



# Adversary Simulation with MITRE CALDERA

Märko Sokser, Luka  
Kukec, Luka Šulentić,  
Luka Hrupec

# Sadržaj

01

Infrastrukturni Inženjer

Kreiranje entraprise  
okruženja za projekt

02

Blue team inžinjer

Implementacija sustava za  
nadzor i detekciju napada

03

Red Team inženjer

Kreiranje napada na  
entraprise okruženje za  
projekt

04

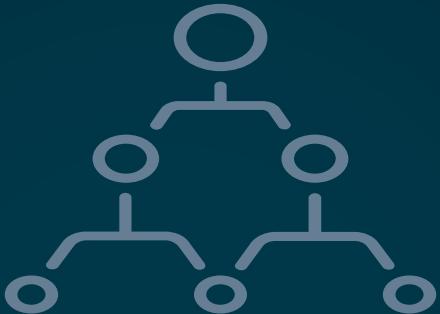
Threat hunter/Analitičar

Analiza ponašanje napada kroz sve faze  
te procijeniti učinkovitost detekcije i obrane



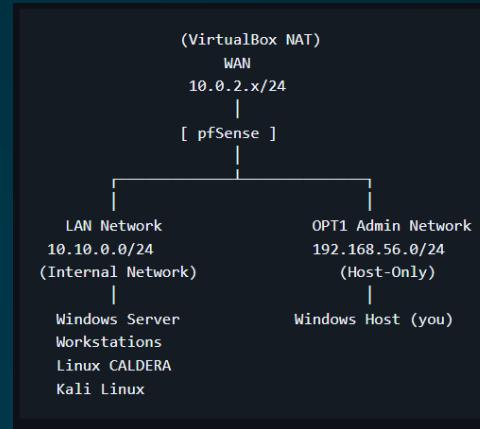
01

Infrastrukturni Inženjer



# Misija

- 6 međusobno povezanih virtualnih strojeva
- -Realistična enterprise mreža (TechNovaNet 10.10.0.0/24)
- Namjerno ranjiva za Red Team
- U potpunosti nadzirana za Blue Team



# Mrežna osnova - pfSense

The screenshot shows the pfSense Community Edition web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area has two tabs: "System Information" and "Netgate Services And Support".

**System Information**

Name	pfSense.technova.lab
User	admin@192.168.56.1 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 95e4297316df2450370f
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT  The system is on the latest version. Version information updated at Sun Nov 30 13:14:29 CET 2025
CPU Type	11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 06 Minutes 08 Seconds
Current date/time	Sun Nov 30 13:19:41 CET 2025

**Netgate Services And Support**

Contract type: Community Support  
Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your [Netgate Device ID \(NDI\)](#) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

# Active Directory okruženje

- Windows Server 2019 Core Controller
- TechNovaNet domena
- Integrirane DNS usluge
- Ranjivi korisnik employee (sl)
- Windows PowerShell

```
C:\Users\vboxuser>ipconfig/all

Windows IP Configuration

Host Name . . . . . : DC-SERVER
Pr[  
No PS C:\Users\vboxuser> Get-ADUser -Filter * | Select SamAccountName  
IP SamAccountName  
WI  
DN  
Ether Administrator  
Guest  
vboxuser  
Co krbtgt  
De admin  
Ph admin_lab  
DH read_team  
Au blue_team  
Li  
IPv4 Address. . . . . : 10.10.0.10(Preferred)
Set-ADAccountPassword -Identity employee -Reset
    -NewPassword (ConvertTo-SecureString "employee123" -AsPlainText -Force)

DNS Servers . . . . . : ::1
                           10.10.0.10
NetBIOS over Tcpip. . . . . : Enabled
```

# Ranjivi Linux server

- Ubuntu 24.04 LTS (10.10.0.51)
- Ranjivi korisnik: webadmin/Webadmin123!
- sudo NOPASSWD:ALL pogrešna konfiguracija
- Apache web server na portu 80
- SSH pristup omogućen sa password autentifikacijom

```
vbubuntu@ubuntu-srv:~$ grep webadmin /etc/passwd
webadmin:x:1001:1001:,:/home/webadmin:/bin/bash
vbubuntu@ubuntu-srv:~$ groups webadmin
webadmin : webadmin sudo users
vbubuntu@ubuntu-srv:~$ id webadmin
uid=1001(webadmin) gid=1001(webadmin) groups=1001(webadmin),27(sudo),100(users)
vbubuntu@ubuntu-srv:~$
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

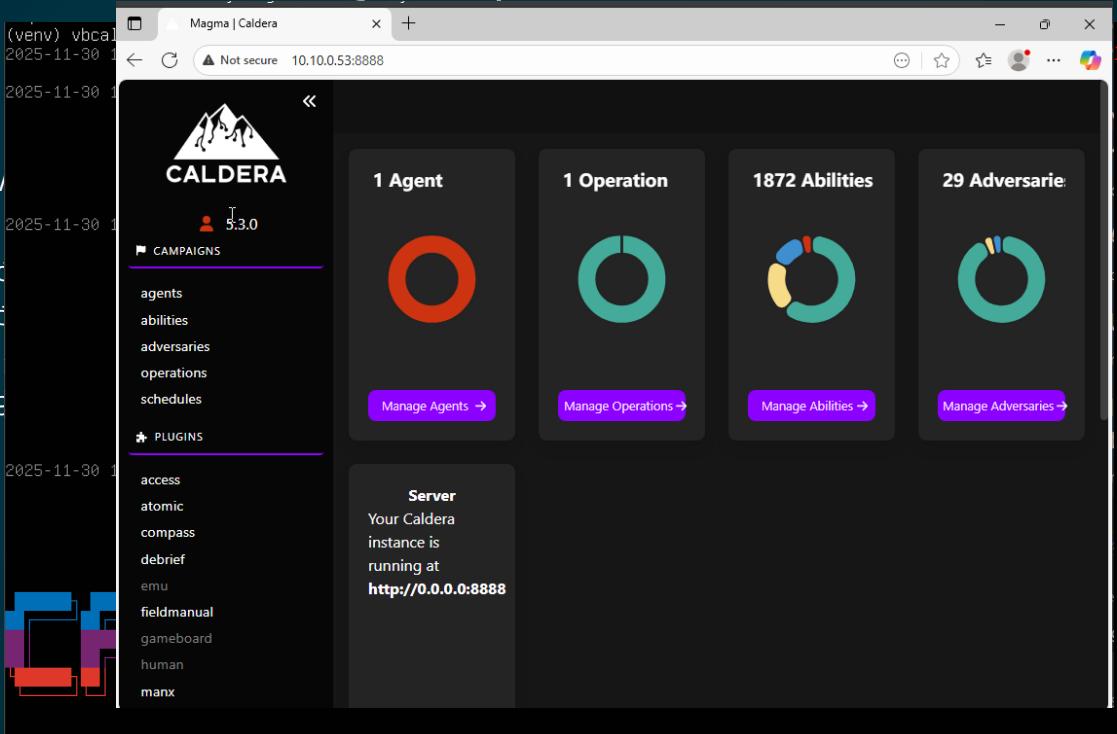
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:
@include /etc/sudoers.d

webadmin ALL=(ALL) NOPASSWD:ALL
```

# Automatizacija napada - CALDERA

- MITRE Campaigns
- Platforma za upravljanje protivnikom
- Sandcat agent



to failed imports  
more functional

# Sigurnosni nadzor - Wazuh SIEM

- Mini-Wazuh SIEM (10.10.0.70) - optimiziran

```
vbubuntu@ubuntu-srv:~$ sudo systemctl daemon-reload
vbubuntu@ubuntu-srv:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
vbubuntu@ubuntu-srv:~$ sudo systemctl start wazuh-agent
vbubuntu@ubuntu-srv:~$ systemctl status wazuh-agent
● wazuh-agent.service - Wazuh
   Loaded: loaded (/usr/lib/
   Active: active (running)
     Process: 1172 ExecStart=/...
      Tasks: 34 (limit: 2267)
     Memory: 425.0M (peak: 426...
        CPU: 4.272s
       CGroup: /system.slice/wazuh-agent
           ├─1204 /var/ossec/bin/wazuh-control
           ├─1212 /var/ossec/bin/wazuh-logcollector
           ├─1226 /var/ossec/bin/wazuh-modulesd
           ├─1236 /var/ossec/bin/wazuh-remoted
           ├─1253 /var/ossec/bin/wazuh-syscheckd
           ├─1447 sh -c -- "/bin/ps -p 235 > /dev/null 2>&1"
           └─1448 /bin/ps -p 235
vbubuntu@ubuntu-srv:~$
```

```
^Cvbwazuh@WAZUH-SIEM:~$ sudo /var/ossec/bin/wazuh-control status
wazuh-clusterd not running...
wazuh-modulesd is running...
wazuh-monitord is running...
wazuh-logcollector is running...
wazuh-remoted is running...
wazuh-syscheckd is running...
wazuh-analusisd is running...
```

```
Wazuh agent_control. List of available agents:
  ID: 000, Name: WAZUH-SIEM (server), IP: 127.0.0.1, Active/Local
  ID: 004, Name: WIN10, IP: any, Active
  ID: 005, Name: ubuntu-srv, IP: any, Active
```

List of agentless devices:

Status	Name	DisplayName
Running	WazuhSvc	Wazuh

# Tailscale VPN

MACHINE	ADDRESSES ⓘ	VERSION	LAST SEEN	
caldera-srv	100.118.97.74 ⓘ	1.90.9 Linux 6.8.0-88-generic	● 11:34 AM SSH... Share... ⋮	
dc-server	100.67.42.81 ⓘ	1.90.9 Windows Server 2019	● 2:23 PM GMT+1 ⋮	
desktop-lbf7a9d	100.73.38.37 ⓘ	1.90.9 Windows 10 21H2	● 1:00 PM GMT+1 ⋮	
pfsense	100.108.74.68 ⓘ	1.54.0 FreeBSD 14.0-CURRENT	● 1:29 PM GMT+1 ⋮	
ubuntu-srv	100.106.9.109 ⓘ	1.90.9 Linux 6.8.0-88-generic	● 11:34 AM GMT+1 ⋮	
wazuh-siem	100.67.231.16 ⓘ	1.90.9 Linux 6.8.0-71-generic	● 11:34 AM GMT+1 ⋮	

02

Blue team Inženjer



# Sigurnosni Nadzor i Instrumentacija (Blue Team)

**Cilj:** Uspostava proaktivnog nadzora nad infrastrukturom.

**Fokus:** Praćenje procesa, mrežne aktivnosti i integriteta sustava.

**Pristup:** Osiguravanje potpune vidljivosti svih kritičnih točaka u realnom vremenu.

## Remote Logging Options

### Enable Remote Logging

Send log messages to remote syslog server

#### Source Address

Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

#### IP Protocol

IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

#### Remote log servers

10.10.0.70:514

IP[:port]

IP[:port]

#### Remote Syslog Contents

- Everything
- System Events
- Firewall Events
- DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- General Authentication Events
- Captive Portal Events
- VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- Gateway Monitor Events
- Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- Network Time Protocol Events (NTP Daemon, NTP Client)
- Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

 Save

```
PS C:\Sysmon> Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 3 | Format-List TimeCreated, Id, Message
```

```
TimeCreated : 12/5/2025 1:12:47 PM
Id          : 22
Message     : Dns query:
               RuleName: -
               UtcTime: 2025-12-05 12:12:46.514
               ProcessGuid: {f00ahfc1-cah5-6932-c702-000000001600}
```

```
vbwazuh@WAZUH-SIEM:~$ sudo tail -20 /var/ossec/logs/alerts/alerts.log
```

```
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
```

```
User: root
```

```
2025-12-05T12:47:37.813547+00:00 ubuntu-srv sudo: vbubuntu : TTY=pts/0 ; PWD=/home/vbubuntu ; USER=root ; COMMAND=/usr/bin/rm /etc/cron.d/test_fim
```

```
tty: pts/0
```

```
pwd: /home/vbubuntu
```

```
command: /usr/bin/rm /etc/cron.d/test_fim
```

```
** Alert 1764938857.1538596: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.31 2.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
```

```
2025 Dec 05 12:47:37 (ubuntu-srv) any->/var/log/auth.log
```

```
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
```

```
User: root
```

```
2025-12-05T12:47:37.814193+00:00 ubuntu-srv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by vbubuntu(uid =1000)
```

```
uid: 1000
```

```
** Alert 1764938857.1539055: - pam,syslog,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,n ist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
```

```
2025 Dec 05 12:47:37 (ubuntu-srv) any->/var/log/auth.log
```

```
Rule: 5502 (level 3) -> 'PAM: Login session closed.'
```

```
User: root
```

```
2025-12-05T12:47:37.816433+00:00 ubuntu-srv sudo: pam_unix(sudo:session): session closed for user root
```

```
vbwazuh@WAZUH-SIEM:~$
```

```
QueryName: signaler-pa.clients6.google.com
QueryStatus: 0
QueryResults: ::ffff:142.251.38.202;
Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
User: TECHNOVA\blue_team
```

```
PS C:\Sysmon>
```

Tailscale - SSH to wazuh-siem — Mozilla Firefox

① about:blank

RuleName: -  
UtcTime: 2025-12-05 12:46:00.258

```
vbwazuh@WAZUH-SIEM:~$ sudo tail -20 /var/ossec/logs/alerts/alerts.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
User: root
2025-12-05T12:47:37.813547+00:00 ubuntu-srv sudo: vbubuntu : TTY=pts/0 ; PWD=/home/vbubuntu ; USER=root ; COMMAND=/usr/bin/rm
/etc/cron.d/test_fim
tty: pts/0
pwd: /home/vbubuntu
command: /usr/bin/rm /etc/cron.d/test_fim

** Alert 1764938857.1538596: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.31
2.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Dec 05 12:47:37 (ubuntu-srv) any->/var/log/auth.log
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: root
2025-12-05T12:47:37.814193+00:00 ubuntu-srv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by vbubuntu(uid=1000)
uid: 1000

** Alert 1764938857.1539055: - pam,syslog,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,n
ist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Dec 05 12:47:37 (ubuntu-srv) any->/var/log/auth.log
Rule: 5502 (level 3) -> 'PAM: Login session closed.'
User: root
2025-12-05T12:47:37.816433+00:00 ubuntu-srv sudo: pam_unix(sudo:session): session closed for user root

vbwazuh@WAZUH-SIEM:~$
```

<de: 088B0,IMPHASH=272245B2988E1E430500B852C4FB5E18  
</des: win.eventdata.parentProcessGuid: {002abfc1-d3de-6932-2d04-000000001600}  
<mi: win.eventdata.parentProcessId: 3376  
<mi: win.eventdata.parentImage: C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe  
<mi: win.eventdata.parentCommandLine: \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"  
<gr: win.eventdata.parentUser: TECHNOVA\\admin\_lab  
</rule: ^C

vbwazuh@WAZUH-SIEM:~\$

SSH Handshake  
Privileged Network  
Microservices

### Edit Firewall Rule

Action: Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

```
PS C:\Windows\system32> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
PS C:\Windows\system32> Get-NetFirewallProfile | Select-Object Name, Enabled
Name      Enabled
----      -----
Domain    True
Private   True
Public    True
```

Windows Defender Firewall with Advanced Security

100.73.38.37

File Action View Help

Back Forward Home Search Filter

Windows Defender Firewall with Advanced Security

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

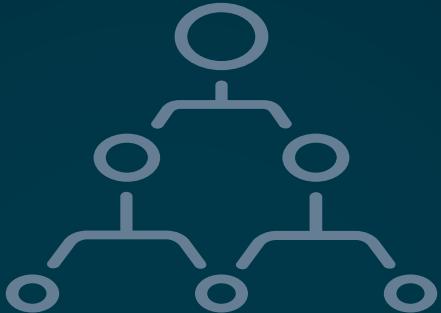
### Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address
Allow RDP 3389 over Tailscale		All	Yes	Allow	No	Any	Any	Any
Allow RDP 3389 TS		All	Yes	Allow	No	Any	Any	Any
Block CALDERA Attacker Inbound		All	Yes	Block	No	Any	Any	10.10.0.53
Block RPC from Ubuntu Server		All	Yes	Block	No	Any	Any	10.10.0.51
Block SMB from Ubuntu Server		All	Yes	Block	No	Any	Any	10.10.0.51
Block WMI from External		All	Yes	Block	No	Any	Any	10.10.0.51, 10.10...

The firewall has limited logging space. Consider enabling logging for everything using a log file, consider using a central syslog server (see the Status: System Logs: Settings page).

03

Red Team Inženjer



# Red Team: Strategija Napada

- **Cilj:** Simulacija APT napada (Advanced Persistent Threat).
- **Alati:** MITRE CALDERA (Sandcat Agents) + Impacket (Python scripts).
- **Lanac Napada (Kill Chain):**
  1. **Initial Access (T1078):** Compromised Credentials (SSH).
  2. **Persistence (T1053):** Cron Jobs / Systemd Services.
  3. **Lateral Movement (T1021.002):** SMB/PsExec (Linux → Windows).
  4. **Exfiltration (T1041):** HTTP POST (Data Theft).

# Red Team: Strategija Napada



# Faza 1: Uspješna Eksplotacija

- Status:  **POTPUNI USPJEH**
- Ključni Vektori Napada:
  1. **SSH Proboj / Slaba Lozinka** (webadmin).
  2. **Eskalacija Privilegija**: sudo NOPASSWD exploit (Shadow file dump).
  3. **Lateralno Kretanje**: Pronađene hardkodirane Admin vjerodajnice u /tmp.
  4. **Rezultat**: Kompromitiran Domain Admin i instaliran agent na Windowsima.

# Faza 1: Dokaz Uspjeha

Project\_Demo\_Run [Download Graph SVG](#)

running

+ Manual Command + Potential Link Operation Details ▾ Filters

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
12/21/2025, 3:31:39 PM GMT+1	success	Identify active user	discovery	xframo	ubuntu-srv	1277	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:32:24 PM GMT+1	success	Simple File Discovery	discovery	xframo	ubuntu-srv	1286	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:33:09 PM GMT+1	success	Port Scan Target	discovery	xframo	ubuntu-srv	1288	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:33:49 PM GMT+1	failed	Lateral Movement Attempt - Standard User	lateral-movement	xframo	ubuntu-srv	1295	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:34:54 PM GMT+1	success	Credential Hunting in Config Files	credential-access	xframo	ubuntu-srv	1315	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:35:54 PM GMT+1	timeout	Lateral Movement - Admin Compromise	lateral-movement	xframo	ubuntu-srv	1322	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:37:34 PM GMT+1	success	Identify active user	discovery	itlfsp	DESKTOP-LBF7A9D	184	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:38:09 PM GMT+1	success	System Information Discovery	discovery	itlfsp	DESKTOP-LBF7A9D	8144	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:39:04 PM GMT+1	success	Security Software Discovery - AV Discovery via WMI	discovery	itlfsp	DESKTOP-LBF7A9D	8380	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:39:49 PM GMT+1	failed	Account Discovery (all)	discovery	itlfsp	DESKTOP-LBF7A9D	6932	<a href="#">View Command</a>	<a href="#">View Output</a> C
12/21/2025, 3:40:24 PM GMT+1	success	Custom Exfiltration (Generate & Steal)	exfiltration	itlfsp	DESKTOP-LBF7A9D	10828	<a href="#">View Command</a>	<a href="#">View Output</a> C

Obfuscator: plain-text  Autonomous

# Faza 2: Potvrda Zaštite

- **Status:** 🛡️ **NAPAD BLOKIRAN**
- **Rezultati Validacije :**
  1. **Eskalacija Privilegija:** 🚫 FAILED (Sudo password required).
  2. **Krađa Vjerodajnica:** 🚫 FAILED (File removed).
  3. **Lateralno Krećanje:** 🚫 FAILED (Network Timeout / Firewall Block).
- **Zaključak:** Attack chain broken at Network & Host level.

# Faza 2: Potvrda Zaštite

Phase2\_Webadmin\_Verify [Download Graph SVG](#)

+ Manual Command + Potential Link Operation Details Filters

running

Obfuscator: plain-text  Autonomous

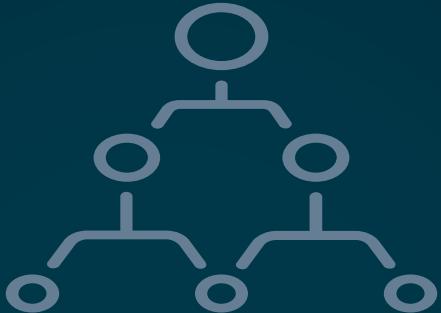
Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
1/2/2026, 5:34:15 PM GMT+1	success	Automated SSH Noise Generator	credential-access	pbojns	ubuntu-srv	3525	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:34:55 PM GMT+1	success	Identify active user	discovery	pbojns	ubuntu-srv	3539	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:35:45 PM GMT+1	timeout	Dump Shadow File (Sudo)	credential-access	pbojns	ubuntu-srv	3547	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:37:25 PM GMT+1	timeout	Noisy Service Creation	persistence	pbojns	ubuntu-srv	3558	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:39:11 PM GMT+1	failed	Simple File Discovery	discovery	pbojns	ubuntu-srv	3564	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:39:41 PM GMT+1	failed	Port Scan Target	discovery	pbojns	ubuntu-srv	3583	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:40:41 PM GMT+1	failed	Lateral Movement Attempt - Standard User	lateral-movement	pbojns	ubuntu-srv	3590	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:41:51 PM GMT+1	failed	Credential Hunting in Config Files	credential-access	pbojns	ubuntu-srv	3598	<a href="#">View Command</a>	<a href="#">View Output</a> ↗
1/2/2026, 5:42:26 PM GMT+1	failed	Lateral Movement - Admin Compromise	lateral-movement	pbojns	ubuntu-srv	3604	<a href="#">View Command</a>	<a href="#">View Output</a> ↗

# Zaključak i Nalazi

- **Kritični Rizik:** Ravna mrežna topologija omogućila je brzo širenje napada.
- **Ljudska Pogreška:** Tvrdo kodirane (hardcoded) vjerodajnice uzrokovale su kompromitaciju domene.
- **Alati:** Bilo je potrebno koristiti prilagođene alate (Python/Impacket) kako bi se zaobišla zadana ograničenja.
- **Konačni Status:** Sustav je sada siguran od osnovnih TTP-ova (Tactics, Techniques, and Procedures).

04

Threat hunter/Analitičar



# Cilj i fokus analize

- **Cilj:** Analizirati ponašanje napada kroz sve faze (Baseline → Phase 1 → Phase 2)
- **Fokus:** Korelacija host, mrežnih i SIEM podataka
- **Pristup:** Threat hunting temeljen na stvarnim artefaktima, a ne samo alertima
- **Ishod:** Procjena učinkovitosti detekcije, vidljivosti i hardening mjera

# Baseline kao temelj analize

- **Baseline = referentna točka za threat hunting**
- Definira normalno ponašanje sustava i korisnika
- Omoćuje razlikovanje:
  - legitimne aktivnosti
  - pozadinske buke
  - stvarnih napada
- Ključan za pouzdanu interpretaciju alerta i logova

```
vbwazuh@WAZUH-SIEM:~$ sudo /var/ossec/bin/agent_control -l
```

Wazuh agent\_control. List of available agents:

```
ID: 000, Name: WAZUH-SIEM (server), IP: 127.0.0.1, Active/Local
ID: 004, Name: WIN10, IP: any, Active
ID: 005, Name: ubuntu-srv, IP: any, Active
```

List of agentless devices:

```
vbwazuh@WAZUH-SIEM:~$
```

# Što je definirano kao baseline

- **Linux:** legitimni SSH logini i uobičajeno sudo korištenje
- **Windows:** normalne prijave, procesi i RDP aktivnosti
- **Mreža (pfSense):** očekivani promet (HTTPS, DNS, NTP)
- **SIEM (Wazuh):** logovi sustava bez kritičnih upozorenja

```
2025-12-10T13:34:01.445217+00:00 ubuntu-srv CRON[2136]: pam_unix(cron:session): session closed for user root
2025-12-10T13:34:13.767162+00:00 ubuntu-srv sudo: pam_unix(sudo:auth): authentication failure; logname=vbubuntu uid=1000 euid=0 tty=/dev/pts/0 ruser=vbubuntu rhost= use
r=vbubuntu
2025-12-10T13:35:01.447555+00:00 ubuntu-srv CRON[2141]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-12-10T13:35:01.447769+00:00 ubuntu-srv CRON[2140]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-12-10T13:35:01.450004+00:00 ubuntu-srv CRON[2140]: pam_unix(cron:session): session closed for user root
2025-12-10T13:35:01.450132+00:00 ubuntu-srv CRON[2141]: pam_unix(cron:session): session closed for user root
2025-12-10T13:35:07.897508+00:00 ubuntu-srv sudo: vbubuntu : 3 incorrect password attempts ; TTY=pts/0 ; PWD=/home/vbubuntu ; USER=root ; COMMAND=/usr/bin/tail -n 50 /va
r/log/auth.log
2025-12-10T13:36:01.453896+00:00 ubuntu-srv CRON[2160]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-12-10T13:36:01.456804+00:00 ubuntu-srv CRON[2160]: pam_unix(cron:session): session closed for user root
2025-12-10T13:36:46.806943+00:00 ubuntu-srv sudo: vbubuntu : TTY=pts/0 ; PWD=/home/vbubuntu ; USER=root ; COMMAND=/usr/bin/tail -n 50 /var/log/auth.log
2025-12-10T13:36:46.807788+00:00 ubuntu-srv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by vbubuntu(uid=1000)
vbubuntu@ubuntu-srv:~$
```

```
vbwazuh@WAZUH-SIEM:~$ sudo /var/ossec/bin/wazuh-control status
[sudo] password for vbwazuh:
Sorry, try again.
[sudo] password for vbwazuh:
wazuh-clusterd not running...
wazuh-modulesd is running...
wazuh-monitord is running...
wazuh-logcollector is running...
wazuh-remoted is running...
wazuh-syscheckd is running...
wazuh-analysisd is running...
wazuh-maild not running...
wazuh-execd is running...
wazuh-db is running...
wazuh-authd is running...
wazuh-agentlessd not running...
wazuh-integratord not running...
wazuh-dbd not running...
wazuh-csyslogd not running...
wazuh-apid is running...
vbwazuh@WAZUH-SIEM:~$
```

# Faza 1: Analiza napada

- Pojava **uspješnog SSH pristupa** s neuobičajenoj izvora
- **Sudo eskalacija bez** lozinke (NOPASSWD)
- Pristup osjetljivim datotekama (/etc/shadow)
- Aktivnosti koje odstupaju od definiranog baselinea

```
vbwazuh@WAZUH-SIEM:~$ sudo tail -n 50 /var/ossec/logs/alerts/alerts.log
- Permissions: rw-rw-r--
- Date: Mon Dec 29 16:50:18 2025
- Inode: 262160
- User: webadmin (1001)
- Group: webadmin (1001)
- MD5: 163c10700a3cd320a3394ead17363de
- SHA1: c00707e96b90dd1038e3741fffd99bf3681601af
- SHA256: 10e22a63465adac1e9e7249f0cal808fb27889880170ef02368fec620d1f9973

** Alert 1767028013.42797: - pam,syslog,pci_dss_10.6.1,gpg13_4.3,gdpr_IV_35.7.d,hipaa_164.312.b,nist_800_53.AU.6,tsc_CC7.2,tsc_CCT7.3,2025 Dec 29 17:06:55 WAZUH-SIEM->/var/log/auth.log Rule: 5501 (level 4) => 'PAM misconfiguration.' 2025-12-29T17:06:53.516893+00:00 WAZUH-SIEM login(4614): PAM unable to dlopen(pam_lastlog.so): cannot open shared object file: No such file or directory

** Alert 1767028015.43218: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53.AU.14,nist_800_53.AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CCT7.3,2025 Dec 29 17:06:55 WAZUH-SIEM->/var/log/auth.log Rule: 5501 (level 3) => 'PAM: Login session opened.' User: vbwazuh 2025-12-29T17:06:53.954166+00:00 WAZUH-SIEM login(4614): pam_unix(login:session): session opened for user vbwazuh(uid=1000) by vbwazuh(uid=0) uid: 0

** Alert 1767028015.43679: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53.AU.14,nist_800_53.AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CCT7.3,2025 Dec 29 17:06:55 WAZUH-SIEM->/var/log/auth.log Rule: 5501 (level 3) => 'PAM: Login session opened.' User: vbwazuh 2025-12-29T17:06:53.991511+00:00 WAZUH-SIEM (systemd): pam_unix(systemd-user:session): session opened for user vbwazuh(uid=1000) by vbwazuh(uid=0) uid: 0

** Alert 1767028257.44145: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53.AU.14,nist_800_53.AC.7,tsc_CCT7.3,2025 Dec 29 17:06:55 WAZUH-SIEM->/var/log/auth.log Rule: 5501 (level 3) => 'PAM: Login session opened.' User: vbwazuh 2025-12-29T17:06:53.991511+00:00 WAZUH-SIEM (systemd): pam_unix(systemd-user:session): session opened for user vbwazuh(uid=1000) by vbwazuh(uid=0) uid: 0
```

```
vbubuntu@ubuntu-srv:~$ sudo zgrep "Accepted password" /var/log/auth.log.2.gz
2025-12-17T19:52:47.391890+00:00 ubuntu-srv sshd[1881]: Accepted password for webad
min from 10.10.0.50 port 50213 ssh2
grep: /var/log/auth.log.2.gz: binary file matches
vbubuntu@ubuntu-srv:~$ 
```

# Faza 1: Analiza napada

- Autentifikacija na Windows s Linux kredencijalima
- Višestruki failed logoni → uspješan logon
- Service creation kao persistence indikator
- Korelacija Linux → Windows → SIEM

System Number of events: 2,841				
Filtered: Log: System; Source: ; Event ID: 7045. Number of events: 22				
Level	Date and Time	Source	Event ID	Task Category
Information	12/21/2025 3:36:26 PM	Service Control ...	7045	None
Information	12/21/2025 3:06:34 PM	Service Control ...	7045	None
Information	12/21/2025 2:47:42 PM	Service Control ...	7045	None
Information	12/21/2025 11:45:35 AM	Service Control ...	7045	None
Information	12/20/2025 1:45:46 PM	Service Control ...	7045	None
Information	12/15/2025 10:03:27 PM	Service Control ...	7045	None
Information	12/15/2025 9:53:18 PM	Service Control ...	7045	None

Event 7045, Service Control Manager

General Details

Friendly View  XML View

+ System

- EventData

<b>ServiceName</b>	bQxi
<b>ImagePath</b>	%systemroot%\sAfTvZpk.exe
<b>ServiceType</b>	user mode service
<b>StartType</b>	demand start
<b>AccountName</b>	LocalSystem

# Faza 2: Analiza nakon hardeninga

- Neuspjeli SSH pokušaji prema Linux hostu
- Onemoćena sudo eskalacija privilegija
- Nema pristupa osjetljivim datotekama (/etc/shadow)
- Napad zaustavljen prije lateralnog kretanja

```
vbubuntu@ubuntu-srv:~$ sudo grep "sudo" /var/log/auth.log | grep webadmin | tail -3
0
2026-01-04T18:25:56.618017+00:00 ubuntu-srv sudo: pam_unix(sudo:auth): auth could n
ot identify password for [webadmin]
2026-01-04T18:25:56.618032+00:00 ubuntu-srv sudo: pam_unix(sudo:auth): auth could n
ot identify password for [webadmin]
vbubuntu@ubuntu-srv:~$ █

vbubuntu@ubuntu-srv:~$ sudo grep "Failed password" /var/log/auth.log | grep webadmi
n | tail -20
[sudo] password for vbubuntu:
2026-01-04T18:16:20.251365+00:00 ubuntu-srv sshd[2895]: Failed password for webadmi
n from 127.0.0.1 port 51472 ssh2
vbubuntu@ubuntu-srv:~$ █
```

# Usporedba faza 1 i 2

Sigurnosni element	Faza 1	Faza 2
SSH pristup	Uspješan	Neuspješan
Privilege escalation	Dozvoljena	Blokirana
Pristup /etc/shadow	Ostvaren	Onemogućen
Lateral movement	Uspješan	Nije moguć
Windows kompromizacija	Da	Ne
Persistence	Uspostavljena	Spriječena

# Zaključak

- Baseline je omogućio pouzdanu analizu i usporedbu
- Faza 1 je potvrdila realnu izloženost napadima
- Faza 2 je dokazala učinkovitost hardening mjera
- Napadni putovi su eliminirani, ne samo detektirani
- SIEM je pružio potvrdu, ne lažan osjećaj sigurnosti

Hvala na  
pažnji!

