Blue Team Level 1 Certification (Standard)

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

~~Section Introduction, Tactics and Techniques~~

~~Spear Phishing~~

~~Impersonation~~

~~Typosquatting and Homographs~~

~~Sender Spoofing~~

~~HTML Styling~~

~~Attachments~~

~~Hyperlinks~~

~~URL Shortening Services~~

~~Use of Legitimate Services~~

~~Business Email Compromise~~

~~[Video] Tactics and Techniques & Examples~~

~~Activity) Reporting on Tactics Used~~

~~Activity) End of Section Review, Tactics and Techniques~~

~~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

Sender Spoofing

Sender spoofing is the process of making the sending address in an email look the same as a legitimate email to make the recipients believe it is coming from a genuine sender. This is typically used with credential harvesters where the attacker wants the recipient to believe the email has actually come from the impersonated company so they will be more likely to enter in valid credentials.

HOW SPOOFING WORKS

In a spoofing attack, the malicious actor sends an email with a "From:" address that appears to be from a source the recipient trusts, such as a well-known brand, work colleague, or family member. There is no verification done at this point, so SMTP emails can use any FROM address they want. Want to send an email that looks like it comes from contact@securityblue.team? You can! (But don't.)

EXAMPLE WALKTHROUGH

Example 1 (FROM address)

Let's put on our black hats and go through an example where we want to phish the user James.Smith@DicksonUnited.co.uk. James has done his security awareness training, and is pretty good at spotting suspicious emails. Any email coming from an external domain is probably going to alert him. So let's pose as the IT service desk at DicksonUnited. We craft an email with the FROM address on our SMTP server set as "ServiceDesk@DicksonUnited.co.uk and send it to James, including a hyperlink to an Office365 credential harvester. James falls for it, because on his end the email looks 100% legitimate, and he doesn't question the call to enter his email details in, as he thinks it's come from the IT Service Desk, who manage email accounts.

Detecting this attack: Although the FROM address will look completely legitimate, we can look at the sending server IP (X-Originating-IP) and perform a WHOis or IP lookup search to determine whether this server actually belongs to the organization the email claims to be from. We will cover email security technology that can prevent against these emails, such as SPF, DKIM, and DMARC, that are elaborated on in **PA6) Taking Defensive Actions**.

Example 2 (FROM address with Reply-to)

If we send an email as *contact@amazon.com*, and we want the user to reply to us, the reply would actually go to contact@amazon.com, and we don't want that, as we'll never see it. That's where the Reply-to address comes in. When crafting our email, we can set a value for the Reply-to address as an email address that we actually have access to, such as *hacktheplanet@gmail.com*, and set the From address to *contact@amazon.com*. Now if the recipient replies, it will be sent to the Gmail address and we can read it.

Detecting this attack: We can look at the Reply-to address and see where replies would be sent. We can then block this address on the email gateway to prevent emails going outbound to this address. We will cover email security technology that can prevent against these emails, such as SPF, DKIM, and DMARC, that are elaborated on in **PA6) Taking Defensive Actions**.

○ T16) Malware and Global Campaigns

● 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics

● 5 Topics

‹ Previous Topic

Back to Lesson

Next Topic ›