CYBERSECURITY ANALYST TERMS CHEATSHEET

BLUE TEAM

- **Honeypots:** a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems.
- **Encryption:** the process of transforming plaintext into ciphertext.
- **Segmentation:** a network security technique that divides a network into smaller, distinct sub-networks that enable network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network.
- **Anti-Virus:** a program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.
- **White Listing**: a cybersecurity strategy under which a user can only take actions on their computer that an administrator has explicitly allowed in advance
- **Firewall:** a capability to limit network traffic between networks and/or information systems.
- **SIEM Alert:** A notification of a possible security event prompting an investigation designed to protect the organization.
- **Least Privilege:** the principle that users and programs should only have the necessary privileges to complete their tasks.
- **Two Factor Authentication:** a process which requires two steps in order to verify a user.
- **Tarpits:** a security mechanism against computer worms and network abuses like spamming.

RED TEAM

- **Phishing:** a digital form of social engineering to deceive individuals into providing sensitive information.
- **Social Engineering:** the art of manipulating people so they give up confidential information, whether it be passwords, bank information, or access to your computer to install malicious software.
- **Spoofing:** faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system.
- **Remote Access:** the ability for an authorized person to access a computer or network from a geographical distance through a network connection a user can only take actions on their computer that an administrator has explicitly allowed in advance.
- **Waterhole:** a specific website that attackers have identified as being frequently visited by their intended target. The attacker places malicious links to malware on the site in the hope that the target will be infected when they go there.
- **Bots:** a computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote the command and control of a remote administrator.
- **Physical Security:** the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise.
- **Security Misconfiguration:** security controls that are inaccurately configured or left insecure, putting your systems and data at risk.
- **Ransomeware:** a type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Malware:** software that compromises the operation of a system by performing an unauthorized function or process.

NATIONAL
CYBER GROUP

NationalCyber.com