**Lab 5 Malware Traffic Analysis using Wireshark**

**1. Goal**

In this lab, students learn three important skills in malware traffic analysis

(1) Display filter expressions

(2) Identify hosts and users

(3) Exporting Objects from Pcap files

Please answer all questions and attach required screenshots, then submit this lab report to D2L.

**2. Display filter expressions**

Step 1: Basic display filter expressions

Wireshark’s display filter bar locates right above the column display section. This is where you type expressions to filter the frames, IP packets, or TCP segments that Wireshark displays from a pcap file. When you type anything in the display filter, Wireshark offers a list of suggestions based on the text you have typed. Three status of the display bar: (a) red: expression not yet accepted; (b) yellow: the expression has been accepted, but it will probably not work as intended; (c) green, the expression has been accepted and should work properly.

Two common ways to filter traffic:

(1) protocols: just typing in the protocol you want to filter. If you type a dot, “.”, after the protocol name, it will provide the list with all actions on this specific protocol.

Graphical user interface, table

Description automatically generated

(2) addresses: “ip.addr==192.168.0.1”, “tcp.port==80”, “udp.port==24”, “eth.addr==ff:ff:ff:ff:ff:ff”, “wlan.add==ff:ff:ff:ff:ff:ff”

In addition, Wireshark’s display filter uses Boolean expression, so you can specify values and chain them together.

(1) equals: == or eq

(2) and: && or and

(3) or: || or or

(4) not: !

(5) contain: contains

What is the filter expression for a ftp request and ip address is 192.168.3.10?

**ftp && ip.addr==192.168.3.10**

What is the filter expression for http request or http response?

**tcp.port==80**

What is the filter expression for dns qurry name that contains apple?

**dns.qury.name contains “apple”**

Step 2: Filters for Web-Based infection Traffic

A web traffic always starts from a client initiate a request to the server (http request or the client says hello to the server). Therefore, a filter expression “http.request or tls.handshake.type == 1” could be applied to follow the flow of web traffic. HTTPS today uses Transport Layer Security (TLS) protocol to establishes an encrypted connection to an authenticated peer over an untrusted network. Earlier, less secure versions of this protocol were called Secure Sockets Layer or SSL. tls.handshake.type ==1 indicates a client says Hello.

Silently, HTTP request also use UDP port on 1900 for Simple Service Discovery Protocol (SSDP). It is a lightweight protocol that used to discover Plug & Play devices, and not associated with normal web traffic. Therefore, when you focus on HTTP traffic, it is better to filter out SSDP protocol using expression like “!(SSDP)” or “!(udp.port==1900)”.

One of the infection indicators is that one device tries to connect to a server repeatedly. Usually, it is a server that has been taken off-line or is refusing a TCP connection for security measurement. Therefore, if you see many TCP retransmission, it indicates the source device is compromised.

These attempted connections can be reveals by including TCP flag SYN (synchronize) using expressions “tcp.flags==2”. SYN packets are used to initiate a connection. In addition to SYN, there are five more flags in TCP: (1) ACK (acknowledgment): confirm initiation request and tear down requests, as well as the data packets have been received (tcp.flags==16); (2) RST (reset): signify the connection is down or maybe the service is not accepting the request (tcp.flags==4); (3) FIN (finish): both the sender and receiver send the FIN packets to gracefully terminate the connection (tcp.flags==1); (4) PSH (push): indicates that the incoming data should be passed on directly to the application instead of getting buffered (tcp.flags==8); (5) URG (urgent): indicate that the data that the packet is carrying should be processed immediately by the TCP stack (tcp.flags==32).

Let us analyze a pcap file. Here is your task:

(1) Please go to this webpage: <https://www.malware-traffic-analysis.net/training/display-filter-expressions.html>.

(2) Download the zip file “Using-Wireshark-display-filters-Emotet-with-IcedID.pcap.zip”.

(3) Unzip the folder with password shown on the webpage.

(4) Use proper filter expression to find the IP address of the host that got infected and the IP address of the destination that this terminal wanted to connect to. Please attach the screenshot of the traffic and explain why you think that IP address is compromised.

**I believe this was the host that was infected and the destination it was trying to connect to. Due to the multiple TCP Retransmissins, I believe this why the IP address is compromised.**

A screenshot of a computer

Description automatically generated

**3. Identifying hosts and Users**

Step 3: Host name and MAC address

Any host generating traffic within your network should have three identifiers: a MAC address, an IP address, and a hostname. In most cases, alerts for suspicious activity are based on IP addresses. If you have access to full packet capture of your network traffic, a pcap retrieved on an internal IP address should reveal an associated MAC address and hostname.

Host information can be filtered on two types of activity: DHCP and NBNS. DHCP traffic can help identify hosts for almost any type of computer connected to your network. NBNS traffic is generated primarily by computer running Microsoft Windows or Apple hosts running MacOS to look for a host on the internal network when a host’s IP address cannot be resolved through the organizational DNS server.

Please identify host name and MAC address by using both DHCP and NBNS protocols, and attach screenshots of the host name and MAC address of the compromised IP address that you found in the previous step.

A white background with black and blue text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Hint: MAC address can be found in Ethernet header in both DHCP and NBNS protocols. The host name can be found in the (1) option fields of the DHCP request that initiated by the IP address; (2) additional records of the NBNS registration packet that initiated by the IP address.

Step 4: Operating System

User-agent strings from headers in HTTP traffic can reveal the operating system. If the HTTP traffic is from an Android device, you might also determine the manufacturer and model of the device.

Graphical user interface, text, application, email

Description automatically generated

Please use the filter expression “http.request and !(ssdp)” to filter out the http request. Then, show the TCP stream of the one with destination IP address is 45.40.150.81.

What is the user-agent information?

**User-agent information contains specific information about the device connecting to another.**

A screenshot of a computer

Description automatically generated

Please attach the TCP three-way handshake between 10.12.3.101 and 45.40.150.81.

A screen shot of a computer

Description automatically generated

**4. Export Objects from a Pcap file**

When reviewing packet captures of suspicious activity, security professionals may need to export objects from the pcaps for a closer examination.

Step 5: Export objects from HTTP traffic

Wireshark provides easy way to export objects, such as html page and files that the client downloaded from servers. Please go to “File 🡪 Export Objects 🡪 HTTP”

Graphical user interface, application

Description automatically generated

Then, you will see a object list. The content type is explained in the column “Content Type”. If you download the content from packet 42. You will see a file named “nsci.txt”. Then, you could use a text editor to open it up. For html files, you could download and open it up in a browser.

Graphical user interface, application

Description automatically generated

Please save the file from packet 42 and packet 325. Then attach screenshots of the content for each file.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Step 6: Export objects from SMTP traffic

Export email follow the same procedure as export files from http. The only difference is you need to choose “IMF” as protocol.

Please download “extracting-objects-from-pcap-example-04.pcap” from webpage <https://www.malware-traffic-analysis.net/training/exporting-objects.html> and unzip it using the password on the webpage. Then, download one email, open it in the text editor, and attach a screenshot of the content here.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Reference**

<https://www.howtouselinux.com/post/tcp-flags>

<https://malware-traffic-analysis.net/index.html>