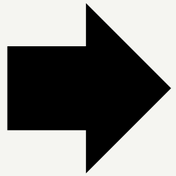
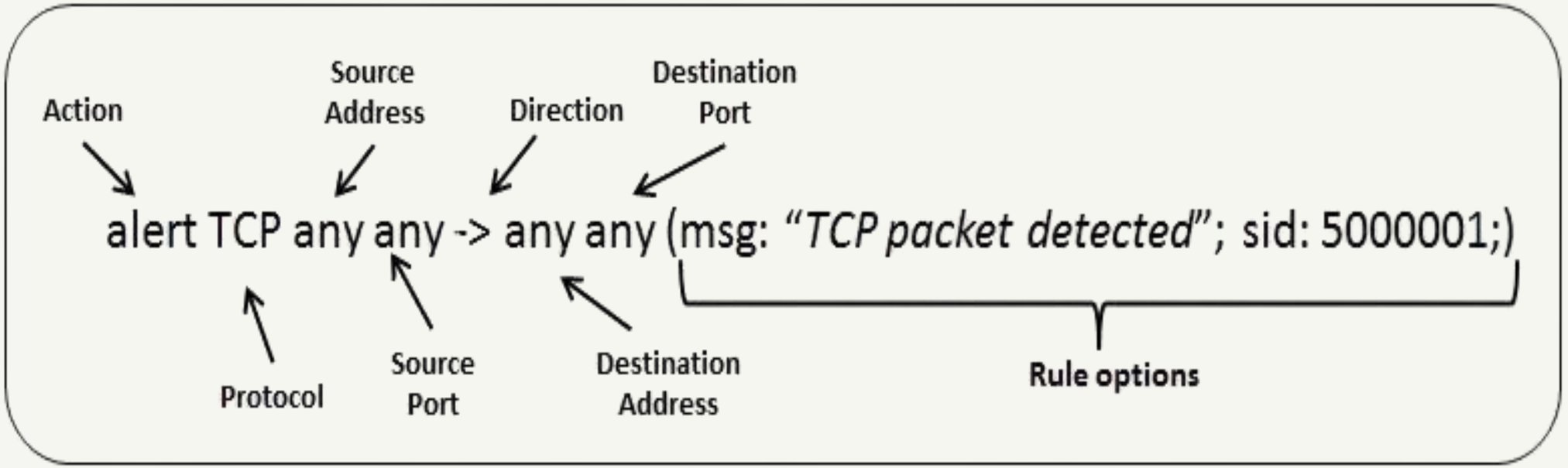
CUSTOM RULES



RULE STRUCTURE



RULE NO: 1

SYN Scan Detection

Rule

```
#1) Generic SYN scan
alert tcp any any -> $HOME_NET 1:20,24:79,81:109,111:142,144:3388,3390:65535 (msg:"SCAN: SYN scan detected";flags:S;flow:stateless;sid:4000001; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.10.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-20 05:45 EST
Nmap scan report for 192.168.10.51
Host is up (0.00083s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 08:00:27:6F:B5:F4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
[sudo] password for user:
11/23-20:59:49.314845  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:3306
11/23-20:59:49.314845  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:8888
11/23-20:59:49.314846  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:995
11/23-20:59:49.314846  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:993
11/23-20:59:49.314846  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:445
11/23-20:59:49.320708  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:443
11/23-20:59:49.314846  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:445
11/23-20:59:49.320708  [**] [1:4000001:1] SCAN: SYN scan detected [**] [Priority: 0] {TCP} 192.168.10.43:44333 -> 192.168.10.51:443
```

RULE NO: 2

FIN Scan Detection

Rule

```
# 2) FIN Scan Detection
alert tcp any any -> $HOME_NET any (msg:"Nmap FIN Scan"; flags:F; flow:stateless;sid:10000302; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ nmap -sF 192.168.10.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 07:27 EST
Nmap scan report for 192.168.10.51
Host is up (0.0019s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
80/tcp   open|filtered http
110/tcp  open|filtered pop3
143/tcp  open|filtered imap
993/tcp  open|filtered imaps
995/tcp  open|filtered pop3s
3389/tcp open|filtered ms-wbt-server
MAC Address: 08:00:27:6F:B5:F4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
[sudo] password for user:
11/23-17:57:17.414498  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:80
11/23-17:57:17.414498  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:50716 -> 192.168.10.51:80
11/23-17:57:17.414499  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:3306
11/23-17:57:17.414499  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:50716 -> 192.168.10.51:3306
11/23-17:57:17.414499  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:587
11/23-17:57:17.414499  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:50716 -> 192.168.10.51:587
11/23-17:57:17.416248  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:21
11/23-17:57:17.416248  [**] [1:100005:1] FTP login attempt [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:21
11/23-17:57:17.416248  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:50716 -> 192.168.10.51:21
11/23-17:57:17.416248  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:1720
11/23-17:57:17.416248  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:50716 -> 192.168.10.51:1720
11/23-17:57:17.416248  [**] [1:100007332:1] RDP: Real Conection  Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:3389
11/23-17:57:17.416248  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:3389
11/23-17:57:17.416248  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:50716 -> 192.168.10.51:3389
11/23-17:57:17.416248  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:199
11/23-17:57:17.416248  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:50716 -> 192.168.10.51:199
11/23-17:57:17.416248  [**] [1:10000302:1] Nmap FIN Scan [**] [Priority: 0] {TCP} 192.168.10.43:50716 -> 192.168.10.51:110
```

RULE NO: 3

Xmas Scan Detection

Rule

```
# 3) Xmas Scan Detection
alert tcp any any -> $HOME_NET any (msg:"Nmap Xmas Scan"; flags:FPU; flow:stateless;sid:10000013; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ nmap -sX 192.168.10.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 07:29 EST
Nmap scan report for 192.168.10.51
Host is up (0.0026s latency).
```

Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
[sudo] password for user:
11/23-17:59:04.017856  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:995
11/23-17:59:04.017856  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:995
11/23-17:59:04.017856  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:113
11/23-17:59:04.017856  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:113
11/23-17:59:04.017856  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:1723
11/23-17:59:04.017856  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:1723
11/23-17:59:04.017856  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:8080
11/23-17:59:04.017856  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:8080
11/23-17:59:04.017857  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:993
11/23-17:59:04.017857  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:993
11/23-17:59:04.017857  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:445
11/23-17:59:04.017857  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:445
11/23-17:59:04.017857  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:587
11/23-17:59:04.017857  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:587
11/23-17:59:04.017857  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:256
11/23-17:59:04.017857  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:256
11/23-17:59:04.018600  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:199
11/23-17:59:04.018600  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.43:57214 -> 192.168.10.51:199
11/23-17:59:04.018600  [**] [1:10000013:1] Nmap Xmas Scan [**] [Priority: 0] {TCP} 192.168.10.43:57214 -> 192.168.10.51:135
```

RULE NO: 4

ICMP Detection

Rule

```
# 4) ICMP ping scan
alert icmp any any -> $HOME_NET any (msg:"SCAN: ICMP echo request";itype:8;sid:4000005; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.10.51
PING 192.168.10.51 (192.168.10.51) 56(84) bytes of data.
64 bytes from 192.168.10.51: icmp_seq=1 ttl=64 time=4.12 ms
64 bytes from 192.168.10.51: icmp_seq=2 ttl=64 time=4.55 ms
64 bytes from 192.168.10.51: icmp_seq=3 ttl=64 time=16.7 ms
64 bytes from 192.168.10.51: icmp_seq=4 ttl=64 time=1.25 ms
64 bytes from 192.168.10.51: icmp_seq=5 ttl=64 time=2.54 ms
64 bytes from 192.168.10.51: icmp_seq=6 ttl=64 time=1.41 ms
```

Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
11/20-16:15:13.678818  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:14.682365  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:15.680674  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:16.685535  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:17.687519  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:18.690219  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:19.691595  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:20.694789  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:21.697305  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
11/20-16:15:22.699130  [**] [1:4000005:1] SCAN: ICMP echo request [**] [Priority: 0] {ICMP} 192.168.10.43 -> 192.168.10.51
```

RULE NO: 5

SSH Login Attempt

Rule

```
# 5) SSH Login Attempt Detected
alert tcp any any -> $HOME_NET 22 (msg:"SSH Login Attempt"; flags:S; sid:1000001; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ ssh user@192.168.10.51
user@192.168.10.51's password:
Permission denied, please try again.
user@192.168.10.51's password:
Permission denied, please try again.
user@192.168.10.51's password:
user@192.168.10.51: Permission denied (publickey,password).
```

Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
[sudo] password for user:
11/23-18:01:25.814836  [**] [1:1000001:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.10.43:42362 -> 192.168.10.51:22
11/23-18:01:39.195980  [**] [1:1000001:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.10.43:48086 -> 192.168.10.51:22
11/23-18:01:46.660707  [**] [1:1000001:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.10.43:57886 -> 192.168.10.51:22
11/23-18:01:50.058717  [**] [1:1000001:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.10.43:58286 -> 192.168.10.51:22
11/23-18:02:04.883585  [**] [1:1000001:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.10.43:41966 -> 192.168.10.51:22
```

RULE NO:6
SSH (Brute force) Attempt

Rule

```
# 6) SSH Bruteforce Attempt
alert tcp any any -> $HOME_NET 22 (msg:"SSH Brute Force Attempt"; flow:to_server,established; detection_filter:track by_src, count 5, seconds 60; sid:1000002;
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ hydra -l user -p pass.txt ssh://192.168.10.51
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 2025-11-20 02:46:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.10.51:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-20 02:46:58
```

Real Time Alert Detection

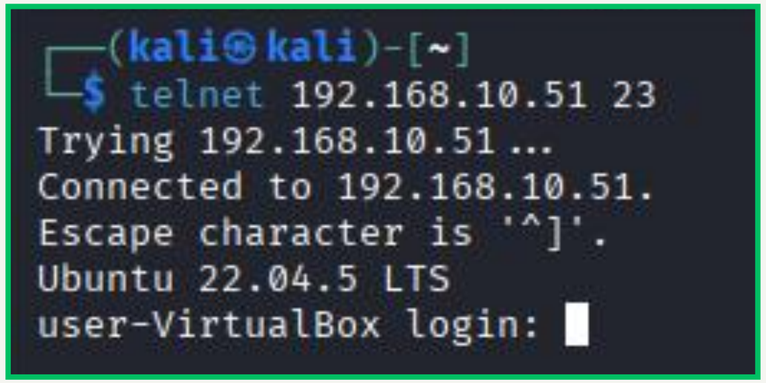
```
11/25-17:46:36.349090  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:56414 -> 192.168.10.51:22
11/25-17:46:33.346296  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:42612 -> 192.168.10.51:22
11/25-17:46:37.719346  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:56372 -> 192.168.10.51:22
11/25-17:46:34.356309  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:42644 -> 192.168.10.51:22
11/25-17:46:36.301207  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:56404 -> 192.168.10.51:22
11/25-17:46:36.914153  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:56344 -> 192.168.10.51:22
11/25-17:46:45.782449  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:56372 -> 192.168.10.51:22
11/25-17:46:40.454226  [**] [1:1000002:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.10.43:56414 -> 192.168.10.51:22
```

RULE NO: 7
Telnet Connection Attempt

Rule

```
# 7) Telnet login attempt to  port (ONLY port 23)
alert tcp any any -> $HOME_NET 23 (msg:"TELNET login attempt"; sid:1000003; rev:1;)
```

Threat Simulation



Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
[sudo] password for user:
11/25-17:54:00.664918  [**] [1:1000003:1] TELNET login attempt [**] [Priority: 0] {TCP} 192.168.10.43:53976 -> 192.168.10.51:23
11/25-17:54:00.668282  [**] [1:1000003:1] TELNET login attempt [**] [Priority: 0] {TCP} 192.168.10.43:53976 -> 192.168.10.51:23
11/25-17:54:00.752239  [**] [1:1000003:1] TELNET login attempt [**] [Priority: 0] {TCP} 192.168.10.43:53976 -> 192.168.10.51:23
11/25-17:54:00.753657  [**] [1:1000003:1] TELNET login attempt [**] [Priority: 0] {TCP} 192.168.10.43:53976 -> 192.168.10.51:23
11/25-17:54:00.756201  [**] [1:1000003:1] TELNET login attempt [**] [Priority: 0] {TCP} 192.168.10.43:53976 -> 192.168.10.51:23
11/25-17:54:00.759318  [**] [1:1000003:1] TELNET login attempt [**] [Priority: 0] {TCP} 192.168.10.43:53976 -> 192.168.10.51:23
```

RULE NO: 8
FTP Connection Attempt

Rule

```
# 8) FTP login attempt to port (ONLY port 21)
alert tcp any any -> $HOME_NET 21 (msg:"FTP login attempt"; sid:100005; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.10.51
Connected to 192.168.10.51.
220 (vsFTPd 3.0.5)
Name (192.168.10.51:kali): ^C
```

Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
[sudo] password for user:
11/25-17:44:47.183127  [**] [1:100005:1] FTP login attempt [**] [Priority: 0] {TCP} 192.168.10.43:43928 -> 192.168.10.51:21
11/25-17:44:47.187532  [**] [1:100005:1] FTP login attempt [**] [Priority: 0] {TCP} 192.168.10.43:43928 -> 192.168.10.51:21
11/25-17:44:47.244095  [**] [1:100005:1] FTP login attempt [**] [Priority: 0] {TCP} 192.168.10.43:43928 -> 192.168.10.51:21
11/25-17:45:05.600167  [**] [1:100005:1] FTP login attempt [**] [Priority: 0] {TCP} 192.168.10.43:57748 -> 192.168.10.51:21
11/25-17:45:05.601323  [**] [1:100005:1] FTP login attempt [**] [Priority: 0] {TCP} 192.168.10.43:57748 -> 192.168.10.51:21
11/25-17:45:05.635188  [**] [1:100005:1] FTP login attempt [**] [Priority: 0] {TCP} 192.168.10.43:57748 -> 192.168.10.51:21
```

RULE NO: 9

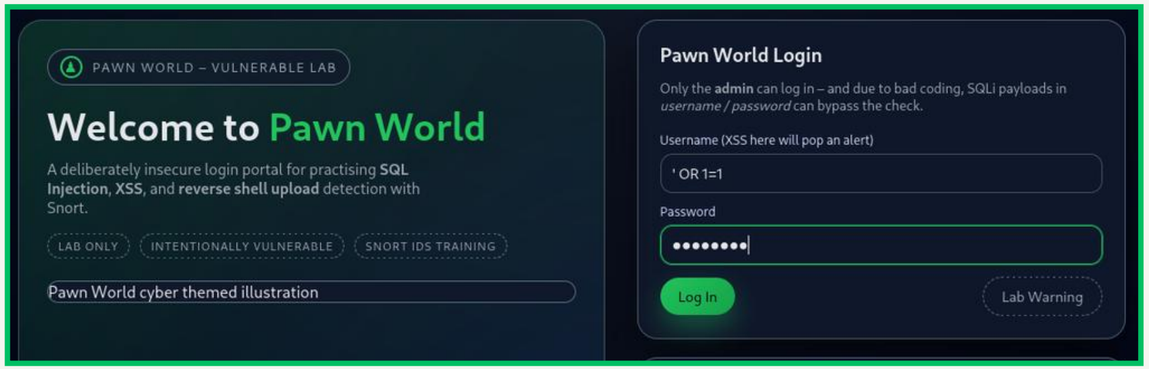
SQL Injection Detection

Rule

```
# 9) SQL Injection Attempt
alert tcp any any -> $HOME_NET 80 (msg:"SQL Injection Attempt Detected";content:"username=%27+OR+1%3D1";sid:100008902; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ curl -X POST "http://192.168.10.51/index.php" \
     -d "username=%27+OR+1%3D1&password=%27+OR+1%3D1"
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Pawn World - Vulnerable Login</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <style>
        * { box-sizing: border-box; margin: 0; padding: 0; }
        body {
            font-family: system-ui, -apple-system, BlinkMacSystemFont, "Segoe UI", sans-serif;
            background: radial-gradient(circle at top, #101827, #020617 60%);
            color: #e5e7eb;
            min-height: 100vh;
            display: flex;
            align-items: center;
            justify-content: center;
            padding: 20px;
        }
```



Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
11/25-10:24:23.280014  [**] [1:100008902:1] SQL Injection Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:37584 -> 192.168.10.51:80
11/25-10:24:53.791534  [**] [1:100008902:1] SQL Injection Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:53334 -> 192.168.10.51:80
11/25-10:25:10.152225  [**] [1:100008902:1] SQL Injection Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:52316 -> 192.168.10.51:80
11/25-10:25:34.819758  [**] [1:100008902:1] SQL Injection Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:52378 -> 192.168.10.51:80
11/25-10:25:35.499892  [**] [1:100008902:1] SQL Injection Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:52394 -> 192.168.10.51:80
11/25-10:25:36.849155  [**] [1:100008902:1] SQL Injection Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:52396 -> 192.168.10.51:80
```

RULE NO: 10

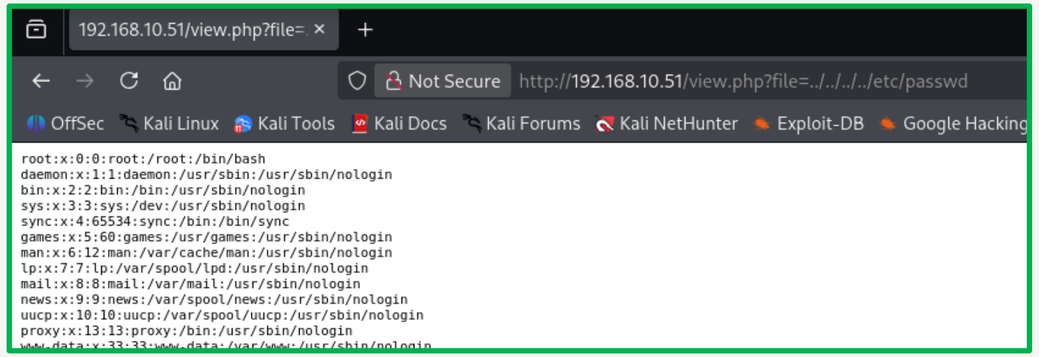
Directory Traversal Detection

Rule

```
# 10) Directory Traversal Attack  Detection
alert tcp any any -> $HOME_NET 80 (msg:"Directory Traversal Attempt Detected";content:"../"; http_uri;nocase;sid:10000301; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ curl "http://192.168.10.51/view.php?file=../../../../etc/passwd"
<pre>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```



Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
11/27-14:06:10.733770  [**] [1:10000301:1] Directory Traversal Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:59824 -> 192.168.10.51:80
11/27-14:07:11.327899  [**] [1:10000301:1] Directory Traversal Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:59136 -> 192.168.10.51:80
11/27-14:07:31.723334  [**] [1:10000301:1] Directory Traversal Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:46192 -> 192.168.10.51:80
11/27-14:07:49.247195  [**] [1:10000301:1] Directory Traversal Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:38096 -> 192.168.10.51:80
11/27-14:07:53.970251  [**] [1:10000301:1] Directory Traversal Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:38096 -> 192.168.10.51:80
11/27-14:07:59.076718  [**] [1:10000301:1] Directory Traversal Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:38096 -> 192.168.10.51:80
```

RULE NO: 11

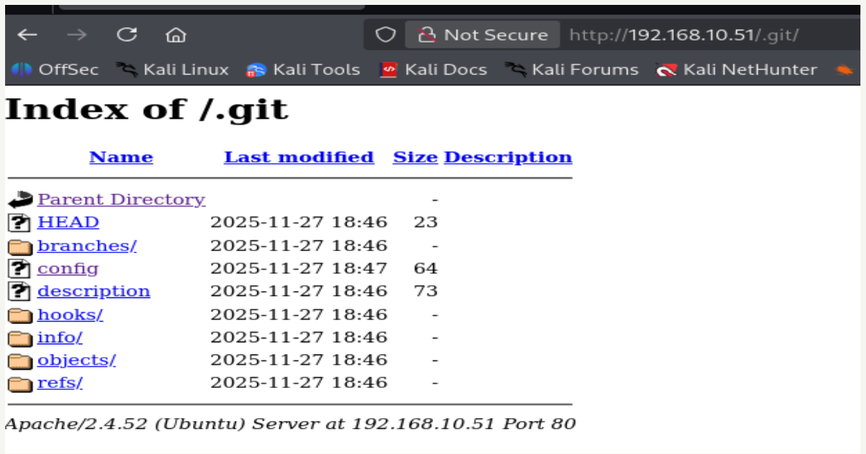
Sensitive File Access Detection

Rule

```
# 11) Sensitive File Access Detection
alert tcp any any -> $HOME_NET 80 (msg:"Sensitive Repository Access - .git Directory";content:"/.git"; http_uri;sid:1000300; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ curl -v http://192.168.10.51/.git/
*   Trying 192.168.10.51:80 ...
* Connected to 192.168.10.51 (192.168.10.51) port 80
* using HTTP/1.x
> GET /.git/ HTTP/1.1
> Host: 192.168.10.51
> User-Agent: curl/8.15.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Thu, 04 Dec 2025 06:43:09 GMT
< Server: Apache/2.4.52 (Ubuntu)
< Vary: Accept-Encoding
< Content-Length: 2289
< Content-Type: text/html;charset=UTF-8
```



Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo nano /etc/snort/rules/local.rules
[sudo] password for user:
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
11/27-18:53:51.835424  [**] [1:1000300:1] Sensitive Repository Access - .git Directory [**] [Priority: 0] {TCP} 192.168.10.43:58678 -> 192.168.10.51:80
11/27-18:54:14.137697  [**] [1:1000300:1] Sensitive Repository Access - .git Directory [**] [Priority: 0] {TCP} 192.168.10.43:39582 -> 192.168.10.51:80
11/27-18:54:56.401548  [**] [1:1000300:1] Sensitive Repository Access - .git Directory [**] [Priority: 0] {TCP} 192.168.10.43:51210 -> 192.168.10.51:80
11/27-18:55:01.820866  [**] [1:1000300:1] Sensitive Repository Access - .git Directory [**] [Priority: 0] {TCP} 192.168.10.43:51214 -> 192.168.10.51:80
11/27-18:55:19.046313  [**] [1:1000300:1] Sensitive Repository Access - .git Directory [**] [Priority: 0] {TCP} 192.168.10.43:59292 -> 192.168.10.51:80
```

RULE NO: 12
SQL Scanning Detection

Rule

```
# 12) SQL Scan Detection
alert tcp any any -> $HOME_NET 80 (msg:"SQLMap Scan Detected";content:"sqlmap"; http_header; nocase;sid:900500; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://192.168.10.51/index.php --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.11#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 laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:49:04 /2025-11-27/

[08:49:04] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=pjb8vk8igev...9loc4ee1u3'). Do you want to use those [Y/n] Y
[08:49:05] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:49:05] [INFO] testing if the target URL content is stable
[08:49:05] [INFO] target URL content is stable
[08:49:05] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms'

[*] ending @ 08:49:05 /2025-11-27/
```

Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
[sudo] password for user:
11/27-19:21:54.892871  [**] [1:900500:1] SQLMap Scan Detected [**] [Priority: 0] {TCP} 192.168.10.43:34924 -> 192.168.10.51:80
11/27-19:21:55.388680  [**] [1:900500:1] SQLMap Scan Detected [**] [Priority: 0] {TCP} 192.168.10.43:34928 -> 192.168.10.51:80
11/27-19:22:04.879050  [**] [1:900500:1] SQLMap Scan Detected [**] [Priority: 0] {TCP} 192.168.10.43:35758 -> 192.168.10.51:80
11/27-19:22:05.377895  [**] [1:900500:1] SQLMap Scan Detected [**] [Priority: 0] {TCP} 192.168.10.43:35768 -> 192.168.10.51:80
```

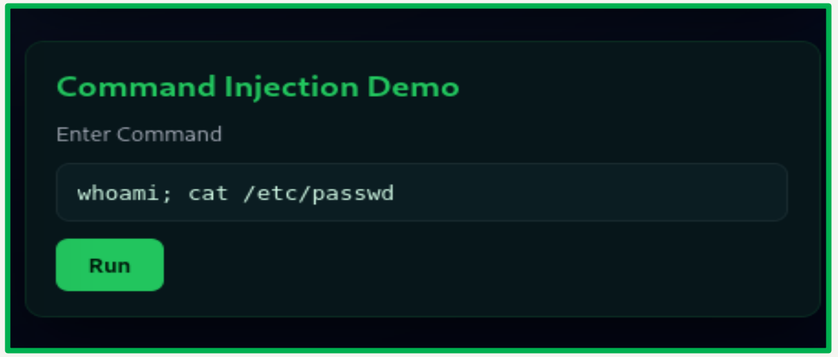
RULE NO: 13
Command Injection Attempt

Rule

```
# 13) Command Injection Attempt
alert tcp any any -> $HOME_NET 80 (msg:"Command Injection Attempt";content:"INJECT_DEMO";sid:1001300; rev:1;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ curl -X POST -d "cmd=whoami;INJECT_DEMO" http://192.168.10.51/
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Pawn World - Vulnerable Login</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <style>
        * { box-sizing: border-box; margin: 0; padding: 0; }
        body {
            font-family: system-ui, -apple-system, BlinkMacSystemFont, "Segoe UI"
            background: radial-gradient(circle at top, #101827, #020617 60%);
            color: #e5e7eb;
```



Real Time Alert Detection

```
user@user-VirtualBox:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
12/04-10:32:35.071111  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:38288 -> 192.168.10.51:80
12/04-10:32:40.343567  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:48424 -> 192.168.10.51:80
12/04-10:32:44.863161  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:48424 -> 192.168.10.51:80
12/04-10:33:51.914987  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:37880 -> 192.168.10.51:80
12/04-10:33:54.862356  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:37894 -> 192.168.10.51:80
12/04-10:33:55.539080  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:37904 -> 192.168.10.51:80
12/04-10:33:56.102416  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:53348 -> 192.168.10.51:80
12/04-10:33:56.596301  [**] [1:1001300:1] Command Injection Attempt [**] [Priority: 0] {TCP} 192.168.10.43:53354 -> 192.168.10.51:80
```

RULE NO: 14
XSS Detection

Rule

```
# 14) XSS Attempt
alert tcp any any -> $HOME_NET 80 (msg:"XSS Attempt Detected";content:"xss_comment=%3Cscript%3Ealert%281%29%3C%2Fscript%3E";sid:100008920; rev:2;)
```

Threat Simulation

```
┌──(kali㉿kali)-[~]
└─$ curl -X POST http://192.168.10.51/index.php \
  -d "xss_comment=%3Cscript%3Ealert%281%29%3C%2Fscript%3E"
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Pawn World - Vulnerable Login</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <style>
        * { box-sizing: border-box; margin: 0; padding: 0; }
        body {
            font-family: system-ui, -apple-system, BlinkMacSystemFont, "Segoe UI", sans
            background: radial-gradient(circle at top, #101827, #020617 60%);
            color: #e5e7eb;
            min-height: 100vh;
            display: flex;
            align-items: center;
            justify-content: center;
            padding: 20px;
        }
        .wrapper {
            max-width: 1100px;
            width: 100%;
            display: grid;
            grid-template-columns: minmax(0, 1.2fr) minmax(0, 1fr);
```

Real Time Alert Detection

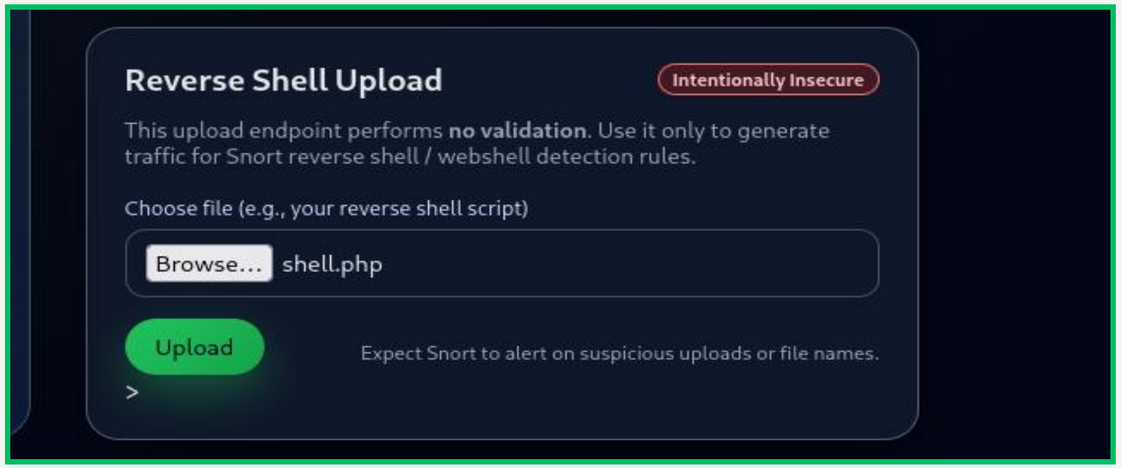
```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
11/25-15:19:53.849669  [**] [1:100008920:2] XSS Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:49126 -> 192.168.10.51:80
11/25-15:20:12.600421  [**] [1:100008920:2] XSS Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:42978 -> 192.168.10.51:80
11/25-15:20:13.290431  [**] [1:100008920:2] XSS Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:42984 -> 192.168.10.51:80
11/25-15:20:13.946519  [**] [1:100008920:2] XSS Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:42994 -> 192.168.10.51:80
11/25-15:20:14.593976  [**] [1:100008920:2] XSS Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:43000 -> 192.168.10.51:80
11/25-15:21:04.017647  [**] [1:100008920:2] XSS Attempt Detected [**] [Priority: 0] {TCP} 192.168.10.43:38234 -> 192.168.10.51:80
```

RULE NO: 15
File Upload Detection

Rule

```
# 15) Reverse Shell Attempt
alert tcp any any -> $HOME_NET 80 (msg:"PHP File Upload Detected (possible reverse shell)";content:"filename=\"";content:".php"; distance:0; within:15;sid:100000910; rev:2;)
```

Threat Simulation



Real Time Alert Detection

```
user@user-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
11/25-10:20:08.189818  [**] [1:100008910:1] PHP File Upload Detected (possible reverse shell) [**] [Priority: 0] {TCP} 192.168.10.43:42778 -> 192.168.10.51:80
11/25-10:20:58.175271  [**] [1:100008910:1] PHP File Upload Detected (possible reverse shell) [**] [Priority: 0] {TCP} 192.168.10.43:49202 -> 192.168.10.51:80
11/25-10:21:11.740090  [**] [1:100008910:1] PHP File Upload Detected (possible reverse shell) [**] [Priority: 0] {TCP} 192.168.10.43:34364 -> 192.168.10.51:80
11/25-10:22:14.120299  [**] [1:100008910:1] PHP File Upload Detected (possible reverse shell) [**] [Priority: 0] {TCP} 192.168.10.43:52252 -> 192.168.10.51:80
11/25-10:22:14.765203  [**] [1:100008910:1] PHP File Upload Detected (possible reverse shell) [**] [Priority: 0] {TCP} 192.168.10.43:52258 -> 192.168.10.51:80
```