|  |  |  |
| --- | --- | --- |
| **Student Name** | **:** |  |
| **Student ID** | **:** |  |
| **Class** | **:** |  |

**Objectives of the exercise:**

By the end of this lab, students should be able to:

* Analyze a phishing attack captured in a PCAP file.
* Identify suspicious DNS, HTTP, and SSL/TLS traffic.
* Detect malicious IPs, domains, and file transfers.
* Apply investigation techniques using Wireshark and VirusTotal.

**Requirement:**

* Wireshark installed on Windows PC
* PCAP File: **12\_2014-10-01-phishing-malware-run-on-a-VM**
* Internet access
* VirusTotal website (<https://www.virustotal.com/>)

**Instruction: Open Wireshark and Load the PCAP file**

1. Open Wireshark.
2. Click Open, browse to the location of **12\_2014-10-01-phishing-malware-run-on-a-VM.**
3. Load the PCAP file into Wireshark.

**Part 1: Inspect HTTP Traffic**

1. Filter HTTP traffic: **http**.

|  |
| --- |
| **Answer:** |
|  |

1. Look for **HTTP GET** requests to fake login pages.

|  |
| --- |
| **Answer:** |
|  |

1. Check if the server responded successfully:
   1. Identify File Data successfully transferred (in bytes).

|  |
| --- |
| **Answer:** |
|  |

1. Identify **HTTP 301/302** redirects:
   1. Right-click an **HTTP packet** → **Follow** > **TCP Stream**.

|  |
| --- |
| **Answer:** |
|  |

* 1. Examine HTTP headers for redirect locations.

|  |
| --- |
| **Answer:** |
|  |

1. List any Redirect Webpages found from the "Location" field.

|  |
| --- |
| **Answer:** |
| https://www.torproject.org/projects/torbrowser.html.en |

**Part 2: Inspect Suspicious SSL/TLS Traffic**

1. Apply filter: **tls**.

|  |
| --- |
| **Answer:** |
|  |

1. Locate Server Hello packet.
   1. Right-click the packet → Expand Transport Layer Security → Select Certificate.

|  |
| --- |
| **Answer:** |
|  |

1. Inspect for:
   1. Self-signed certificates.

|  |
| --- |
| **Answer:** |
|  |

* 1. Expired certificates.

|  |
| --- |
| **Answer:** |
|  |

1. Identify any suspicious indicators.

|  |
| --- |
| **Answer:** |
| 1. Login redirection to unknown site – various issuers (right-click any server hello packet, check the issuer in the certificates)      1. Self-signed TLS cert to suspicious domain – various subjects (right-click any server hello packet, check the issuer in the certificates)      1. DNS queries to random or lookalike domains (use dns filter). |

**Part 3: Identify Malicious IP**

1. Copy the IP addresses from suspicious traffic (from Part 2).

|  |
| --- |
| **Answer:** |
| Use the redirect webpages from part 1: <https://www.torproject.org/projects/torbrowser.html.en>  IP address: 204.8.99.146 |

1. Check each IP address using VirusTotal.

|  |
| --- |
| **Answer:** |
|  |

1. Identify if the IP is flagged as malicious by any vendors.

|  |
| --- |
| **Answer:** |
|  |

1. List the vendor names that flagged the IPs.

|  |
| --- |
| **Answer:** |
| Webroot (Malicious - Low)  MC-000150-MW: Indicators of Compromise Associated with Hive Ransomware - according to source ArcSight Threat Intelligence - 1 year ago  Contextual Indicators: The URL is known benign by Check Point's Threat Cloud Contextual Indicators: The domain is popular among websites with good reputation Contextual Indicators: The domain’s Alexa rank is 6485 Created On: 2006:10:17 00:00:00 VirusTotal Link: https://www.virustotal.com/gui/domain/eb4a598e265be2ab9581e18ee5332d89ba1efeb94058f06ecd16a7b882d4f0bc/detection Classification Description: Legitimate website which does not serve any malicious purpose. |

**Part 4: Analysis of Phishing Attacks**

**Discuss:**

1. The importance of firewalls or DNS filtering in detecting and blocking phishing attacks.

|  |
| --- |
| **Answer:** |
| **Any relevant answers. Provide at least 2 points.**   1. **Firewalls act like security guards** – They block bad websites and suspicious connections before they can reach your computer. This helps stop phishing attacks from stealing your data. 2. **DNS filtering stops you from visiting fake websites** – Even if you click on a phishing link, DNS filtering checks if the website is dangerous and blocks it, so you don’t get tricked. |

**Elaborate:**

1. Methods users can use to recognize phishing websites, such as:

|  |
| --- |
| **Answer:** |
| **Any relevant answers. Provide at least 2 points.**   1. **Check the URL carefully** – Phishing sites often use misspelled names or extra words, like paypa1.com instead of paypal.com. 2. **Look for HTTPS and the padlock symbol** – Real websites usually use secure connections. No padlock or a warning sign means it could be fake. 3. **Watch for urgent or scary messages** – Phishing sites often say things like “Your account is locked!” to make you panic and act fast. 4. **Don’t trust pop-ups asking for login info** – Real websites rarely ask for passwords in pop-up windows. 5. **Check for poor design or grammar** – Fake sites often have spelling mistakes, weird logos, or low-quality design. |