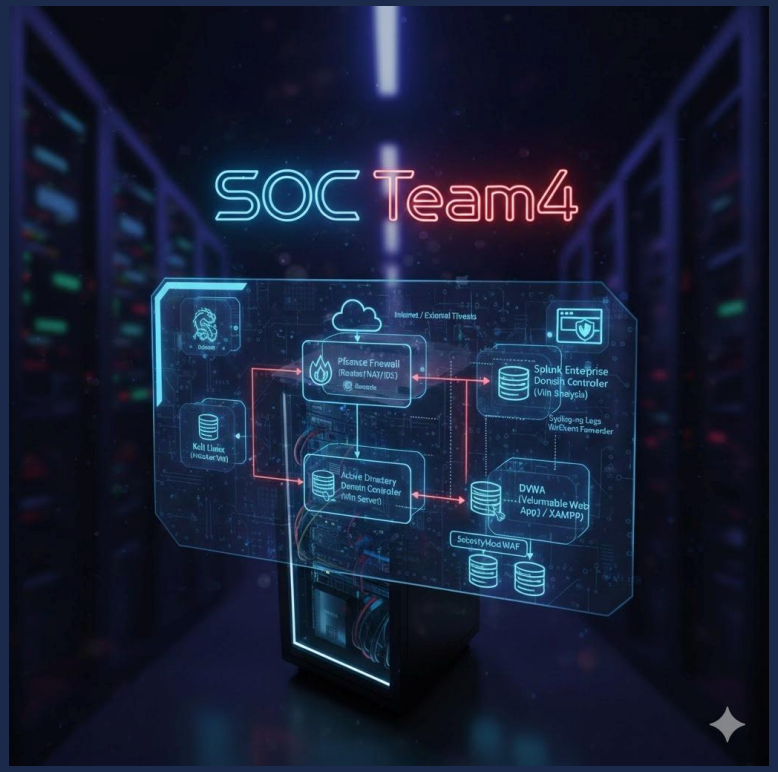
Building & Operating a Mini Security Operations Center (SOC)

SOC Implementation and Threat Detection

Team 4 — DEPI 2026

Release 6 | May 2026



Agenda

1. Project Overview & Objectives
2. Lab Architecture & Network Topology
3. VM Inventory & Infrastructure
4. Detection & Monitoring Stack
5. Project Timeline & Milestones
6. Team Roles & Task Assignment
7. Use Case 1: Brute Force Attack
8. Use Case 2: SQL Injection
9. Use Case 3: Network Scanning
10. Use Cases 4-5: Lateral Movement & Privilege Escalation
11. Risk Assessment & KPIs
12. Testing & Quality Assurance
13. Findings & Recommendations
14. Q&A / Live Demo

Project Overview & Objectives

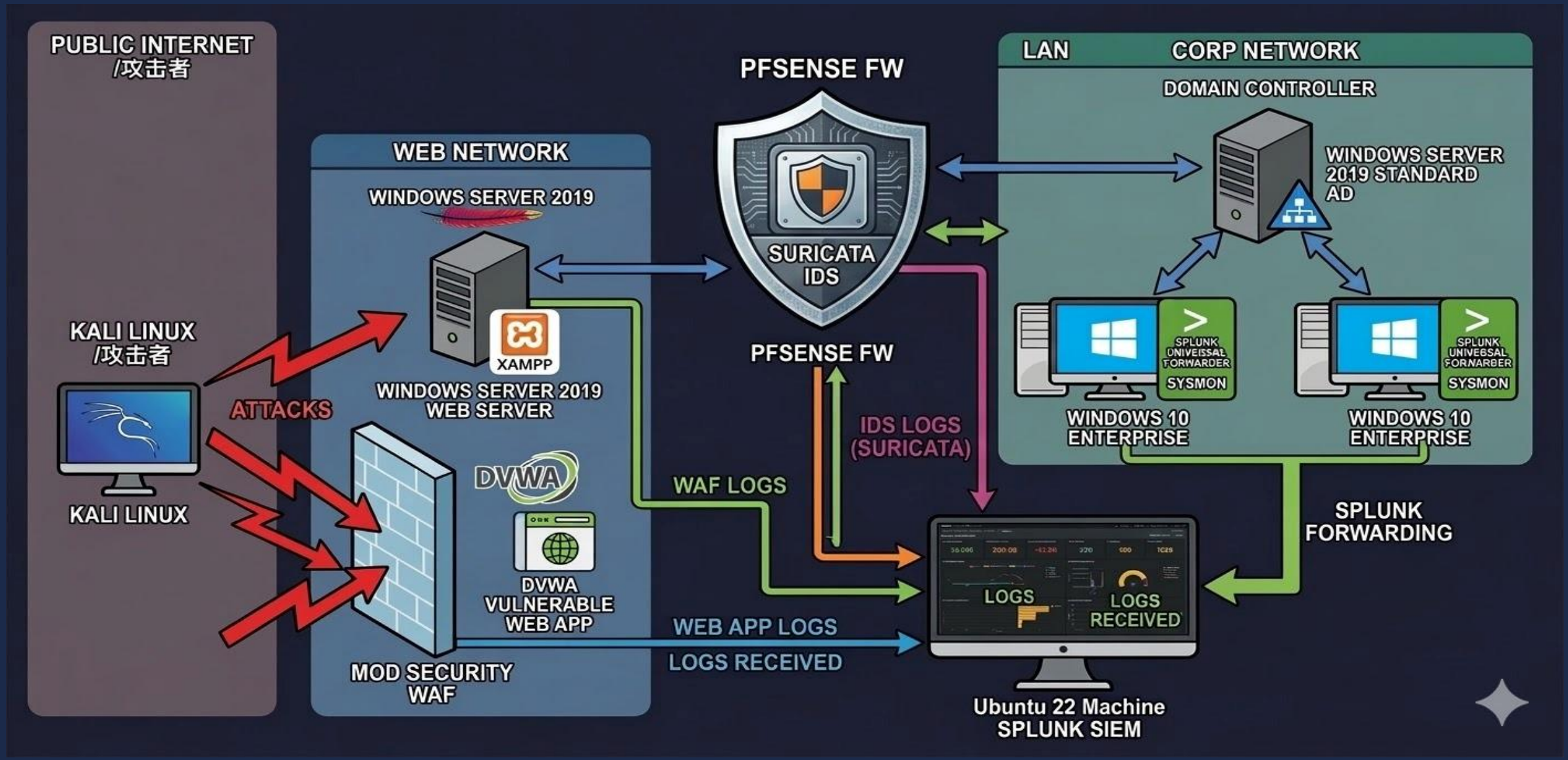
OVERVIEW:
This project designs, implements, and operates a Mini SOC in a virtualized lab environment simulating a corporate network with Active Directory, a web application (DVWA), workstations, pfSense firewall, Suricata IDS, ModSecurity WAF, and centralized Splunk SIEM.

OBJECTIVE 1:
Simulate a full SOC workflow:
Log Ingestion --> Threat Detection --> Triage --> Reporting

OBJECTIVE 2:
Build a functional SOC using enterprise-grade tools:
* Splunk Enterprise (SIEM / monitoring)
* pfSense (firewall / network segmentation)
* Suricata (IDS/IPS on pfSense)
* ModSecurity (Web Application Firewall on XAMPP)
* Sysmon + Universal Forwarders (endpoint visibility)

Attacks are simulated from Kali Linux to validate 5 detection use cases.

Lab Architecture & Network Topology

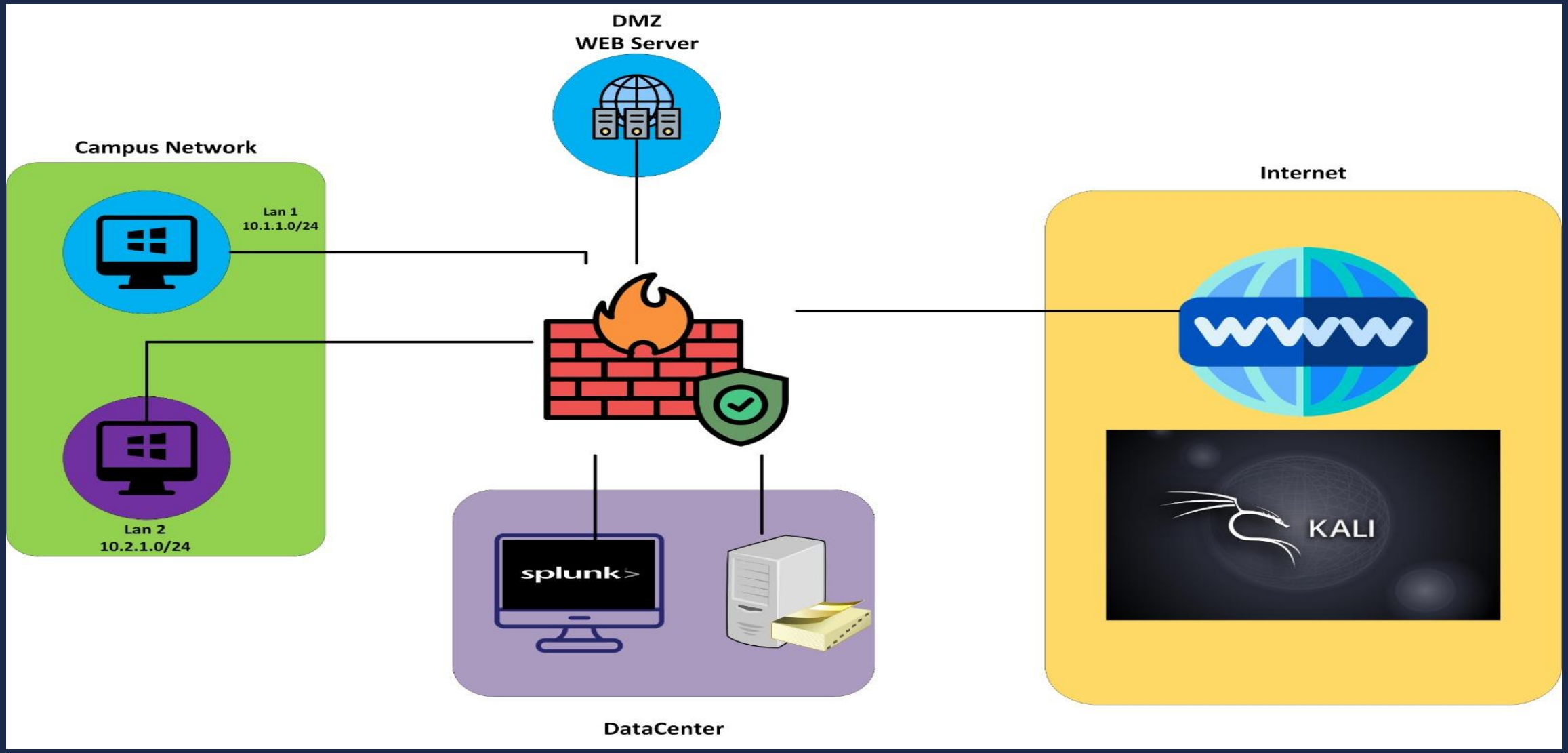


Lab Architecture & Network Topology

```
ARCHITECTURE:
  KALI (Attacker)  ----ATTACKS---->  WEBSRV (DMZ)  ---->  pfSense + Suricata
  192.168.250.128                192.168.120.100      192.168.250.129
                          DVWA + ModSec            |
                          Apache + MariaDB         |
                                        v
                     TEAM4-DC (AD) ........... Ubuntu SPLUNK SIEM
                     192.168.254.140          192.168.254.156
                     TEAM4-PC1 (HR) 10.1.1.100      (All logs here)
                     TEAM4-PC2 (Fin) 10.2.1.100

NETWORK SEGMENTATION (pfSense — 5 Interfaces):
  WAN   192.168.250.0/24  -->  Internet / External Exposure     (VMnet0)
  LAN   192.168.254.0/24  -->  DataCenter / Management          (VMnet1)
  DMZ   192.168.120.0/24  -->  Web Hosting (WEBSRV)             (VMnet2)
  OPT1  10.1.1.0/24       -->  Corporate HR Department          (VMnet3)
  OPT2  10.2.1.0/24       -->  Corporate Finance Department     (VMnet4)
```

Lab Architecture & Network Topology



Infrastructure: VMs & Credentials

Hostname	OS	IP Address	Role	Domain
TEAM4-DC	Win Server 2019	192.168.254.140	Domain Controller (AD/DNS)	SOC.DEPI
WEBSRV	Win Server 2019	192.168.120.100	XAMPP + DVWA + MariaDB	SOC.DEPI
TEAM4-PC1	Win 10 Ent.	10.1.1.100	HR Workstation	SOC.DEPI
TEAM4-PC2	Win 10 Ent.	10.2.1.100	Finance Workstation	SOC.DEPI
pfsense	freebsd:11.2	192.168.254.2 192.168.120.1 10.1.1.1 10.2.1.1 192.168.250.129 192.168.120.1	FW	Non-Domain
UBUNTU	UBUNTU 22.04	192.168.254.156	SPLUNK SIEM	Non-Domain
KALI	Kali 2025.4	192.168.250.128	Attacker (VAPT)	Non-Domain

Detection Stack & Splunk Index Map

Layer	Tool	Source / Index	Purpose
Layer 1	ModSecurity WAF	waf	Detect SQLi, XSS on WEBSRV
Layer 2	Suricata IDS/IPS	suricata	Network intrusion detection on pfSense
Layer 3	pfSense Filterlog	pfsense_fw	Firewall traffic logging (allow/deny)
Layer 4	Apache Access Log	webapp	HTTP request logging on WEBSRV
Layer 5	Sysmon + WinEventLog	windows_dc	DC process/logon/network events
Layer 6	Sysmon (UF)	windows_pc1	HR workstation endpoint telemetry
Layer 7	Sysmon (UF)	windows_pc2	Finance workstation endpoint telemetry
Layer 8	Sysmon (UF)	windows_websrv	Web server host-level events

Timeline, Milestones & Team Assignment

4-WEEK SPRINT:

Week 1 (Mar): Splunk + pfSense + DC setup --> Log pipeline operational
Week 2 (Apr): UF + Sysmon + Suricata + ModSec --> Correlation rules documented
Week 3 (May): SPL rules + Attack simulations --> Triage sheets + IOCs
Week 4 (May): IR Playbook + Report + Demo --> Final submission

MILESTONES:

M1 (Jan 27) Project Proposal
M2 (Mar 1) Literature Review
M3 (Apr 3) System Design
M4 (May 17) Functional SOC
M5 (May 24) Final Report + Presentation

TEAM ASSIGNMENT:

Abdalaziz Mohammad --> AD, Sysmon, GPO, Windows Logging
Ahmed Hamdy --> Splunk Installation
Marko Maged --> pfSense Firewall
Ahmed Atef --> Suricata IDS/IPS
Bassam Alsayed --> XAMPP Web Server + DVWA
Ahmed Tarek --> ModSecurity WAF

Timeline, Milestones & Team Assignment

4-WEEK SPRINT:

Week 1 (Mar): Splunk + pfSense + DC setup --> Log pipeline operational
Week 2 (Apr): UF + Sysmon + Suricata + ModSec --> Correlation rules documented
Week 3 (May): SPL rules + Attack simulations --> Triage sheets + IOCs
Week 4 (May): IR Playbook + Report + Demo --> Final submission

MILESTONES:

M1 (Jan 27) Project Proposal
M2 (Mar 1) Literature Review
M3 (Apr 3) System Design
M4 (May 17) Functional SOC
M5 (May 24) Final Report + Presentation

TEAM ASSIGNMENT:

Abdalaziz Mohammad --> AD, Sysmon, GPO, Windows Logging
Ahmed Hamdy --> Splunk Installation
Marko Maged --> pfSense Firewall
Ahmed Atef --> Suricata IDS/IPS
Bassam Alsayed --> XAMPP Web Server + DVWA
Ahmed Tarek --> ModSecurity WAF

Timeline, Milestones & Team Assignment

Team4 Project Installing Sequence

installing windows server 2019 and AD

installing first windows 10 enterprise machine

installing second windows 10 enterprise machine

install splunk on ubuntu

AD Environment CONFIGURATIONS

installing Splunk Forwarder on THE AD machine

installing Splunk Forwarder on THE First WINDOWS 10 ENTERPRISE machine

installing Splunk Forwarder on THE SECOND WINDOWS 10 ENTERPRISE machine

installing splunk forwarder on windows Server 2019 for XAMP and DVAW machines

Preparing AD machine Before installing Splunk Forwarder

Preparing Splunk machine to receive from Splunk Forwarder

Preparing THE First WINDOWS 10 ENTERPRISE machine before installing Splunk Forwarder

Preparing THE Second WINDOWS 10 ENTERPRISE machine before installing Splunk Forwarder

Preparing windows Server 2019 for XAMP and DVAW machines Before installing splunk forwarder

installing splunk forwarder FOR WEB APP. AND WAF on windows Server 2019 for XAMP and DVAW machines

installing modsecurity WAF on windows Server 2019 for XAMP and DVAW machine

Timeline, Milestones & Team Assignment

- installing kali linux
- installing SYSMON on THE AD machine and configure splunk to receive it
- installing SYSMON on THE FIRST WINDOWS 10 ENTERPRISE machine and configure Splunk to receive from it
- installing SYSMON on THE Second WINDOWS 10 ENTERPRISE machine and configure Splunk to receive from it
- installing XAMP Web Server and DVAW WEB App. on windows Server 2019 for machine
- AD Environment CONFIGURATIONS for Preparing to The Simulation of The Attacks
- installing SYSMON on windows 2019 WITH XAMP AND DVWA and configure splunk to receive it
- installing pfsense FW and segmentation
- Config. Pfsense FW RULES and send FW log to splunk part1
- Config. Pfsense FW RULES and send FW log to splunk part2
- installing suricata and config rules and send log to splunk
- reinstalling splunk and configure indexes and data sources
- pfsense FW Rules for INTER-VLAN routing
- Development the SOC lab by adding another HOST
- team4- project documentation release 4
- pfsense use case
- suricata use case
- NETWORK SCANNING USE CASE attacking dvwa we app

Use Case 1: Brute Force Attack

Description: Multiple failed authentication attempts from a single source IP against RDP/SSH/Web.
Why It Matters: Leads to account compromise, data breaches, and ransomware deployment.
Data Sources: Windows EventCode 4625 (Failed Logon), /var/log/secure, HTTP 401 status codes.
MITRE ATT&CK: T1110 — Brute Force

```
Payload:
hydra -L /usr/share/wordlists/metasploit/namelist.txt -p WrongPass123 192.168.254.140 rdp
OR
for i in {1..20}; do net rdp share -I 192.168.254.140 -U fakeuser%wrongpass; done

SPL:
index="windows_dc" EventCode=4625
| stats count min(_time) as firstTime
    max(_time) as lastTime
    by Source_Network_Address, Account_Name
| where count >= 5
| eval severity="high"
```

kali-linux-2025.4-vmware-amd64 for VAPT - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer
- Windows Server 2019 AD
- Windows 10 x64 pc1
- Windows 10 x64 pc2
- kali-linux-2025.4-vmware-amd64 for VAPT
- Windows Server 2019 for XAMP and DVWA
- Pfsense FW
- Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-li...

1 2 3 4 02:25 PM

kali@kali: ~

Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.254.140
PING 192.168.254.140 (192.168.254.140) 56(84) bytes of data.
64 bytes from 192.168.254.140: icmp_seq=1 ttl=127 time=2.72 ms
64 bytes from 192.168.254.140: icmp_seq=2 ttl=127 time=2.54 ms
64 bytes from 192.168.254.140: icmp_seq=3 ttl=127 time=1.09 ms
64 bytes from 192.168.254.140: icmp_seq=4 ttl=127 time=270 ms
64 bytes from 192.168.254.140: icmp_seq=5 ttl=127 time=2.59 ms
^C
--- 192.168.254.140 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.087/55.742/269.780/107.020 ms

┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/wordlists/metasploit/namelist.txt -p WrongPass123 192.168.254.140 rdp

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-05-16 07:16:27
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to re
cover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1909 login tries (l:1909/p:1), ~478 tries per task
[DATA] attacking rdp://192.168.254.140:3389/
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[STATUS] 90.00 tries/min, 90 tries in 00:01h, 1820 to do in 00:21h, 3 active
[ERROR] freerdp: The connection failed to establish.
[STATUS] 88.67 tries/min, 266 tries in 00:03h, 1644 to do in 00:19h, 3 active
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[STATUS] 87.29 tries/min, 611 tries in 00:07h, 1299 to do in 00:15h, 3 active
[ERROR] freerdp: The connection failed to establish.
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~]
└─$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

27°C مشمس | Search | ENG | 02:25 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 13:59 16 ماي

Search | Splunk 10.2.0 | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/search?q=search index%3D"windows_dc" EventCode%3D4625%0A| stats count min(90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

New Search

SPL | Convert to SPL2 | Save As | Create Table View | Close

```
index="windows_dc" EventCode=4625
| stats count min(_time) as firstTime
    max(_time) as lastTime
    by Source_Network_Address, Account_Name
| where count >= 5
| eval severity="high"
```

Time range: Last 24 hours

✓ 1,230 events (5/15/26 1:00:00.000 PM to 5/16/26 1:59:47.000 PM) | No Event Sampling | Job | Verbose Mode

Events (1,230) | Patterns | Statistics (8) | Visualization

Show: 20 Per Page | Format | Preview: On

Source_Network_Address	Account_Name	count	firstTime	lastTime	severity
192.168.250.128	-	1230	1778885005.409	1778929185.395	high
192.168.250.128	10	6	1778885009.016	1778929162.677	high
192.168.250.128	12	6	1778885007.478	1778929162.742	high
192.168.250.128	14	5	1778885011.042	1778929164.706	high
192.168.250.128	15	6	1778885011.271	1778929164.755	high
192.168.250.128	16	5	1778885011.528	1778888414.196	high
192.168.250.128	2	5	1778885013.564	1778929167.049	high
192.168.250.128	4	5	1778885015.586	1778929169.080	high

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

27°C مشمس | Search | ENG | 01:59 م 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 14:01 16 ماي

Search | Splunk 10.2.0 | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/search?q=search index%3D"windows_dc" EventCode%3D4625%0A| stats count min(90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

New Search

SPL | Convert to SPL2 | Save As | Create Table View | Close

```
index="windows_dc" EventCode=4625
| stats count min(_time) as firstTime
    max(_time) as lastTime
    by Source_Network_Address, Account_Name
| where count >= 5
| eval severity="high"
```

Time range: All time (real-time)

101 of 319 events matched | No Event Sampling | Job | Verbose Mode

Events (101) | Patterns | **Statistics (1)** | Visualization

Show: 20 Per Page | Format

Source_Network_Address	Account_Name	count	firstTime	lastTime	severity
192.168.250.128	-	100	1778929221.818	1778929270.905	high

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

27°C مشمس | Search | ENG | 02:01 م 2026/05/16

Use Case 2: SQL Injection (SQLi)

Description: Malicious SQL code inserted into URLs/forms to manipulate the database (OWASP Top 10 #1).
Why It Matters: Data exfiltration of PII/financial data, authentication bypass, Remote Code Execution.
Data Sources: Apache access logs (webapp index), ModSecurity WAF logs (waf index).
MITRE ATT&CK: T1190 — Exploit Public-Facing Application

```
Payload:
1' UNION SELECT user, password FROM users #
OR
' OR '1’=‘1
OR
sqlmap -u http://192.168.120.100/dvwa/vulnerabilities/sqli//?id=1&Submit=Submit

SPL:
index=* "UNION"
| stats values(sourcetype) as "Source Types",
    count by host

-- Alternative (WAF + Web combined) --
(index=waf OR index=webapp) ("UNION SELECT" OR "OR 1=1")
| rex field=_raw "GET (?<url>.+?) HTTP"
| table _time host url
```

kali-linux-2025.4-vmware-amd64 for VAPT - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer
- Windows Server 2019 AD
- Windows 10 x64 pc1
- Windows 10 x64 pc2
- kali-linux-2025.4-vmware-amd64 for VAPT
- Windows Server 2019 for XAMP and DVWA
- Pfsense FW
- Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-li...

1 2 3 4 02:57 PM

Vulnerability: SQL Injectio

CPU usage: 6.7%

Not Secure http://192.168.120.100/dvwa/vulnerabilities/sqli/?id=1'+UNION+SELECT+user%2C+password+FROM+users+%23&Submit

OffSec | Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | Welcome :: Damn Vul... | Neo4j Browser | Welcome :: Damn Vul...

DVWA

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript Attacks
- Authorisation Bypass
- Open HTTP Redirect
- Cryptography
- API
- DVWA Security

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 02:57 2026/05/16

kali-linux-2025.4-vmware-amd64 for VAPT - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer
- Windows Server 2019 AD
- Windows 10 x64 pc1
- Windows 10 x64 pc2
- kali-linux-2025.4-vmware-amd64 for VAPT
- Windows Server 2019 for XAMP and DVWA
- Pfsense FW
- Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-li...

1 2 3 4 03:16 PM

Vulnerability: SQL Injectio

Not Secure http://192.168.120.100/dvwa/vulnerabilities/sqli/?id='+OR+'1'%3D'1&Submit=Submit#

OffSec | Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | Welcome :: Damn Vul... | Neo4j Browser | Welcome :: Damn Vul...

DVWA

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript Attacks
- Authorisation Bypass
- Open HTTP Redirect
- Cryptography
- API
- DVWA Security

Vulnerability: SQL Injection

User ID: Submit

```
ID: ' OR '1'='1
First name: admin
Surname: admin

ID: ' OR '1'='1
First name: Gordon
Surname: Brown

ID: ' OR '1'='1
First name: Hack
Surname: Me

ID: ' OR '1'='1
First name: Pablo
Surname: Picasso

ID: ' OR '1'='1
First name: Bob
Surname: Smith
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 03:16 2026/05/16

kali-linux-2025.4-vmware-amd64 for VAPT - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-li...

1 2 3 4 02:56 PM

kali@kali: ~

Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.120.100
PING 192.168.120.100 (192.168.120.100) 56(84) bytes of data.
64 bytes from 192.168.120.100: icmp_seq=1 ttl=127 time=1.32 ms
64 bytes from 192.168.120.100: icmp_seq=2 ttl=127 time=1.40 ms
64 bytes from 192.168.120.100: icmp_seq=3 ttl=127 time=1.18 ms
64 bytes from 192.168.120.100: icmp_seq=4 ttl=127 time=0.732 ms
^C
--- 192.168.120.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.732/1.157/1.395/0.257 ms

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.120.100/dvwa/vulnerabilities/sqli//?id=1&Submit=Submit"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.10.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal law
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 07:53:44 /2026-05-16/

[07:53:44] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.120.100/dvwa/login.php'. Do you want to follow? [Y/n] y
[07:53:47] [CRITICAL] WAF/IPS identified as 'ModSecurity (Trustwave)'
you have not declared cookie(s), while server wants to set its own ('security=low;PHPSESSID=unafi5eb2d7...gnbajmqeie'). Do you want to use those [Y/n] y
[07:53:51] [INFO] testing if the target URL content is stable
[07:53:51] [WARNING] GET parameter 'id' does not appear to be dynamic
[07:53:51] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[07:53:52] [INFO] testing for SQL injection on GET parameter 'id'
[07:53:52] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:53:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[07:53:52] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:53:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[07:53:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[07:53:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[07:53:52] [INFO] testing 'Generic inline queries'
[07:53:52] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[07:53:52] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[07:53:52] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[07:53:53] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[07:53:53] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[07:53:53] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[07:53:53] [INFO] testing 'Oracle AND time-based blind'
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 02:56 2026/05/16

kali-linux-2025.4-vmware-amd64 for VAPT - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-li...

1 2 3 4 02:57 PM

kali@kali: ~

Session Actions Edit View Help

```
got a 302 redirect to 'http://192.168.120.100/dvwa/login.php'. Do you want to follow? [Y/n] y
[07:53:47] [CRITICAL] WAF/IPS identified as 'ModSecurity (Trustwave)'
you have not declared cookie(s), while server wants to set its own ('security=low;PHPSESSID=unafi5eb2d7...gnbajmqeie'). Do you want to use those [Y/n] y
[07:53:51] [INFO] testing if the target URL content is stable
[07:53:51] [WARNING] GET parameter 'id' does not appear to be dynamic
[07:53:51] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[07:53:52] [INFO] testing for SQL injection on GET parameter 'id'
[07:53:52] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:53:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[07:53:52] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:53:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[07:53:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[07:53:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[07:53:52] [INFO] testing 'Generic inline queries'
[07:53:52] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[07:53:52] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[07:53:52] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[07:53:53] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[07:53:53] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[07:53:53] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[07:53:53] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[07:53:55] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[07:53:55] [WARNING] GET parameter 'id' does not seem to be injectable
[07:53:55] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[07:53:55] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[07:53:55] [INFO] testing for SQL injection on GET parameter 'Submit'
[07:53:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:53:56] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[07:53:56] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:53:56] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[07:53:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[07:53:56] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[07:53:56] [INFO] testing 'Generic inline queries'
[07:53:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[07:53:57] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[07:53:57] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[07:53:57] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[07:53:57] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[07:53:57] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[07:53:57] [INFO] testing 'Oracle AND time-based blind'
[07:53:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[07:53:57] [WARNING] GET parameter 'Submit' does not seem to be injectable
[07:53:57] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that the
re is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 07:53:57 /2026-05-16/
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 02:57 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 14:56 16 ماي

Search | Splunk 10.2.0 | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/search?q=search index%3D* "UNION"%0A| stats values(sourcetype) as "Source Types 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

New Search

SPL | Convert to SPL2 | Save As | Create Table View | Close

```
index=* "UNION"
| stats values(sourcetype) as "Source Types",
    count by host
```

Time range: All time (real-time)

18 of 18 events matched | No Event Sampling | Job | Verbose Mode

Events (18) | Patterns | Statistics (2) | Visualization

Show: 20 Per Page | Format

host	Source Types	count
192.168.254.2	_json	6
WEBSRV	apache:access modsecurity:json	12

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 02:56 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

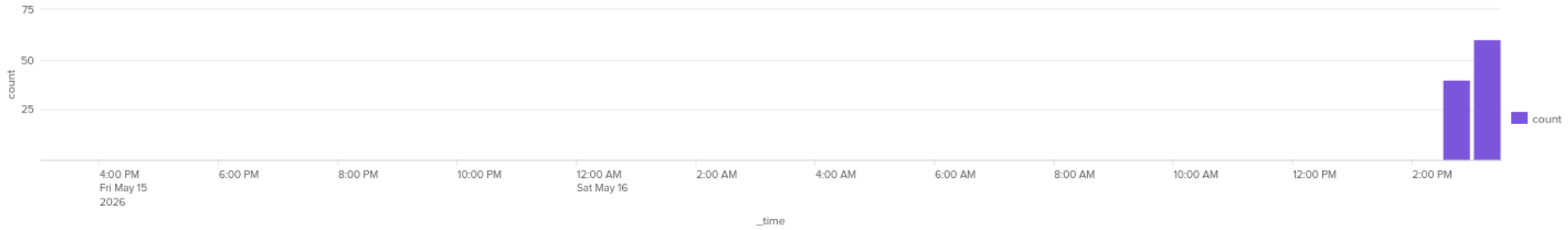
Activities | Firefox Web Browser | 15:19 16 ماي

Dashboards | Splunk 10.2 | WORKING DASHBOARD | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/working_dashboard_panels 90%

No results found.

PANEL 3 — SQLi ATTACKS



PANEL 4 — DNS RECON

No results found.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 03:19 م 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 15:19 16 ماي

Dashboards | Splunk 10.2 | SQL Injection (Works on y | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadministrator%2Fsearch%2Fsaved%2Fsearches%2FSQL%... 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

SQL Injection (Works on your old DVWA attack)

Edit

SQL Injection (Works on your old DVWA attack)

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by administrator. Edit
Modified: May 12, 2026 10:15:56 PM
Alert Type: Real-time. Edit

Trigger Condition: Per-Result. Edit
Actions: 2 Actions Edit
Add to Triggered Alerts
Send email

Trigger History

20 per page

Prev 1 2 3 Next

	TriggerTime	Actions
1	2026-05-16 15:16:15 EEST	View Results
2	2026-05-16 15:16:10 EEST	View Results
3	2026-05-16 15:15:49 EEST	View Results
4	2026-05-16 15:15:44 EEST	View Results
5	2026-05-16 15:15:43 EEST	View Results
6	2026-05-16 15:15:41 EEST	View Results
7	2026-05-16 15:13:03 EEST	View Results
8	2026-05-16 15:12:58 EEST	View Results
9	2026-05-16 15:12:46 EEST	View Results
10	2026-05-16 15:12:41 EEST	View Results
11	2026-05-16 15:12:41 EEST	View Results
12	2026-05-16 15:12:38 EEST	View Results
13	2026-05-16 15:10:58 EEST	View Results
14	2026-05-16 15:10:53 EEST	View Results

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 03:19 م 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 15:18 16 ماي

Dashboards | Splunk 10.2 | Triggered Alerts | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/triggered_alerts?eai%3Aacl.app=search&eai%3Aacl.owner=*&severity=*&alert_name 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Triggered Alerts

Filter

App: Search & Report... | Owner: All owners | Severity: All severity | Alert name: All alerts

Showing 1 - 20 of 5198 results | Show: 20 per p... | 1 of 260 pages

Time	Alert name	App	Type	Severity	Mode	Actions
2026-05-16 15:16:15 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:16:10 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:15:49 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:15:44 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:15:43 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:15:41 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:15:00 EEST	Brute Force Detection2 - Failed Logons	search	Scheduled	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:13:03 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:12:58 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:12:46 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:12:41 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:12:41 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:12:38 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:10:58 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:10:53 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:10:33 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:10:18 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:10:13 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:10:12 EEST	SQL Injection (Works on your old DVWA attack)	search	Real-time	High	Per Result	View Results | Edit Alert | Delete

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 03:18 م 2026/05/16

Use Case 3: Network Scanning (Reconnaissance)

Description: Mapping live hosts, open ports, and running services using Nmap — Cyber Kill Chain Phase 1.
Why It Matters: High-fidelity precursor to exploitation; early detection enables hardening.
Data Sources: pfSense firewall logs (filterlog), Suricata IDS alerts.
MITRE ATT&CK: T1046 — Network Service Discovery | T1595 — Active Scanning

```
Payload:
nmap -Pn -sS -A -p- -T4 192.168.254.140
nmap -Pn -sS -A -p- -T4 10.1.1.100
nmap -Pn -sS -A -p- -T4 10.2.1.100
nmap -Pn -sS -A -p- -T4 192.168.120.100
nmap -Pn -sS -A -p- -T4 192.168.250.129

SPL:
index=pfsense_fw
| stats dc(dest_port) as scanned_ports
        count by src_ip dest_ip
| where scanned_ports > 20
| sort - scanned_ports
OR
index=pfsense_fw src_ip=192.168.250.128
| stats dc(dest_port) as unique_ports
        values(dest_port) as ports
        by src_ip dest_ip
| where unique_ports > 15
| sort - unique_ports
```

kali-linux-2025.4-vmware-amd64 for VAPT - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-li...

1 2 3 4 04:30 PM

kali@kali: ~

Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.250.129
PING 192.168.250.129 (192.168.250.129) 56(84) bytes of data.
64 bytes from 192.168.250.129: icmp_seq=1 ttl=64 time=0.514 ms
64 bytes from 192.168.250.129: icmp_seq=2 ttl=64 time=0.411 ms
64 bytes from 192.168.250.129: icmp_seq=3 ttl=64 time=0.542 ms
64 bytes from 192.168.250.129: icmp_seq=4 ttl=64 time=2.00 ms
^C
--- 192.168.250.129 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.411/0.867/2.001/0.656 ms

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sS -A -p- -T4 192.168.250.129

Starting Nmap 7.98 ( https://nmap.org ) at 2026-05-16 09:23 -0400
Nmap scan report for 192.168.250.129
Host is up (0.00064s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.4 (protocol 2.0)
53/tcp open  domain  (generic dns response: REFUSED)
80/tcp open  http    nginx
|_http-title: pfSense - Login
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.98%I=7%D=5/16%Time=6A087032%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0\0");
MAC Address: 00:0C:29:2F:B1:19 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.64 ms 192.168.250.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.05 seconds

┌──(kali㉿kali)-[~]
└─$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

31°C مشمس | Search | ENG | 04:30 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 15:51 16 ماي

Search | Splunk 10.2.0 | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/search?s=%2FservicesNS%2Fadministrator%2Fsearch%2Fsaved%2Fsearches%2FAler 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

Alert 1 — Port Scan Detection

SPL | Convert to SPL2 | Save | Save As | View | Create Table View | Close

```
index=pfsense_fw
| stats dc(dest_port) as scanned_ports
        count by src_ip dest_ip
| where scanned_ports > 20
| sort - scanned_ports
```

Time range: All time

✓ 1,186,847 events (before 5/16/26 3:46:50.000 PM) | No Event Sampling | Job | Verbose Mode

Events (1,186,847) | Patterns | Statistics (7) | Visualization

Show: 20 Per Page | Format | Preview: On

src_ip	dest_ip	scanned_ports	count
192.168.250.129	192.168.250.128	42	556
192.168.250.128	192.168.250.129	65530	538116
192.168.250.128	192.168.120.100	64401	225764
192.168.250.128	192.168.254.140	57348	113576
192.168.250.128	10.1.1.100	49607	84489
192.168.250.128	10.2.1.100	42345	56682
8.8.8.8	192.168.250.129	44	44

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

أيام حارة قادمة 30°C | Search | ENG | 03:51 م 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 15:56 16 ماي

Search | Splunk 10.2.0 | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/search?s=%2FservicesNS%2Fadministrator%2Fsearch%2Fsaved%2Fsearches%2FAler 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

Alert 1 — Port Scan Detection

SPL | Convert to SPL2 | Save | Save As | View | Create Table View | Close

```
index=pfsense_fw src_ip=192.168.250.128
| stats dc(dest_port) as unique_ports
        values(dest_port) as ports
        by src_ip dest_ip
| where unique_ports > 15
| sort - unique_ports
```

Time range: All time

✓ **1,026,448 events** (before 5/16/26 3:54:43.000 PM) | No Event Sampling | Job | Verbose Mode

Events (1,026,448) | Patterns | **Statistics (5)** | Visualization

Show: 20 Per Page | Format | Preview: On

src_ip	dest_ip	unique_ports	ports
192.168.250.128	192.168.250.129	65530	1 10 100 1000 10000 10001 10002 10003 10004 10005 10006 10007 10008 10009 1001 10010 10011 10012 10013 10014 10015

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 03:56 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 15:57 16 ماي

Alert 1 — Port Scan Dete | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadministrator%2Fsearch%2Fsaved%2Fsearches%2FAlert% 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

Alert 1 — Port Scan Detection

Edit

Alert 1 — Port Scan Detection

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by administrator. Edit
Modified: ..... May 13, 2026 1:25:39 AM
Alert Type: ..... Real-time. Edit

Trigger Condition: .. Per-Result. Edit
Actions: ..... 1 Action Edit
Add to Triggered Alerts

Trigger History

20 per page

Prev 1 2 3 4 5 6 7 8 9 ... Next

	TriggerTime	Actions
1	2026-05-16 15:36:31 EEST	View Results
2	2026-05-16 15:36:29 EEST	View Results
3	2026-05-16 15:36:29 EEST	View Results
4	2026-05-16 15:36:28 EEST	View Results
5	2026-05-16 15:36:27 EEST	View Results
6	2026-05-16 15:36:27 EEST	View Results
7	2026-05-16 15:36:26 EEST	View Results
8	2026-05-16 15:36:26 EEST	View Results
9	2026-05-16 15:36:25 EEST	View Results
10	2026-05-16 15:36:25 EEST	View Results
11	2026-05-16 15:36:24 EEST	View Results
12	2026-05-16 15:36:24 EEST	View Results
13	2026-05-16 15:36:23 EEST	View Results
14	2026-05-16 15:36:22 EEST	View Results

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 03:57 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 15:59 16 ماي

Triggered Alerts | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/triggered_alerts?eai%3Aacl.app=search&eai%3Aacl.owner=*&severity=*&alert_name 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Triggered Alerts

Filter

App: Search & Report... | Owner: All owners | Severity: All severity | Alert name: All alerts

Showing 1 - 20 of 5468 results | Show: 20 per p... | 1 of 274 pages

Time	Alert name	App	Type	Severity	Mode	Actions
2026-05-16 15:36:31 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:29 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:29 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:28 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:27 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:27 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:26 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:26 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:25 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:25 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:24 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:24 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:23 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:22 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:21 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:20 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:20 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:19 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete
2026-05-16 15:36:19 EEST	Alert 1 — Port Scan Detection	search	Real-time	High	Per Result	View Results | Edit Alert | Delete

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 03:59 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 16:04 16 ماي

Dashboards | Splunk 10.2 | Dashboards | Splunk 10.2 | My Fourth Dashboard | Sp | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/my_fourth_dashboard?form.global_time.earliest=-24h%40h&form.global_time.latest 70%

splunk>enterprise Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

My Fourth Dashboard

My Fourth Dashboard

Download | Display | 100 % | Actions | Edit

Global Time Range

Last 24 hours

Top Scanned Hosts

dest_ip	count
192.168.250.129	230923
192.168.120.100	173225
192.168.254.140	50445
34.107.243.93	2374

Prev 1 2 Next

Top Scanned Ports

dest_port	count
443	4810
53	4780
3389	3657
80	3147
123	619

Prev 1 2 3 4 5 ... Next

Scan Timeline

_time	count
2026-05-16T16:00:00.000+03:00	31
2026-05-16T15:30:00.000+03:00	90351
2026-05-16T15:00:00.000+03:00	15601
2026-05-16T14:30:00.000+03:00	1574
2026-05-16T14:00:00.000+03:00	2491

Prev 1 2 3 Next

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 04:04 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 16:07 16 ماي

Dashboards | Splunk 10.2 | Nmap Reconnaissance M | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/nmap_reconnaissance_monitoring?tab=layout_1&form.global_time.earliest=0&form. 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

Nmap Reconnaissance Monitoring

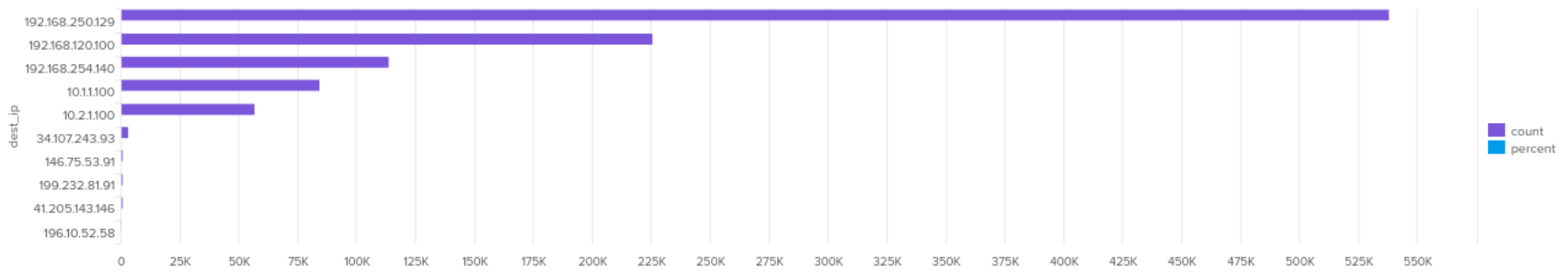
Nmap Reconnaissance Monitoring

Download | Display | 100 % | Actions | Edit

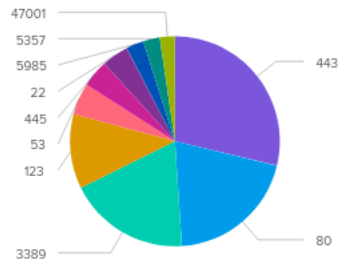
Global Time Range

All time

Panel 1 — Top Scanned Hosts



Panel 2 — Top Targeted Ports



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 04:07 2026/05/16

Ubuntu 64-bit For Splunk - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
  - Windows Server 2019 AD
  - Windows 10 x64 pc1
  - Windows 10 x64 pc2
  - kali-linux-2025.4-vmware-amd64 for VAPT
  - Windows Server 2019 for XAMP and DVWA
  - Pfsense FW
  - Ubuntu 64-bit For Splunk

Home | Ubuntu 64-bit For Splunk | Pfsense FW | Windows 10 x64 pc1 | Windows Server 2019 AD | Windows 10 x64 pc2 | Windows Server 2019 for XAMP... | kali-lin...

Activities | Firefox Web Browser | 16:07 16 ماي

Dashboards | Splunk 10.2 | Nmap Reconnaissance M | pfSense.SOC.DEPI - Statu | testmyids.com/

localhost:8000/en-US/app/search/nmap_reconnaissance_monitoring?tab=layout_1&form.global_time.earliest=0&form. 90%

splunk>enterprise | Apps | Administrator | 6 Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Modules | Search & Reporting

Nmap Reconnaissance Monitoring

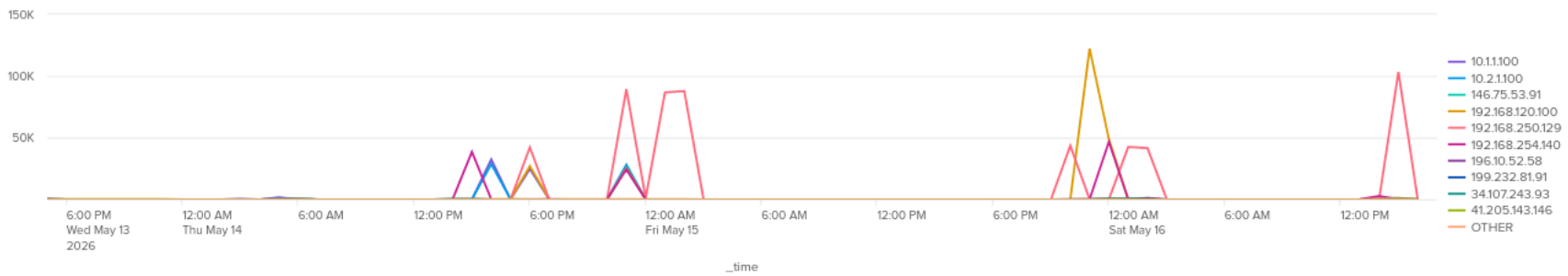
Nmap Reconnaissance Monitoring

Download | Display | 100 % | Actions | Edit

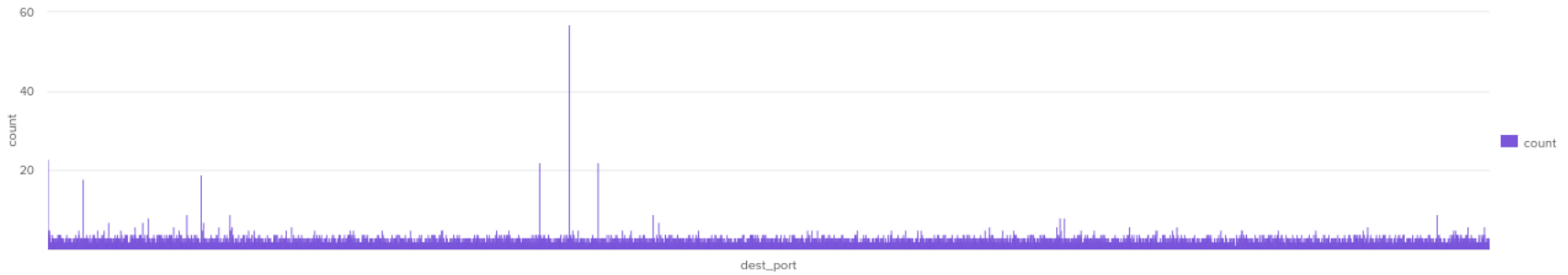
Global Time Range

All time

Panel 3 — Scan Timeline



Panel 4 — AD Recon Activity



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C مشمس | Search | ENG | 04:07 2026/05/16

Risk Assessment & Key Performance Indicators

RISK ASSESSMENT:

Risk	Impact	Mitigation
Resource Exhaustion	High	Limit Win10 VMs to 2GB RAM each
IP Address Conflicts	Medium	Strict IP standard; never change subnets
Log Injection Failure	High	Verify UF connectivity via ping + telnet 9997
WAF False Positives	Medium	Run ModSecurity in Detection-Only first

KEY PERFORMANCE INDICATORS (KPIs):

99% System Uptime
Splunk web interface availability over 4-week test phase

100% Log Coverage
All critical hosts (TEAM4-DC, WEBSRV, pfSense) forwarding successfully

0 False Negatives
Zero missed detections during SQLi and NTLM relay simulations

< 2 min Response Time
Alert generation in Splunk within 2 minutes of trigger event

Testing & Quality Assurance

Test ID	Scenario	Expected Outcome	Status
TC-01	Brute Force from Kali (192.168.250.128)	Splunk alert after >= 5 failed logons	PASSED
TC-02	SQL Injection on DVWA (UNION SELECT)	ModSecurity logs + Splunk dashboard shows UNION	PASSED
TC-03	Nmap Scan (-sV -A -p-) via WAN	pfSense/Suricata logs traffic; Splunk alert fires	PASSED

Findings & Recommendations

FINDINGS:

* i5-1235U / 16GB RAM successfully handles the complete 7-VM lab
* All 5 use cases detected and validated with zero false negatives
* Multi-layer detection (WAF + IDS + Endpoint + SIEM) works as designed
* pfSense network segmentation effectively isolates attack paths
* Splunk provides powerful correlation across all log sources

RECOMMENDATIONS:

* Upgrade to 32GB RAM for scaling beyond 10 use cases
* Add dedicated Syslog-ng server for Linux log scalability
* Integrate SOAR platform for automated IP blocking
  (pfSense API triggered by Splunk high-severity alerts)
* Add threat intelligence feeds (AlienVault OTX, Tor exit nodes)
  for IOC enrichment in Splunk lookups
* Transition ModSecurity from Detection-Only to Enforcement mode

GRADING CRITERIA:

40% Technical Implementation (Splunk/pfSense configuration)
30% Testing (Attack simulations and validation)
20% Documentation (Report, playbooks, architecture docs)
10% Presentation

Incident Response (IR) Phase

Incident Response Framework:

The SOC IR Lifecycle (NIST SP 800-61)

- **Preparation:** Hardening pfSense, configuring Suricata rules, and deploying Splunk Universal Forwarders.
- **Detection & Analysis:** Monitoring the "Security Posture" dashboard. Identifying Nmap scans (recon) and SQLi payloads (exploitation).
- **Containment:** Using pfSense "EasyRule" to block Attacker IP (192.168.250.128) at the WAN interface.
- **Post-Incident:** Reviewing logs to close the vulnerability in DVWA or reset DC passwords.
- **Visual:** A circular diagram showing the 4 phases of NIST IR.

Incident Response (IR) Phase

Incident Response Framework:

Playbook - Network Reconnaissance (Nmap)

IR Playbook: Reconnaissance Detection

- **Trigger:** Splunk Alert "High Volume Port Scan Detected".
- **Identification:** * Source: Kali Linux (192.168.250.128).
  - Method: TCP SYN Scan (-sS).
- **Response Actions:**
  - Verify if the scan hit internal "Critical Assets" (Team4-DC).
  - Temporary Block: Blacklist the Kali IP on pfSense for 60 minutes.
  - Triage: Determine if this was a precursor to a larger attack.
- **Visual:** A flowchart showing "Detection -> Triage -> Block -> Notify".

Incident Response (IR) Phase

Incident Response Framework:

Playbook - Web Exploitation (SQLi)

IR Playbook: SQL Injection Attempt

- **Trigger:** WAF Alert (ModSecurity) index="waf" showing "UNION SELECT".
- **Identification:** * Target: WEBSRV (192.168.120.100).
  - Impact: Attempted Database credential theft.
- **Response Actions:**
  - **Immediate:** Block Source IP at the WAF level.
  - **Analysis:** Check access.log to see if the HTTP 200 response returned data or just an error.
  - **Remediation:** Set DVWA security level to "Medium/High" or patch the PHP code.
- **Visual:** A screenshot of the ModSecurity "Audit Log" showing the blocked SQL payload.

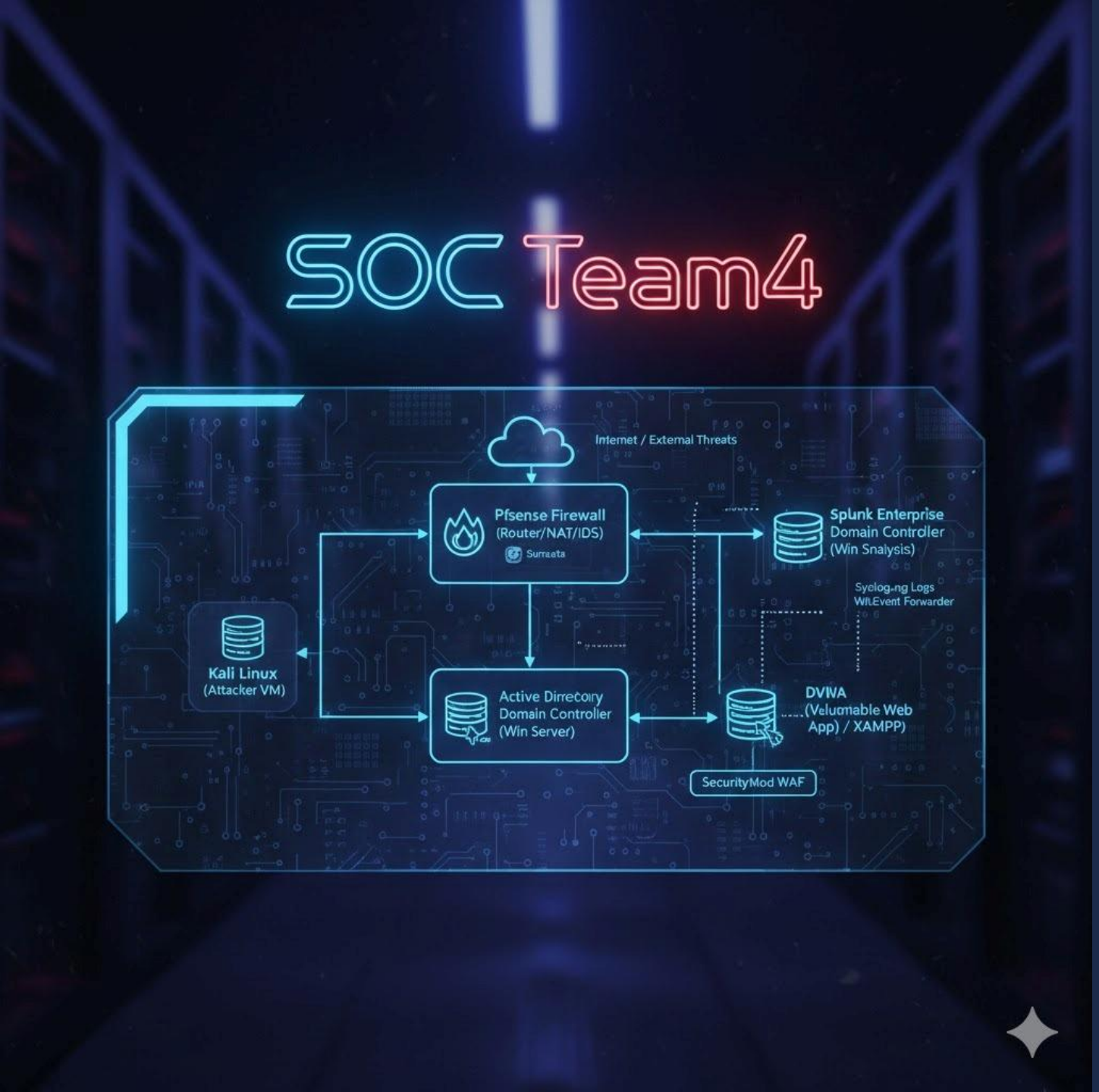
Incident Response (IR) Phase

Incident Response Framework:

IR Metrics & Mitigation Results

Containment & Recovery Results

- **Mean Time to Detect (MTTD):** < 45 Seconds (from Kali scan start to Splunk alert).
- **Mean Time to Respond (MTTR):** < 3 Minutes (manual IP block on pfSense).
- **Containment Success:** 100% of simulated attacks were isolated to the DMZ; no lateral movement to the Corporate Network was successful.
- **Evidence Preservation:** All logs (Suricata, Sysmon, Apache) successfully indexed in Splunk for forensic review.
- **Visual:** A "Success" checkmark icon next to each of your 5 Use Cases.



Thank You!

Questions & Live Demo

We can demonstrate live:
- Nmap scan detection in Splunk (pfSense logs)
- SQL Injection payload capture (ModSecurity + Apache)
- Brute force alert trigger (EventCode 4625)

SOC Team 4 — DEPI 2026 | Release 4 | May 2026