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
  - Section Introduction, Emails and Phishing
  - How Electronic Mail Works
  - Anatomy of an Email
  - What is Phishing?
  - Impact of Phishing
  - Further Reading Material, Phishing Analysis
  - Phishing Analysis Glossary
  - Activity) End of Section Review, Emails and Phishing
- 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

How Electronic Mail Works

Before we teach you about phishing, it's important that you understand how electronic mail works, both in terms of protocols and infrastructure. This lesson will go over protocols such as SMTP and POP3, email servers, relays, and email clients. Once you have a good understanding of how email works, we will cover how emails are composed, and how we can retrieve useful information from them with the ultimate goal of protecting an organization from future phishing attacks.

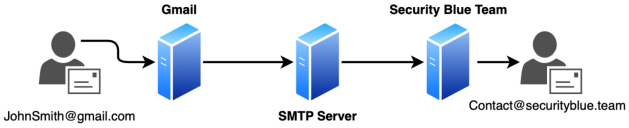
EMAIL ADDRESSES

Most people send emails on a daily basis – but what actually is an email address, and how does it help us to send and receive emails? Email addresses are composed of two parts, a mailbox and a domain. Let's take a look at an example:

In the above example we can see that the mailbox (also known as the 'localpart') is named **"contact"** and the domain is **"securityblue.team"**. We use a number of other mailboxes here at SBT, including:

- **certified@securityblue.team**
- **business@securityblue.team**
- **joshua@securityblue.team**

So in its simplest form, email addresses help us to select the recipient of our message to ensure it reaches the right person or people. In the below example the sender is **JohnSmith** (mailbox) **@gmail.com** (domain), and the recipient is **contact** (mailbox) **@securityblue.team** (domain):



Don't worry about the servers or how emails are actually transported, we'll cover that in the below sections.

EMAIL PROTOCOLS

TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 2 Quizzes
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
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 | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 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

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol works on TCP port 25 by default, is a communication protocol for electronic mail transmission. Once an email is created it is sent to the organization's SMTP server, which transports the email to the next server, before it eventually reaches the SMTP server of the recipient organization.

However, the world is moving away from port 25 and the new standard is becoming TCP port 587. This port, coupled with TLS encryption, will ensure that email is submitted securely and following the guidelines set out by the IETF.

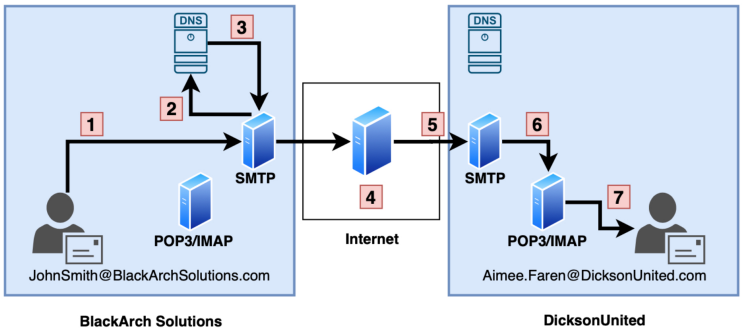
Post Office Protocol 3 (POP3)

Post Office Protocol (POP) is an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server, with version 3 (POP3) being the most widely-used version on the internet. POP works by contacting your email server and downloading all emails from it. Once they are downloaded onto your system, they are deleted from the email server. This means that after the email is downloaded, it can only be accessed using the computer that downloaded the emails and trying to access your emails from a different device will not work.

Internet Mail Access Protocol (IMAP)

IMAP allows you to access your email wherever you are, from any device. When you read an email message using IMAP you're reading it from the email server. As a result, you can check your email from different devices, such as from a laptop, desktop, and mobile phone. IMAP still allows for emails to be downloaded, but you must manually click to save the email locally. This method for accessing emails is a lot more common than using POP, as it allows for better accessibility.

In the below diagram, we will be following a scenario where John Smith working at BlackArch Solutions is emailing a friend, Aimee Faren at DicksonUnited. We will cover which protocols are used to deliver emails, and make them accessible by clients.



1. John Smith writes the message in his email client, which is sent to the organization's outbound SMTP server. At this point, the server doesn't understand where "DicksonUnited.com" is.
2. The outbound SMTP server queries the DNS server to find the IP address that is associated with "DicksonUnited.com".
3. The result is sent back to the SMTP server so it now understands where to send the email to.
4. The message is sent across the internet and may pass through other SMTP servers on the way.
5. The email reaches the destination domain's outbound SMTP server.
6. The email is moved from the first server via SMTP to a different server running either POP3 or IMAP, which allows the recipient to log into a client and access the email that is stored on the mail server.

WEBMAIL

While we can access emails via an email client such as the Outlook application or Mozilla's Thunderbird program, a more convenient method is to use webmail. These are web-based email accounts, such as those offered by

Exam Preparation
Using RDP and SSH
How to Start Your Exam

Hotmail/Outlook, Gmail, and Yahoo Mail. Internet service providers often provide free webmail accounts as part of their internet service package. Webmail allows users to access their emails as long as they have access to an Internet connection and a web browser. As with any web application, webmail's main advantage over the use of a desktop email client is the ability to send and receive email from anywhere via a web browser, such as your laptop, desktop, phone, or tablet. The main disadvantage is that email cannot be accessed without an internet connection, which can be done with an email client, where emails are downloaded and stored locally.

GoDaddy has a great short article on webmail.

Previous Topic
Back to Lesson
Next Topic

Privacy & Cookies Policy
Privacy - Terms