Blue Team Level 1 Certification (Standard)
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
Section Introduction, Phishing Response
Video) Phishing Response Walkthrough
Phishing Response Brief
Lab) Phishing Response Challenge
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
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

Video) Phishing Response Walkthrough

This video is designed to provide you with a complete walkthrough, from email analysis to basic report writing, so that you can complete this next activity, and prepare for phishing-related aspects of the Blue Team Level 1 practical exam. This video will encompass everything you have learned so far in this domain.

Transcript:

In this video, we'll be walking through an entire phishing invesitgation. The email we'll be analysing is a TV licensing-themed message, trying to entice the recipient to click on a link.

First we need to record a brief description of the email. This should typically be one or two sentences about the styling and intent. We are going to mention the email is impersonating TV Licensing, and is well styled.

Next, it's time to retrieve artifacts. We'll open the email using Sublime Text 2 and start collecting email-based artifacts. First we grab the sending address under the "from" property.

Below that is the subject line, date the email was sent, the recipient, and we can search for the sender IP address, which is 40.92.4.54 in this scenario. We need to get the reverse dns result of this IP, so let's use the whois search by domain tools to retrieve the hostname. We can see it's owned by Microsoft, and is an outlook server, which makes sense as the sending address is an @hotmail address.

We need to URL from the email, so we'll carefully right-click and select copy-hyperlink.

Now we start the analysis stage. Let's put the domain into VirusTotal to see the reputation. Looks like it's been flagged for malicious and phishing activity. Next we'll put the URL into URL2PNG to see what the page looks like. It seems the site is no longer

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
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

active. Let's double check in wannabrowser. Again, we're told the site is no longer available.

Performing a WHOis search for the domain shows us that it was created 42 days ago. This is very suspicious – domains that are used for malicious activity and have a low domain age are typically created purely for malicious intent, as opposed to being a legitimate domain that has been compromised.

We need to note down the results from our virustotal, URL2PNG, wannabrowser, and WHOis searches.

Next we need to decide on defensive measures. As the domain has been flagged on virustotal for malicious and phishing activity, and that it has been linked in malicious emails sent to an employee, along with the fact it has a very young domain age, there doesn't appear to be any negative impact to the business if we block the domain.

Next is the email defensive measures. As the sender is using a Hotmail address, the best response would be to block this address on the email gateway, preventing it from delivering more malicious emails.

And there we have it! It's time to put your skills to the test. In the next activity you will be required to identify malicious emails mixed with legitimate emails, and analyse them to collect artifacts and determine appropriate defensive measures.

Previous Topic
Mark Complete
Next Topic
Back to Lesson