CYBR Investigation – Stage 1: Mapping the External Network

1. Mapping the crime scene

Explore the pcap file and fill out the blanks in the tables with the details of the devices on the network.

*Note: To make it easier for you the number of empty cells is the number of suspicious activities you should point out.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Host IP Address** | | 8.8.8.8 | | | | | | |
| **Host MAC Address** | | 34:49:5b:0c:1a:b7 | | | | | | |
| **Number of connections** | | | 4 | | | | | |
| **Destination IP Address** | **Destination MAC Address** | | | **Protocol Used** | **Content of communication** | **Additional information** | **Sus?** | **Timestamp** |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | DNS | Replying to DNS query | Queried for   * [www.funny-cat-photos.com](http://www.funny-cat-photos.com/) * [www.secmobile.com.sg](http://www.secmobile.com.sg/) | No | Jul 22, 2024 17:33:42.000000000 Malay Peninsula Standard Time  (Either timestamp is fine, the funny-cat-photos packet time or secmobile packet time mark as correct) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Host IP Address** | | 5.4.3.2 | | | | | | |
| **Host MAC Address** | | 00:26:0b:b2:74:d2 | | | | | | |
| **Number of connections** | | | 19 | | | | | |
| **Destination IP Address** | **Destination MAC Address** | | | **Protocol Used** | **Content of communication** | **Additional information** | **Suspicious?** | **Timestamp** |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | HTTP | Obtaining secmobile webpage | HTTP reply has 2 custom flags. | Yes | 2934838 |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | FTP | Successful login to the FTP server and download a file called Secmobile.4.2.1.exe |  | Yes |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Host IP Address** | |  | | | | | | |
| **Host MAC Address** | |  | | | | | | |
| **Number of connections** | | |  | | | | | |
| **Interesting details (If any)** | | | Device Brand: Oracle | | | | | |
| **Destination IP Address** | **Destination MAC Address** | | | **Protocol Used** | **Content of communication** | **Additional information** | **Sus?** | **Timestamp** |
| 8.8.8.8 |  | | | DNS | DNS query | Queried for:   * [www.secmobile.com](http://www.secmobile.com/) * [www.funny-cat-photos.com](http://www.funny-cat-photos.com/) | No |  |
| 5.4.3.2 | 00:26:0b:b2:74:d2 | | | HTTP | Obtaining Secmobile webpage | NIL | No |  |
| 5.4.3.2 |  | | | FTP | Logging in requests and downloading a file | NIL | Yes |  |
|  | 00:0f:20:e6:c0:13 | | | TCP |  | NIL | Yes |  |
| 10.0.0.37 |  | | | TCP |  | NIL | Yes |  |
|  | 00:0f:20:d4:4f:3a | | | TCP |  | NIL | Yes |  |
| 10.0.0.100 |  | | | Telnet |  | NIL | Yes |  |
|  |  | | | SMTP |  | NIL | Yes |  |
|  | 00:0f:20:d4:4f:3a | | | HTTP | Established 3-way handshake. After receive HTML, no further traffic | NIL | No |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Host IP Address** | | 10.0.0.12 | | | | | |
| **Host MAC Address** | | 00:22:fb:9e:c9:d7 | | | | | |
| **Number of connections** | | | 8 | | | | |
| **Interesting details (If any)** | | | Device Brand: Intel | | | | |
| **Destination IP Address** | **Destination MAC Address** | | **Protocol Used** | **Content of communication** | **Additional information** | **Sus?** | **Timestamp** |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | TCP | Rejecting connection to ports 21, 23, 25, 80. Could be port scanning | NIL | Yes | 2582812 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Host IP Address** | | 10.0.0.37 | | | | | | |
| **Host MAC Address** | | 00:0d:56:a2:b8:52 | | | | | | |
| **Number of connections** | | | 15 | | | | | |
| **Interesting details (If any)** | | | Device Brand: Siemens | | | | | |
| **Destination IP Address** | **Destination MAC Address** | | | **Protocol Used** | **Content of communication** | **Additional information** | **Sus?** | **Timestamp** |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | TCP | TCP SYN Scan (port scanning) | NIL | Yes | 2663216 |
| 104.16.107.144 | 00:26:0b:8f:bb:8f | | | HTTP | Accessed [www.funny-cat-photos.com](http://www.funny-cat-photos.com/) | NIL | No | 3135348 |
| 8.8.8.8 | 34:49:5b:0c:1a:b7 | | | DNS | DNS query | Queried for:   * [www.funny-cat-photos.com](http://www.funny-cat-photos.com/) | No | 3115272 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Host IP Address** | | 10.0.0.100 | | | | | |
| **Host MAC Address** | | 00:0f:20:d4:4f:3a | | | | | |
| **Number of connections** | | | 15 | | | | |
| **Destination IP Address** | **Destination MAC Address** | | | **Protocol Used** | **Content of communication** | **Suspicious?** | **Timestamp** |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | TCP | Port scanning? | Yes |  |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | Telnet | Login credentials? | Yes |  |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | SMTP | 3-way handshake established; no further communication upon SMTP message sent | Yes |  |
| 10.0.0.5 | 00:0f:4b:5f:0c:b9 | | | HTTP | 3-way handshake established; sent webpage | No |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Host IP Address** | | 192.168.0.11 | | | | |
| **Host MAC Address** | | 00:16:3e:f3:d9:b2 | | | | |
| **Number of connections** | | | 1 | | | |
| **Interesting details (If any)** | | | - | | | |
| **Destination IP Address** | **Destination MAC Address** | | | **Protocol Used** | **Content of communication** | **Suspicious?** |
| 239.255.255.250 | 01:00:5e:7f:ff:fa | | | SSDP | SSDP Notify | No |

Communication without IP address

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source MAC Address** | **Destination MAC Address** | **Protocol Used** | **Contents of message** | **Suspicious?** |
| 00:0d:56:d3:55:17 | Broadcast | ARP |  |  |

1. Hidden actions

**Question**: Was there any suspicious activity? If so, what was the source and what did it try to do?

**Answer**:

*Example: Yes, it gained access to 192.168.1.1*

*The intruder did:*

* *Host scan: Reconnaissance on the network to search for live hosts.*

*These activities are indicative of lateral movement attempts and reconnaissance.*

1. Trace the communications

**Question**: Were there any Command & Control (C&C) communications? If so, write the details of the communication.

**Answer**:

*Example: There were the HTTP communications with server 8.8.8.8:*

*The intruder did:*

* *HTTP Request*
  + *Host: www.google.com*
  + *User-Agent: Mozilla/5.0*
  + *Accept: text/html*

1. Lateral Movement

*Example: There were the SCP communications with server 19.16.1.45:*

*The intruder did:*

* *HTTP Request*
  + *Host: 19.16.1.45*
  + *Username: admin*
  + *Password: admin*
  + *Filename: file.ps1*
  + *File data: Random bytes (10 bytes)*
* *This activity shows that the attacker downloaded a file onto the target system to laterally access the private network*

1. Security issues

**Question**: Are there any potential security issues? Explain your answer.

**Answer**:

*Example: These are suspicious activities by host 192.168.1.1*

* *Host scan*
  + *These scans should not be occouring on a secure network*