Blue Team Level 1 Certification (Standard) ‹

Introduction to BTL1

✓ ~~Welcome to Blue Team Level 1!~~
● 4 Topics

✓ ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

✓ ~~Introduction to Security Fundamentals~~
● 1 Topic

✓ ~~Soft Skills~~
● 7 Topics

✓ ~~Security Controls~~
● 5 Topics | 1 Quiz

✓ ~~Networking 101~~
● 6 Topics | 1 Quiz

✓ ~~Management Principles~~
● 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ ~~PA1) Introduction to Emails and Phishing~~
● 7 Topics | 1 Quiz

✓ ~~PA2) Types of Phishing Emails~~
● 10 Topics | 2 Quizzes

✓ ~~PA3) Tactics and Techniques Used~~
● 12 Topics | 2 Quizzes

✓ ~~PA4) Investigating a Phishing Email~~
● 8 Topics | 2 Quizzes

✓ ~~PA5) Analysing URLs, Attachments, and Artifacts~~
● 8 Topics | 1 Quiz

○ PA6) Taking Defensive Actions
● 12 Topics | 1 Quiz

○ PA7) Report Writing
● 7 Topics | 1 Quiz

○ PA8) Phishing Response Challenge
● 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence
● 7 Topics

○ TI2) Threat Actors & APTs
● 6 Topics | 2 Quizzes

○ Section Introduction, Actors

○ Common Threat Agents

○ Motivations

○ Actor Naming Conventions

○ What are APTs?

○ Tools, Techniques, Procedures

Activity) Threat Actor Research

Activity) End of Section Review, Actors

○ TI3) Operational Threat Intelligence
● 7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence
● 7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence

Motivations

Blue Team Level 1 Certification (Standard) > TI2) Threat Actors & APTs > Motivations IN PROGRESS

When we consider why people or groups conduct cyber attacks and operations, there are a number of motivations that may be involved. Motivations can typically be classed into one of four high level categories:

- **Financial Motives**
- **Political Motives**
- **Social Motives**
- **Unknown Motives**

FINANCIAL MOTIVES

Financial motives can be applied in a number of different ways. Whether it's an individual trying to make some quick money, a cyber crime syndicate bringing in more funds, or a government team trying to disrupt financial operations of hostile countries, money plays a large part in motivating cyber attacks.

- **Individual Financial Motives –** Corporate espionage is the act of retrieving private information from an organization and selling it for financial gain, potentially to competitors. This could be seen as a good idea by disgruntled employees who are planning on leaving their current organization soon and want to make a bit of money on the side before they leave.

- **Cyber Crime Financial Motives –** The theft and sale of confidential and personal information is a very lucrative activity and is generally the main motive for cyber crime syndicates. Ransomware is an ever-increasing threat where attackers deploy malware that encrypts any accessible files on the infected system and demands a ransom for the decryption key so the system owner can get their files back. Ransomware was estimated to cost businesses $1 billion in 2016, which increased to $8 billion in 2018, an 800% increase. The average cost of a ransomware attack in 2019 is estimated to be around $133,000. Criminals may also deploy cryptocurrency mining software on compromised systems in order to collect digital coins and cash these in. Another example of financial motives is the use of banking trojans, specialized malware that is designed to steal credentials to online banking websites to steal money from victims and transfer it to attacker-owned mule accounts.

- **Government Financial Motives –** A North Korea APT named Lazarus Group is made of two smaller teams, BlueNorOff, and AndAriel. Whilst AndAriel conducts prolonged and covert cyber operations against government targets in other countries, BlueNorOff focuses on hacking financial institutions such as banks, in order to steal funds. It is believed that this team is responsible for collecting funds to provide more resources to the other group within Lazarus. North Korea is subject to a number of economic sanctions from the US, and the perfect way to bypass these is by converting any stolen funds into the Monero cryptocurrency, using the darkweb as an unrecorded method of pulling funds into the country.

POLITICAL MOTIVES

Political motives are typically involved when nation-state teams, controlled and funded by governments, target governments in hostile nations. These attacks could be to disrupt operations of other countries, commit espionage and steal confidential information, send a message to the people of the target country, or other reasons that give the attacking country an advantage over their target.

- Cyber war is becoming an ever-more common reality. Not only does this type of warfare not require deployment of personnel, there is no geographical barriers, provided the target systems are connected to the internet in some way, or the air-gap can be compromised. An example of political motives being used in an act of cyber war was the Stuxnet virus, believed to be developed by the United States and Israel, used to target and degrade Iran's nuclear program, using not one, but **four** zero day exploits to ensure it could complete its mission.

- Another example of political motivations is when an individual or group (such as hacktivists) attempt to make a statement or express their political views by defacing government websites or using distributed denial-of-service attacks to take websites or services offline temporarily.

- Disinformation campaigns, whilst not technically cyber attacks, are an online activity where governments use bot accounts, dummy accounts, and paid advertising to spread incorrect information in an attempt to influence viewers. This type of activity is usually observed around government elections.

SOCIAL MOTIVES

Social motives are associated with self-beliefs. There are two main social motives associated with cyber attacks; making a statement and voicing your opinions on a subject that is important to you, or trying to boost your reputation or social status.

- Script kiddies, the derogatory term used to describe individuals with limited technical knowledge, are often known for operating with social motives, such as trying to boost their reputation and "showing off" to their friends, or people on the internet. This typically involves the script kiddie boasting online about their ability to conduct cyber attacks such as website defacement or distributed denial of service attacks, and then attempting to conduct these attacks using pre-built tools that require no skills or knowledge, such as online "stressors" or "booters" which are DDoS-as-a-service platforms, where you enter in your target and pay to launch attacks without needing any knowledge of botnets or networking.

- It's not just script kiddies that are looking for fame and attention. A number of hackers love to show off their illegal activity by posting to social media in order to increase their following and time in the spotlight. A great example of this is the disbanded group Lizard Squad, which are known for conducting distributed denial of service attacks against gaming companies, whilst tweeting on Twitter to gain attention. In August and November 2014 this group claimed responsibility for DDoSing League of Legends servers, Destiny servers, and PlayStation Network servers as well as DDoSing Xbox Live and Playstation Network at Christmas to prevent legitimate access to online features.

UNKNOWN MOTIVES

In some cases, it may not be immediately clear as to why a cyber attack was attempted or successfully conducted. This can make attribution harder as we can't use patterns to link the actor or actors to an established and documented threat group. In some cases, the motives may become clear in the future once more evidence has been collected and analyzed.

Previous Topic

Mark Complete ✓

Next Topic

Back to Lesson