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
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes

Prevention: Email Defenses

We have already covered basic email defenses in the Security Fundamentals domain. This lesson will cover typical email defenses in more detail, and what they do to protect the organization from attacks. We have already covered email defenses in detail in the Phishing Analysis domain Defensive Measures section. Let's recap on typical security controls to protect against malicious emails, URLs, and attachments.

SPF, DKIM, DMARC

Domain (DNS) records can be used for a wide variety of purposes, such as enabling a mail server to use a custom domain, host a website, and also offers the ability to set up anti-spoofing records as well. With many cyber-attacks coming from phishing emails and spoofing, these domain records help protect custom domain names from being exploited by an attacker. The following three record types; **SPF**, **DKIM** and **DMARC**; can be used together to help strengthen the security of an organizations email service.

Sender Policy Framework (SPF):

A Sender Policy Framework (SPF) record is a type of DNS (TXT) record that can help prevent an email address from being forged. This record is established to identify the hostnames or IP addresses that are allowed to send emails for your custom domain. When having an SPF record specified on your domain, this helps prevent a malicious actor from spoofing your domain. The SPF TXT record contains three parts: the declaration of the record type, the IP addresses and external domains that can send on your domain's behalf and an enforcement rule.

Domain Keys Identified Mail (DKIM):

Domain Keys Identified Mail (DKIM) is a method of email authentication that cryptographically verifies if an email has been sent by its trusted servers and hasn't be tampered during transmission. The way that DKIM works is that when the mail server sends an email, an encrypted hash of the email contents is generated using a private key and then it adds this hash to the email header as a DKIM signature. The receiving server will be able to verify whether the email contents have not been tampered with by looking up the corresponding public key in the domains DNS records. Once the receiving mail server decrypts the email with the public key, it calculates a new hash and verifies whether the original and the newly generated hash match to ensure email message integrity.

Domain-based Message Authentication, Reporting & Conformance (DMARC):

Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication, policy and reporting protocol. DMARC is built largely off of concepts taken from SPF and DKIM, but it adds several improvements for those protocols. This type of record allows the domain owner to specify what should happen if emails fail both SPF and DKIM checks. There are three basic options that the mail server can take: none, quarantine and reject.

MARKING EXTERNAL EMAILS

Employees must understand the risk of external emails. Although they could be legitimate from entities such as customers, employee personal email addresses, vendors, suppliers, and potential clients – the majority of phishing emails will come from external addresses. In platforms such as Microsoft Exchange or Office365, there is the ability to alter the subject line or body text of an email address that is coming into the organization to alert the recipient that this email isn't an internal communication, and could potentially be malicious. This simple warning can make

DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
Section Introduction, Preparation
Preparation: Incident Response Plan
Preparation: Incident Response Teams
Preparation: Assest Inventory and Risk Assessments
Prevention: DMZ
Prevention: Host Defenses
Prevention: Network Defenses
Legacy Activity) Setting up a Firewall
Prevention: Email Defenses
Prevention: Physical Defenses
Prevention: Human Defenses
Activity) End of Section Review, Preparation
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam

employees think twice about interacting with an external email, such as opening an attachment or clicking on a hyperlink.

A good idea is to apply a rule where any email coming from an external sender into the organisation has the subject line appended with a very short message, such as "[EXTERNAL]" or "[EXT]". Appending messages to subject lines can be counterproductive, and make it hard for employees to read subject lines at a glance, so some organizations opt to add a message to the top of the email body content using a bright font color such as red, so that it stands out and isn't missed by employees.

SPAM FILTER

Spam filters were created with the end-user in mind. Since the rise of email messaging and the internet in the 1990s, more and more cyber-attacks can often be delivered through email services. Phishing attempts, social engineering and payloads delivered through email can all be caught through a spam filter, depending on the type of filter and how they are configured. Because of the plethora of filters, there are three main types of spam filters that could be utilized:

1. **Gateway Spam Filters –** Ones that sit behind an on-premises firewall of a network. These can often be utilized by larger enterprise organizations and an example of a Gateway filter is the Barracuda email security gateway
2. **Hosted Spam Filters –** These are ones that are hosted within the cloud. These work very similar to gateway spam filters but are able to able to update more quickly than some of the on-premises filters and an example of a hosted filter is SpamTitan.
3. **Desktop Spam Filters –** These filters are user-installed and are typically used in SOHO scenarios. One major drawback of these kinds of filters is that they can sometimes be categorized as "Freeware" and you may not fully know what the application is installing on your system

DATA LOSS PREVENTION

Data loss prevention or data leak prevention is the name given to security controls that work to prevent business information such as files or confidential messages including information such as banking or employee details leaving the organization, in this case via email. Depending on the DLP solution in use, it can monitor outgoing emails at different levels, such as:

- email body content
- email headers
- email attachments of various types
- nested attachments of various types

If the DLP solution deems important information is about to be sent out of the organisation, these emails will not make it past the email gateway and will not be sent. Emails can be scanned for specific keywords, or use regex queries to flag messages containing certain content. If a disgruntled employee wants to send business critical information to a rival organization before they are fired, they could attempt to send documents outside the organization by email – DLP would detect this, alert the security team, and prevent the email from being sent.

SANDBOXING

Malicious attachments get through email gateways. This is often because pre-defined rules and configurations are used to block specific file types or naming conventions, meaning that files which look legitimate, such as Microsoft Office documents with malicious macros can sail through and land in employee mailboxes. This is where attachment sandboxing comes in – emails that include file attachments are extracted and analysed, and files and detonated (run) in a virtual environment, where everything is monitored to see actually what happens when a file is executed. If any malicious indicators are observed, such as trying to download additional files from a malicious domain, or trying to create or alter existing processes, the attachment is classed as malicious, and the email will not be delivered.

ATTACHMENT RESTRICTIONS

It isn't a good idea to block attachments outright – employees will have difficulty sending legitimate documents internally and externally. The most appropriate way to approach this situation is to consider what file types are

often used for malicious purposes, which file types the organisation deals with on a regular basis, and whether blocking them would have any negative impact on the business. The most obvious file types that are used for malicious activity are:

- **.exe** (Executable)
- **.vbs** (Visual Basic Script)
- **.js** (JavaScript)
- **.iso** (Optical Disk Image)
- **.bat** (Windows Batch File)
- **.ps/.ps1**
- **.htm/.html**

SECURITY AWARENESS TRAINING

Employees should routinely undergo security awareness training, that reminds them of their role in protecting the organisation, as it is everyone's job. This training should focus on policies that employees must adhere to, but also cover phishing topics such as; how to spot an email, and what to do when they find a suspicious email. This type of training works to address phishing at the human level, as it is a social engineering attack, and needs an employee to fall victim for the attack to succeed. Routine simulated phishing campaigns should be conducted against employees to gather metrics based on the number of employees that reported the emails as being malicious, and the number of employees that clicked on the link. Employees that have unfortunately fallen for the phishing attack should be given additional training and time to ensure they are able to spot and respond to these attacks in the future.

Previous Topic

Mark Complete

Next Topic

Back to Lesson