CyberSN®

Where talent meets its match_

Threats, Vulnerabilities and Attacks

WCCC Workshop
May 17, 2021
9:00AM – 10:40AM

Mr. Dom Glavach
Chief Security Officer and Chief Strategist

Today's Session

CyberSN
Where talent meets its match.


Cybersecurity Background


Red, Blue and You


Threats


Vulnerabilities


Attacks

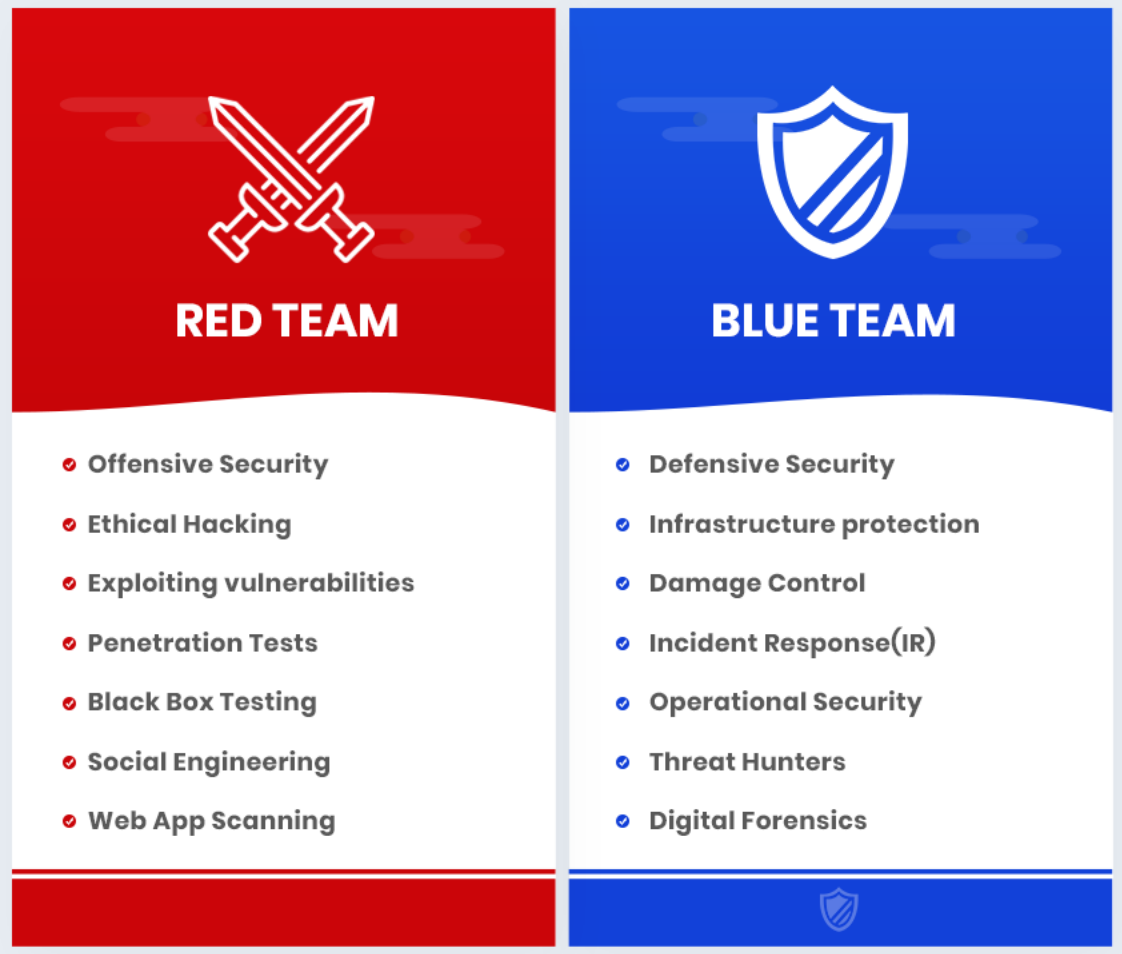

Lab

Cybersecurity Background

CyberSN
Where talent meets its match.

Career in Cybersecurity	Passion Curiosity Education Responsibility
Jobs	45 Job Categories 700+ Job titles More attacks then professionals
Today's Session	Interactive The best defense is a good offense

Red, Blue and You



Example resources

RED TEAM - https://www.exploit-db.com/

BLUE TEAM - https://isc.sans.edu/

EVERONE - https://www.kali.org/

Images from: https://hackernoon.com

Threats

Threat	An activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.
Threat Environment	Online space where cyber threat actors conduct malicious cyber threat activity.
Threat Actor	Groups or individuals who aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks.
Motivation	Threat actors value access to devices, processing power, computing resources, and information for different reasons. **Profit, Espionage, Satisfaction, Discontent, Ideologic, Curiosity**

Threat Actors

Nation-states	(APT) **Motivation**: Espionage
Cybercriminals	(Organized Crime) **Motivation**: Profit
Hacktivists	(Groups) **Motivation**: Satisfaction
Terrorist Groups	(Cyber Terrorists) **Motivation**: Disruption
Thrill-seekers	(Lone Wolves) **Motivation:** Curiosity/Satisfaction
Insider	(People) **Motivation**: None/Discontent

Threat Types

- Viruses
- Crypto-malware
- Ransomware
- Worm
- Trojan
- Rootkit
- Keylogger
- Adware
- Spyware
- Bots
- RAT
- Logic Bomb
- Backdoor
- RCE

Vulnerabilities

CyberSN
Where talent meets its match.

Race Conditions

Vulnerabilities Due to:

- End-of-Life Systems
- Embedded Systems
- Lack of Vendor Support

Untrained People

Improperly Configured Accounts

Improper Input/Error Handling

Misconfiguration/Default Configuration

Weak Cipher Suites and Implementations

Memory/Buffer Vulnerability

Resource Exhaustion

Architecture/Design Weaknesses

New Threats/Zero Day

Attacks

CyberSN
Where talent meets its match.

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

Interactive Lab

Capture the Flag (CTF) lab	Simulated attack space for learning and competitions
Tools needed	Web browser and curiosity
Target	Natas

//Begin

https://overthewire.org/wargames/natas/

Level 0 - Together

//Steps

CyberSN
Where talent meets its match.

Bookmark: https://overthewire.org/wargames/natas/

Username: natus0

Password natus0

Web Application Security CTF (each level requires login)