



Day 5

ZROC102

Module 2: Endpoint Security



LETSDEFEND Platform



Endpoint Security

This is the Endpoint Security Section that displays all endpoint devices in the network, to collect detailed information, isolate the compromised device(s) in order to prevent malicious software.

EndpointManagement

Freemium

Search anything...

JackRamsey
172.16.17.23

Katie
172.16.17.35

SusieHost
172.16.17.5

MarkPRD
172.16.17.88

MikeComputer
172.16.17.14

MarksPhone
10.15.15.12

KatharinePRD
172.16.15.78

#37

HOSTNAME	IP ADDRESS	OS	CLIENT / SERVER	REQUEST CONTAINMENT
JackRamsey	172.16.17.23	Windows Server 2019	Client	<input checked="" type="checkbox"/>

General Info:

Bit Level: 64 Bit

Domain : LetsDefend

Primary User: Jack

Last Login: Sep, 13, 2021, 10:32 PM

Details

Browser History

Command History

Network Connections

Process List

Action

Connect

Endpoint Security

Details of the endpoint devices can be analyzed by clicking on them. In this example, the “**Browser History**” was clicked to view web pages the user visited.

The screenshot displays a web-based interface for endpoint security management. On the left, a 'General Info' panel lists device details: Bit Level (64 Bit), Domain (LetsDefend), Primary User (Jack), and Last Login (Sep, 13, 2021, 10:32 PM). The main area is titled 'Details' and contains a sidebar with navigation options: Browser History (highlighted with a red box and a red circle labeled '1'), Command History, Network Connections, and Processes. A 'Browser History' window (highlighted with a red box and a red circle labeled '2') is open, showing a list of visited URLs with timestamps. The URLs include a Google search for 'pandas', a Google Docs spreadsheet, a Gmail email, and a Google search for 'dmoz+dataset'. The interface also shows a 'HOSTS' table with columns for IP, Hostname, and Client/Server status, and a 'Genera' section at the bottom.

General Info:	Details
Bit Level: 64 Bit	Browser History (1)
Domain : LetsDefend	> Command History
Primary User: Jack	Network Connections
Last Login: Sep, 13, 2021, 10:32 PM	Processes

Browser History (2)	
13.05.2021 21:10:	https://www.google.com/search/client=firefox-b-a&b&biw=1366&bih=654&ei=w7usWuPnBYjN0gSBzYqwCA&q=pandas+str.split%28%29&oq=pandas+str.split%28%29&gs_l=psy-ab.4...24330.27765.0.28165.12.11.0.0.0.356.356.3-1.1.0....0...1c.1.64.psy-ab..11.1.355...0.0.dVQ_NVwZOHQ
23.05.2021 14:10:	https://docs.google.com/spreadsheets/d/1xXwarcQZAHluorveZsACtXRdmNFbwGtN3VMNhcTdEyQ/editgid=0
29.05.2021 13:51:	https://mail.google.com/mail/u/0/h/1d64alfbg1g9w//zy=e&f=1
08.05.2021 18:46:	https://doc-0s-4k-docs.googleusercontent.com/docs/securesc/t083m4guvvg402isi4ctvv572ualr0u3c/i2lbtldagmkfd972gr9shrtlr0cqeuh7/1521460800000/11343036508320484936/00337561621857813616/1XrW7Kn_P5fjuUmTqu1dNrr0XR_NCHMa3/e=download&nonce=qgj1umq9ogfbc&user=00337561621857813616&hash=c9ru326qobtuhpdpk6595f2t0d9a8r6h
08.05.2021 12:39:	https://www.google.com/search/q=dmoz+dataset&ie=utf-8&oe=utf-8&client=firefox-b-ab

HOSTS	CLIENT / SERVER
JackRa	Client

Endpoint Security

Similarly, as done via the previous page, you can view command history by clicking on the hyperlink names – Command History, Network Connections and Process List.

Details

🔍 Browser History

>_ Command History

1

🔗 Network
Connections


2

⚙️ Process List

3

Endpoint Security

To disconnect a device from the network, if you are certain the device has been compromised, please click the **“Request Containment”** button.

OS	CLIENT / SERVER	REQUEST CONTAINMENT
Windows Server 2019	Client	

Source

- <https://app.letsdefend.io/endpoint/>
- <https://app.letsdefend.io/tutorial/videos/>