Blue Team Level 1 Certification (Standard)

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

✓ ~~Section Introduction, Defensive Measures~~

✓ ~~Preventative Measures: Marking External Emails~~

○ Preventative Measures: Email Security Technology

○ Preventative Measures: Spam Filter

○ Preventative Measures: Attachment Filtering

○ Preventative Measures: Attachment Sandboxing

○ Preventative Measures: Security Awareness Training

○ Reactive Measures: Immediate Response Process

○ Reactive Measures: Blocking Email-Based Artifacts

○ Reactive Measures: Blocking Web-Based Artifacts

○ Reactive Measures: Blocking File-Based Artifacts

○ Reactive Measures: Informing Threat Intelligence Team

Activity) End of Section Review, Defensive Measures

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

Preventative Measures: Spam Filter

Blue Team Level 1 Certification (Standard) > PA6) Taking Defensive Actions > Preventative Mea... IN PROGRESS

Spam can be classified as unwanted commercial emails or soliciting emails and these messages can often lead to annoyances, lost time/money and potentially malware depending on the intentions of the spammer and the actions done by the user. To prevent these kinds of messages from being delivered into email systems inboxes, spam filters were created. There are hundreds, if not thousands of spam filters used throughout the world and these are used in conjunction with existing email services or are built into services such as Gmail and Outlook. These filters use rulesets, algorithms, machine learning, community interaction and a variety of other techniques to determine what emails are spam, and what emails are legitimately meant for the receiver.

WHY IS IT IMPORTANT?

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 excess 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 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

TYPES OF SPAM FILTERS

Since each vendor/email service uses different kinds of spam filters, these can be broadly classified by the way they detect spam:

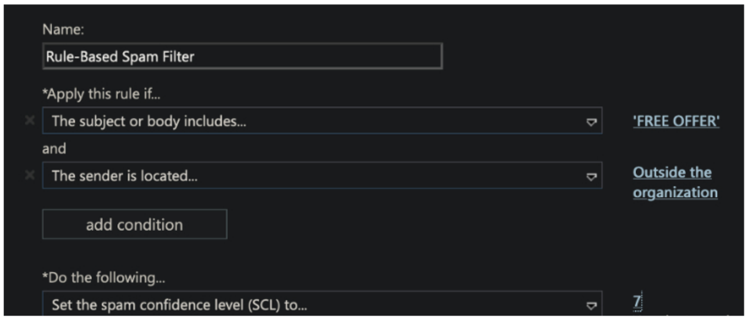
Content Filters

A content filter is the classic depiction of a spam filter and uses information in the email header and body to try to determine whether the email is legitimate or spam. When looking at the header, the filter could cross-reference the header with published blacklists or known spamming networks and automatically classify it as spam. When this filter scans the body of the message it could, for example, look for adult-oriented content and determine that as spam, based on preferences set on the account.

Rule-Based Filters

A rule-based filter allows for emails to be filtered based on predetermined criteria. A good example of this is Mail Flow rules in Microsoft Exchange where you could say:

If the subject or body contains "FREE OFFER" and the Sender is located Outside of the Organization, raise the likelihood of the message being spam



Name:
Rule-Based Spam Filter

*Apply this rule if...
The subject or body includes... 'FREE OFFER'
and
The sender is located... Outside the organization

*Do the following...
Set the spam confidence level (SCL) to... 7

Bayesian Filters

Bayesian filters have become one of the most intelligent types of spam filters that can be used. This is because it can often utilize concepts such as machine learning, to learn the users' spam preferences. For example, when the user marks an email as spam, it can analyze the characteristics of that message and use that information to block similar messages from going to the inbox. One slight downside to this kind of filter, however, is that it can often require a large amount of spam to efficiently utilize the machine learning capabilities.

While there are many other kinds of filters, the three listed above are some of the most widely used. One important thing to note about spam filters is that they need to be configured correctly to work properly. If the individual maintaining a Bayesian filter flags legitimate email, then the system will start classifying legitimate email as spam. It is important to maintain proper configurations and provide user-training on what should and shouldn't be considered spam.

CONCLUSION

A spam filter is arguably the most basic email defense an organization can deploy to reduce the number of spam and unsolicited emails reaching employee mailboxes. Whilst some phishing emails will still bypass this defense, by reducing emails that are not business-related, employees will have less junk in their mailboxes and will report fewer emails to the security team, so they can focus on real phishing emails.

Previous Topic | Mark Complete ✓ | Next Topic

Back to Lesson