Mini-Project 3 Checkpoint 1

ECE/CS 498DS
Spring 2020

Name1 (NetID1), Name2 (NetID2), Name3 (NetID3)

Task 0

0.6.(a) Which http pcap file represents legitimate activity, and which represents attacker activity?

http.pcap' represents attacker activity, and 'http2.pcap' represents legitimate activity.

0.6.(b) Are there any Content-Type headers in legitimate activity pcap file? If there are, list those Content-Type headers.

Since no packets in http2.pcap has an HTTP layer, we cannot find content-type in http2.pcap.

Task 1 – HTTP Traffic Analysis

- Task 1. 1. a Report the **UNIX timestamp** of the first attempted scan on the vulnerable server

Answer: e UNIX timestamp of the first attempted scan on the vulnerable server is 2018-03-18 12:41:43.610774

- Task 1. 1.b What is the **IP address** of the vulnerable server?

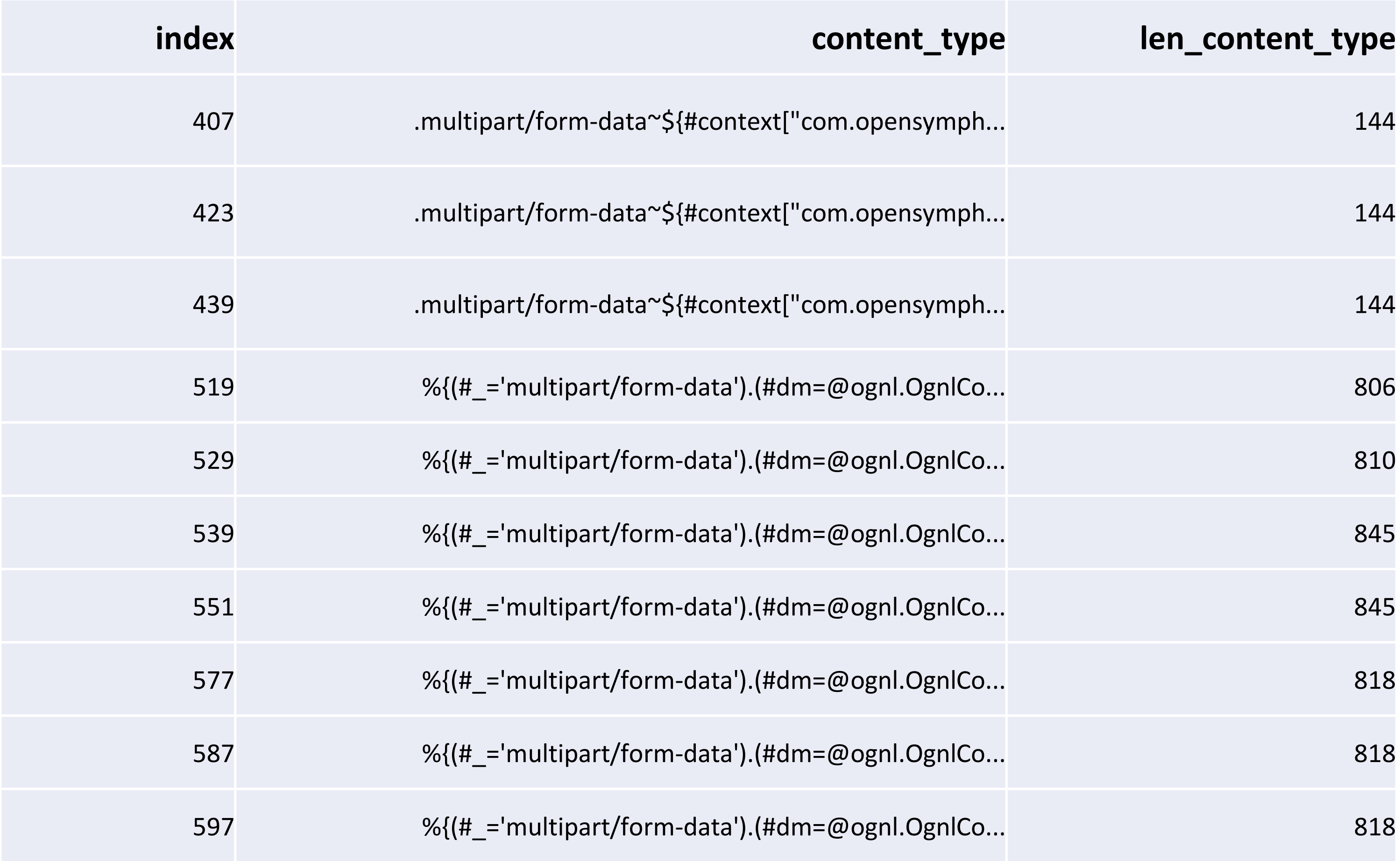
Answer: The IP address of the vulnerable server is 172.17.0.2

- Task 1. 1.c What is the **port** of the vulnerable server?

Answer: The port of the vulnerable server is 8080

Task 1 – HTTP Traffic Analysis

- 2.a Provide a list of the Content-Type headers sent to the vulnerable server from the provided HTTP packet capture. For each Content-Type header, provide its length as well.



index	content_type	len_content_type
407	.multipart/form-data~${#context["com.opensymph...	144
423	.multipart/form-data~${#context["com.opensymph...	144
439	.multipart/form-data~${#context["com.opensymph...	144
519	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	806
529	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	810
539	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	845
551	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	845
577	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	818
587	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	818
597	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	818

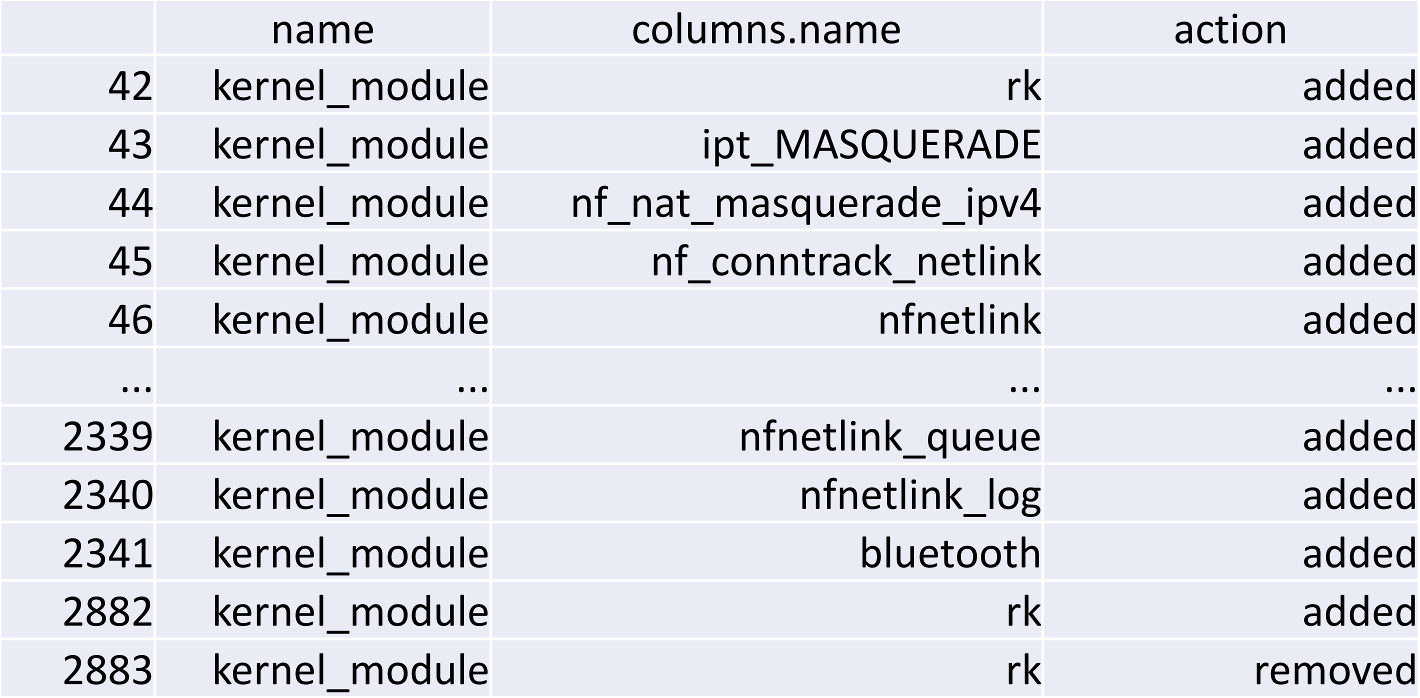
Task 1 – HTTP Traffic Analysis

- 2.b Fill in the blanks in the table below

Command Name	Present in the attack?	Interpretation of the command
whoami	*Yes*	*Displays the name of the current user*
wget	Yes	*Retrieves content from web servers*
ls	Yes	*Lists computer files in Unix and Unix-like operating systems*
cat	No	
cd	No	
insmod	Yes	*Loads the specified kernel modules into the kernel*
ssh	No	
lsmod	No	

Task 1 – Host Logs Analysis

1.a Provide a list of kernel modules added or removed from the system: (Output table from code)



	name	columns.name	action
42	kernel_module	rk	added
43	kernel_module	ipt_MASQUERADE	added
44	kernel_module	nf_nat_masquerade_ipv4	added
45	kernel_module	nf_conntrack_netlink	added
46	kernel_module	nfnetlink	added
...	...	...	...
2339	kernel_module	nfnetlink_queue	added
2340	kernel_module	nfnetlink_log	added
2341	kernel_module	bluetooth	added
2882	kernel_module	rk	added
2883	kernel_module	rk	removed

1.b What is the attacker-controlled kernel module?

The attacker-controlled module is rk.ko.

Task 1 – Host Logs Analysis

1.c How did you verify that the module was loaded onto the server?
Answer: "The module was loaded onto the server because the following command is run:"
#cmd=‘insmod rk.ko.1’

Also, from df_oslogs, we identify the following items:

	name	columns.name	action	calendarTime
42	kernel_module	rk	added	Tue Feb 6 00:34:09 2018 UTC
113	kernel_module	rk	removed	Tue Feb 6 00:34:50 2018 UTC
2882	kernel_module	rk	added	Mon Mar 19 15:58:54 2018 UTC
2883	kernel_module	rk	removed	Mon Mar 19 15:58:58 2018 UTC

Task 1 – Host Logs Analysis

2. What is the **file name** that contains the internal hostnames?

The file name that contains the internal hostnames is 'known_hosts”.

Task 1 – Host Logs Analysis

3. Do you observe any evidence that the attacker extracted the internal host names via HTTP in the logs?
(If yes, report the log line. If not, briefly explain why not.)

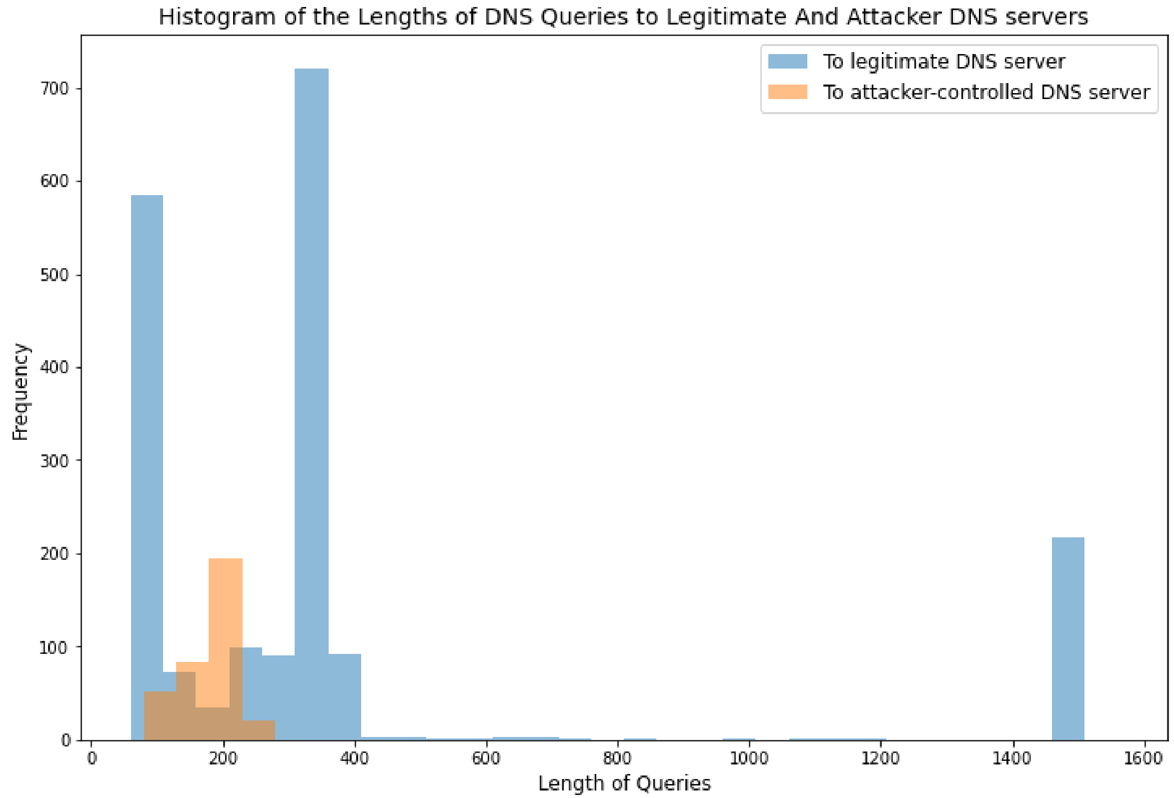
From the HTTP content type headers, we have found nothing related to the internal hostname file.
Therefore, we conclude that the attacker is not using HTTP to access the file.

Task 1 – DNS Traffic Analysis

1(a) Provide the IP address of the attacker-controlled DNS server:
Answer: From the content type headers, we find the IP address '162.212.156.148' following wget. Therefore, the attacker-controlled server is 162.212.156.148.

1(b) Provide the IP address of the legitimate DNS server:
Answer: We can identify the legitimate server by finding the source IP when destination IP is the bad server. The legitimate server is 10.0.2.15.

2. Histogram of the length of DNS queries:


Histogram of the Lengths of DNS Queries to Legitimate And Attacker DNS servers
To legitimate DNS server
To attacker-controlled DNS server
Frequency
Length of Queries