; understanding phishing is key to identifying and mitigating social engineering attacks.
Malware	Malicious software; identifying and understanding different malware types (like viruses, worms) is crucial for defense.
DDoS (Distributed Denial of Service)	Overwhelms a service with traffic; recognizing DDoS patterns is essential for maintaining service availability.

Create by: Ron Sharon
https://www.linkedin.com/in/ron-sharon/

Botnet	Network of infected devices; crucial for understanding large-scale cyber threats.
SSL Inspection	Monitoring encrypted SSL/TLS traffic; important for detecting hidden threats.
Proxy Server	Intermediary between user and internet; understanding proxies is key for analyzing web traffic and bypassing restrictions.
WAF (Web Application Firewall)	Protects web applications; important for defending against web-based attacks.
Layer 7 (Application Layer)	Top layer of OSI model; understanding this layer is key for application-level security.
Layer 3 (Network Layer)	Handles routing and forwarding; crucial for understanding IP-level communications.
Layer 4 (Transport Layer)	Manages end-to-end communication; key for understanding TCP/UDP traffic.
Zero Trust Security Model	Assumes no inherent trust in network; important for implementing strict access controls.
Egress Filtering	Controls outgoing network traffic; vital for preventing data exfiltration.
Ingress Filtering	Monitors incoming traffic; important for blocking unauthorized access.
MAC Address (Media Access Control Address)	Unique identifier for network interfaces; crucial for network hardware identification.
ARP (Address Resolution Protocol)	Resolves IP addresses to MAC addresses; understanding ARP is key for network mapping.
Ransomware	Malware that encrypts data for ransom; important to know for preventing and responding to data hostage situations.
Sandboxing	Isolates applications for safe testing; vital for analyzing suspicious files.
IDS/IPS Signature	Patterns used to detect threats; understanding these helps in configuring and optimizing intrusion detection/prevention.
Incident Response	Process for handling security incidents; essential knowledge for mitigating and recovering from attacks.
Rootkit	Software that grants unauthorized access; crucial to understand for deep-level system threats.
SOC (Security Operations Center)	Centralized unit for handling security issues; core concept for SOC analysts.
Anomaly Detection	Identifying deviations from normal behavior; important for uncovering subtle security threats.
Endpoint Security	Protecting individual devices; crucial for a holistic security approach.
Cryptography	Study of secure communication techniques; fundamental for securing data.
Patch Management	Process of updating software; vital for maintaining security and functionality.
Compliance Standards (like GDPR, HIPAA)	Legal requirements for data protection; understanding these is key for maintaining legal and ethical standards.
Risk Assessment	Evaluating potential threats; essential for proactive security planning.

Create by: Ron Sharon
https://www.linkedin.com/in/ron-sharon/

Asset Management	Tracking organizational resources; crucial for security and operational efficiency.
Threat Intelligence	Information about emerging or existing threats; important for staying ahead of potential security issues.
Honeypot	Decoy system for attracting attackers; useful for gathering threat information.
Log Analysis	Examining records of network or system activity; fundamental for detecting and investigating security incidents.
SIEM (Security Information and Event Management)	Collects and analyzes security data from various sources; vital for real-time analysis, event correlation, and incident response.
SOAR (Security Orchestration, Automation, and Response)	Automates responses to cyber threats; essential for streamlining security operations and reducing response times.
Vulnerability Assessment	Process of identifying and prioritizing vulnerabilities; crucial for proactive security measures.
Penetration Testing	Simulated cyber attacks to test defenses; important for identifying weaknesses in security posture.
Threat Hunting	Proactively searching for cyber threats; key for identifying hidden or emerging threats.
Cyber Espionage	Unauthorized probing to steal intellectual property; understanding this helps in protecting sensitive information.
Dark Web Monitoring	Surveillance of hidden online networks; important for early detection of data breaches or illicit activities.
Two-Factor Authentication (2FA)	Adds an extra layer of security beyond passwords; crucial for verifying user identities.
Spear Phishing	Targeted phishing attacks; understanding this is key for recognizing sophisticated social engineering tactics.
Root Cause Analysis	Determining the underlying cause of a security incident; essential for preventing future occurrences.
Identity and Access Management (IAM)	Controls user access to resources; critical for ensuring that only authorized users have access.
Endpoint Detection and Response (EDR)	Real-time monitoring and response to threats on endpoints; vital for endpoint security.
Network Segmentation	Dividing a network into smaller parts; important for limiting the spread of attacks.
Cloud Security	Protecting data stored online; crucial in today's cloud-dominated environments.
Mobile Device Management (MDM)	Secures and manages mobile devices; important for protecting against mobile security threats.
Advanced Persistent Threat (APT)	A prolonged and targeted cyberattack; understanding APTs is key for recognizing and responding to sophisticated threats.
Cyber Resilience	The ability to prepare for, respond to, and recover from cyber attacks; essential for maintaining business continuity.
Data Loss Prevention (DLP)	Strategies to prevent data breaches; crucial for protecting sensitive information.
Forensic Analysis	Examining digital evidence after a security incident; important for understanding how an attack occurred.
Security Audit	Comprehensive evaluation of an organization's information system security; vital for ensuring compliance and security standards.

Create by: Ron Sharon
https://www.linkedin.com/in/ron-sharon/

Cross-Site Scripting (XSS)	Injecting malicious scripts into webpages; understanding XSS is important for web application security.
SQL Injection	Inserting malicious SQL queries; crucial for defending against database attacks.
Zero-Day Exploit	Attacking a previously unknown vulnerability; understanding this is key for anticipating and mitigating unforeseen threats.
Cryptography	The practice of secure communication; fundamental for data protection.
Blockchain	Distributed ledger technology; important for understanding emerging security applications.
Incident Response Plan	A predefined strategy for handling security incidents; essential for effective and timely response.
Business Continuity Planning (BCP)	Preparing for maintaining business functions during a crisis; crucial for minimizing impact of disruptions.
Disaster Recovery (DR)	Strategies for recovering from major failures; important for restoring systems and data after a disaster.
Risk Management	Process of identifying, assessing, and controlling threats; key for a comprehensive security strategy.
Social Engineering	Manipulating individuals to gain confidential information; understanding this is critical for recognizing non-technical threats.
Man-in-the-Middle Attack (MitM)	Intercepting communication between two parties; crucial for understanding network-based attacks.
Session Hijacking	Illegally taking over a user session; important for protecting user credentials and sessions.
File Integrity Monitoring (FIM)	Detects changes in files; vital for identifying unauthorized file modifications.
Access Control List (ACL)	Specifies who can access certain resources; essential for data and resource protection.
Public Key Infrastructure (PKI)	Framework for managing digital certificates; important for secure electronic transactions.
Security Policy	Formal set of rules on how to manage, protect, and distribute sensitive information; crucial for maintaining organizational security standards.
Blue Team	Internal security team that defends against both real attackers and Red Teams; key for maintaining strong defense mechanisms.
Red Team	Group that simulates cyber attacks; important for testing the effectiveness of security measures.
Purple Team	Blend of Red and Blue Teams; crucial for enhancing security defenses through collaborative testing.
White Hat Hacker	Ethical hacker who helps improve security systems; understanding their role is important for security improvement.
Black Hat Hacker	Hacker with malicious intent; key for understanding the range of cyber threats.
Grey Hat Hacker	Hacker who operates without malicious intent but without authorization; understanding their motivations is important for security analysis.
Cyber Warfare	Use of technology to attack a nation; crucial for understanding state-level cyber threats.

Create by: Ron Sharon
https://www.linkedin.com/in/ron-sharon/

Data Encryption Standard (DES)	A once-common symmetric-key method of data encryption; important for historical context of cryptography.
Transport Layer Security (TLS)	Protocol for secure internet communications; vital for protecting data in transit.
Secure Shell (SSH)	Protocol for secure system administration and file transfers; important for secure network management.
Hypertext Transfer Protocol Secure (HTTPS)	Secure version of HTTP; crucial for secure web browsing.
Content Delivery Network (CDN)	System of distributed servers; important for improving web performance and security.
Security by Design	Incorporating security in the software development process; key for creating inherently secure applications.
Security Awareness Training	Educating employees about cybersecurity; essential for mitigating human-factor risks.
ping	Checks network connectivity to another IP address.
tracert	Traces the route packets take to a specified host.
ipconfig	Displays all current TCP/IP network configuration values.
netstat	Displays active TCP connections, ports, etc.
nslookup	Queries DNS to obtain domain name or IP address mapping.
pathping	Combines the functions of `ping` and `tracert`.
arp	Displays and modifies the IP-to-Physical address translation tables.
getmac	Shows the MAC address of network adapters.
route	Views and modifies the IP routing table.
netsh	A tool to configure network settings.
net	Displays or modifies the network settings.
net user	Adds or modifies user accounts, or displays user account information.
net view	Displays network resources or computers.
net localgroup	Adds, displays, or modifies local groups.
net start / net stop	Starts or stops a network service.
sc	Manages services (start, stop, query, etc.).
tasklist	Displays all currently running processes.
taskkill	Terminates tasks by process ID or image name.
sfc	Scans and verifies the integrity of system files.
chkdsk	Checks disk for errors and displays status.
diskpart	Disk partitioning utility.
fsutil	Displays or configures file system properties.
systeminfo	Displays system configuration information.
whoami	Displays user, group, and privileges information.
wevtutil	Retrieves information about event logs and publishers.
cipher	Encrypts/decrypts files and folders.
certutil	Utility for certification authority (CA) files and services.
cacls / icacls	Displays or modifies access control lists (ACLs) of files.
xcopy	Copies files and directory trees.
robocopy	Advanced utility for copying files and directories.
attrib	Displays or changes file attributes.
shutdown	Allows proper shutdown or restart of the computer.
gpupdate	Updates Group Policy settings.
gpresult	Displays Group Policy information for a machine or user.

Create by: Ron Sharon
https://www.linkedin.com/in/ron-sharon/

bcdedit	Manages Boot Configuration Data.
bootrec	Utility for repairing boot configuration.
reg	Console tool for editing the registry.
wmic	Displays WMI information inside interactive command shell.
powercfg	Configures power settings.
find / findstr	Searches for strings in files.
timeout	Pauses command processing for a specified period of time.
fc	Compares two files and displays the differences.
convert	Converts FAT volumes to NTFS.
diskpart	Disk management from the command line.
driverquery	Displays current device driver status and properties.
openfiles	Displays files opened by remote users.
recover	Recovers readable information from a bad or defective disk.
replace	Replaces files.
set	Displays, sets, or removes environment variables.
telnet	Communicates with another host using the Telnet protocol.