IoRL ISF - Internet of Radio-Light Integrated Security Framework

Marcin Gregorczyk
m.gregorczyk@tele.pw.edu.pl
Warsaw University of Technology

IoRL is a 5G PPP project funded by the EC H2020 research programme

ISF elements

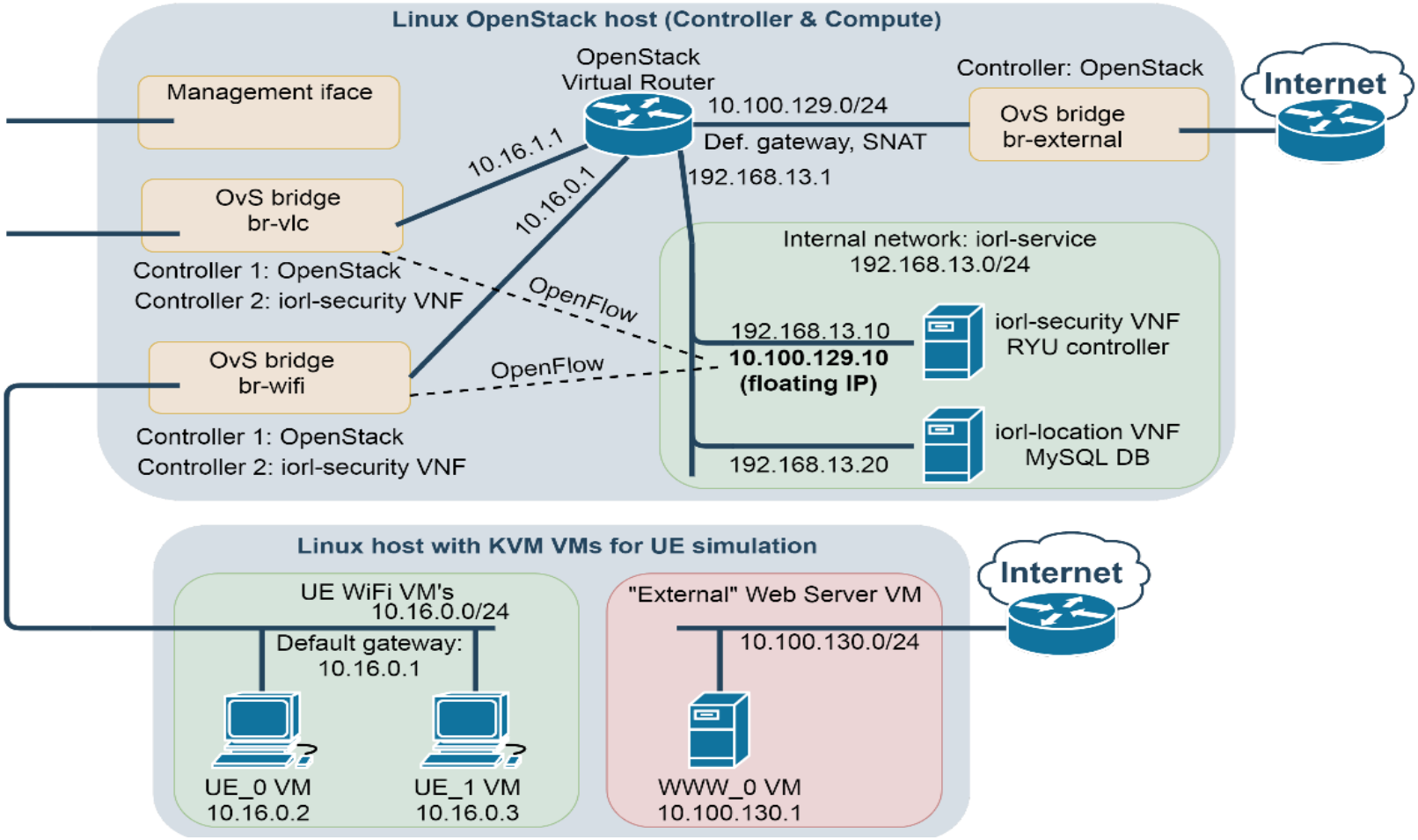
- RYU SDN controller automatically monitors, intercepts and blocks malicious traffic passing through the Open vSwitch,
- Security web dashboard administrators can view detected security issues, enable/disable modules and alter their configuration,
- Integration with IoRL location service. Dashboard can report location of malicious devices by querying IoRL location database.

Mitigation against common attacks across multiple network layers and more

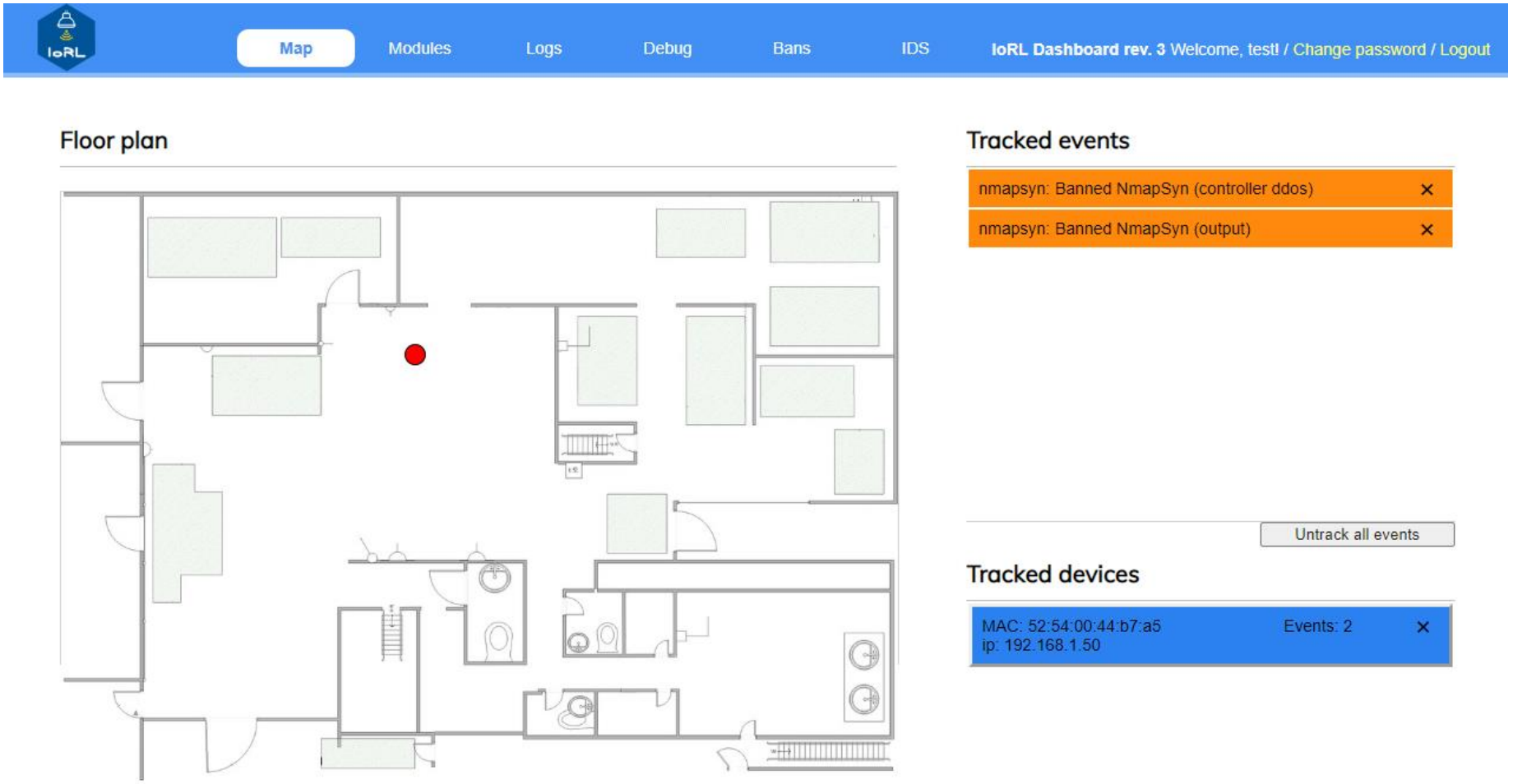
- TCP SYN port scan (Rogue transmitter)
- DHCP server address pool exhaustion (Denial of Service)
- Traffic sniffing (Eavesdropping)
- IP address spoofing (Rogue transmitter)

- **Modules added during 6 months extension:**
- Generic network traffic filtering via firewall rules,
- DoS attacks against SDN controller,
- Integrated Intrusion Detection System

Architecture

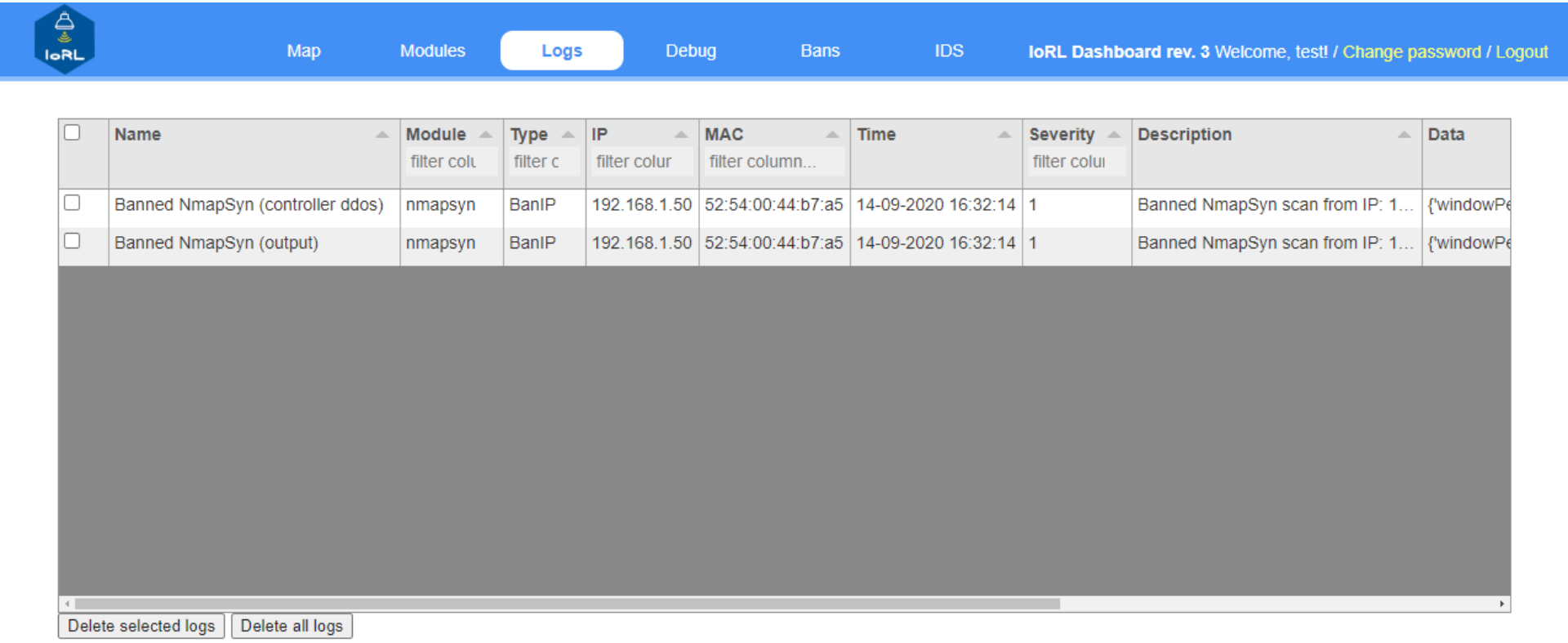


Main screen of the dashboard

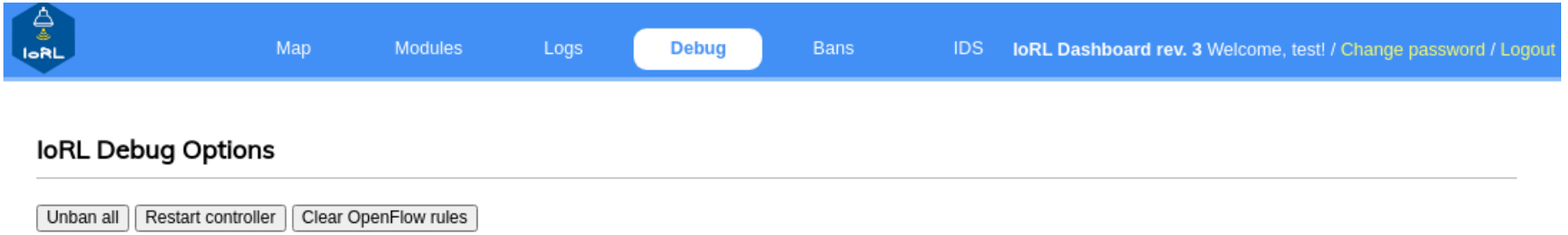


Modules configuration

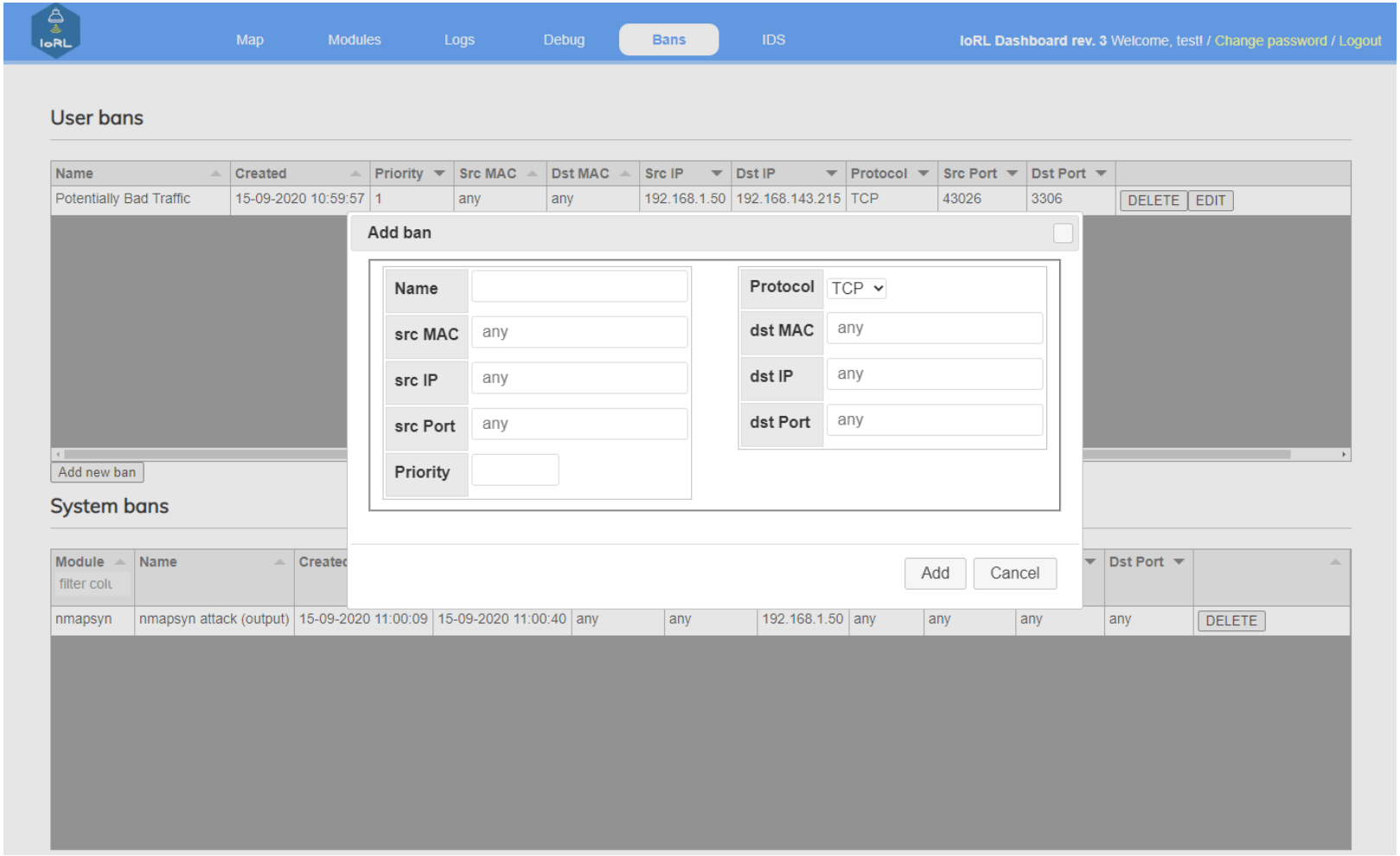
Log screen of the dashboard



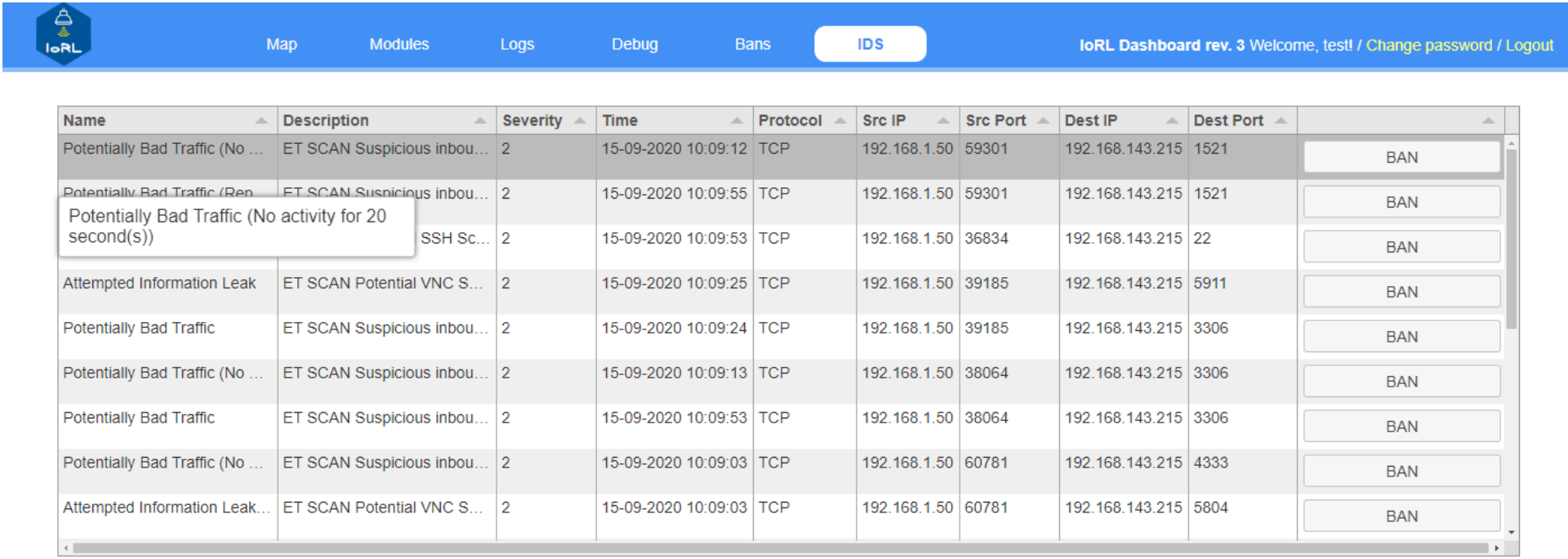
Debug Options



Bans and firewall functionality

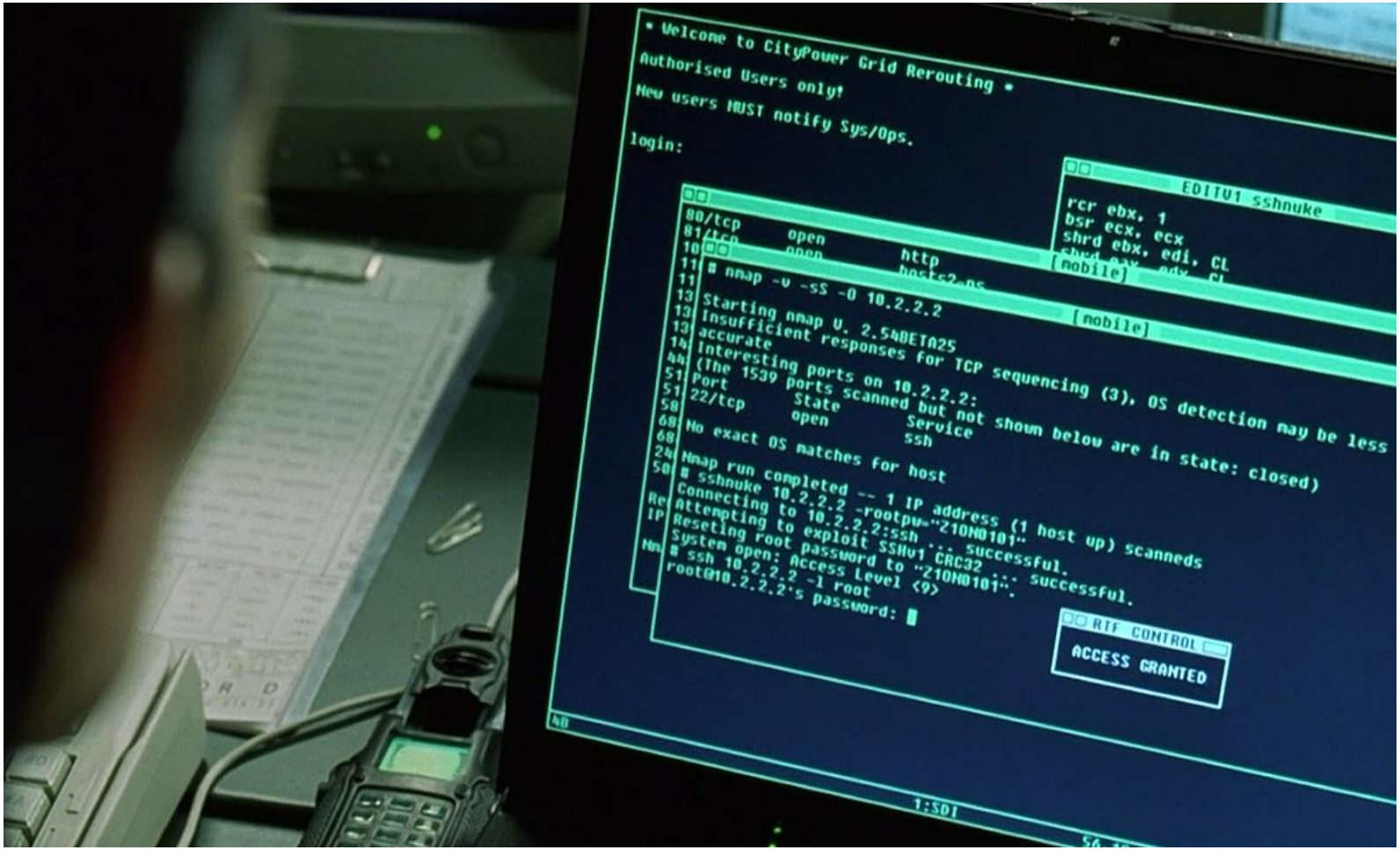


IDS module - Suricata



Name	Description	Severity	Time	Protocol	Src IP	Src Port	Dest IP	Dest Port	
Potentially Bad Traffic (No ...	ET SCAN Suspicious inbou...	2	15-09-2020 10:09:12	TCP	192.168.1.50	59301	192.168.143.215	1521	BAN
Potentially Bad Traffic (Rep...	ET SCAN Suspicious inbou...	2	15-09-2020 10:09:55	TCP	192.168.1.50	59301	192.168.143.215	1521	BAN
	SSH Sc...	2	15-09-2020 10:09:53	TCP	192.168.1.50	36834	192.168.143.215	22	BAN
Attempted Information Leak	ET SCAN Potential VNC S...	2	15-09-2020 10:09:25	TCP	192.168.1.50	39185	192.168.143.215	5911	BAN
Potentially Bad Traffic	ET SCAN Suspicious inbou...	2	15-09-2020 10:09:24	TCP	192.168.1.50	39185	192.168.143.215	3306	BAN
Potentially Bad Traffic (No ...	ET SCAN Suspicious inbou...	2	15-09-2020 10:09:13	TCP	192.168.1.50	38064	192.168.143.215	3306	BAN
Potentially Bad Traffic	ET SCAN Suspicious inbou...	2	15-09-2020 10:09:53	TCP	192.168.1.50	38064	192.168.143.215	3306	BAN
Potentially Bad Traffic (No ...	ET SCAN Suspicious inbou...	2	15-09-2020 10:09:03	TCP	192.168.1.50	60781	192.168.143.215	4333	BAN
Attempted Information Leak...	ET SCAN Potential VNC S...	2	15-09-2020 10:09:03	TCP	192.168.1.50	60781	192.168.143.215	5804	BAN

“Matrix Reloaded”



ISF in action – nmap module disabled

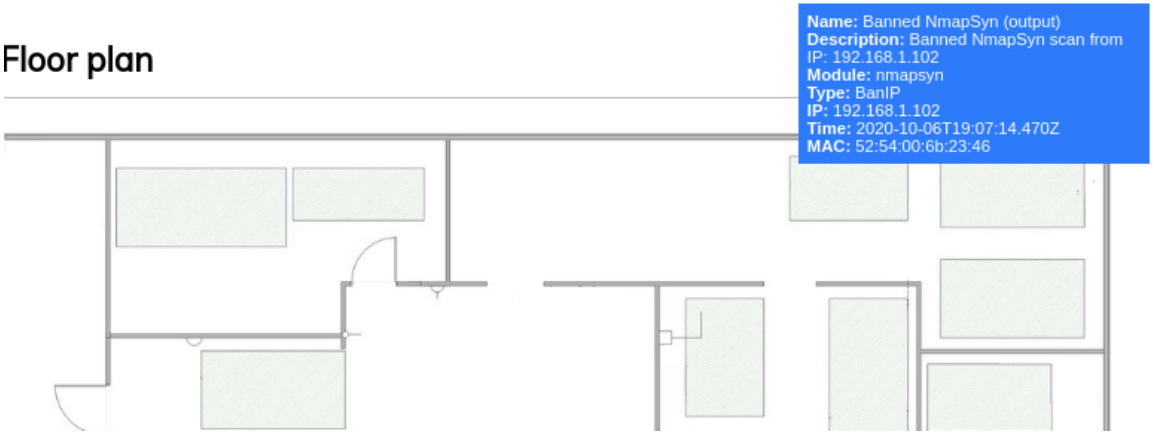
```
root@ue2:~# time nmap -Pn  -p- 192.168.143.215 -n -T5 -e eth1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-06 20:46 CEST
Nmap scan report for 192.168.143.215
Host is up (0.00020s latency).
Not shown: 65509 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2379/tcp  open  etcd-client
2380/tcp  open  etcd-server
3260/tcp  open  iscsi
3306/tcp  open  mysql
4369/tcp  open  epmd
5000/tcp  open  upnp
5672/tcp  open  amqp
5900/tcp  open  vnc
5901/tcp  open  vnc-1
5902/tcp  open  vnc-2
5903/tcp  open  vnc-3

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds

real        0m0,850s
```

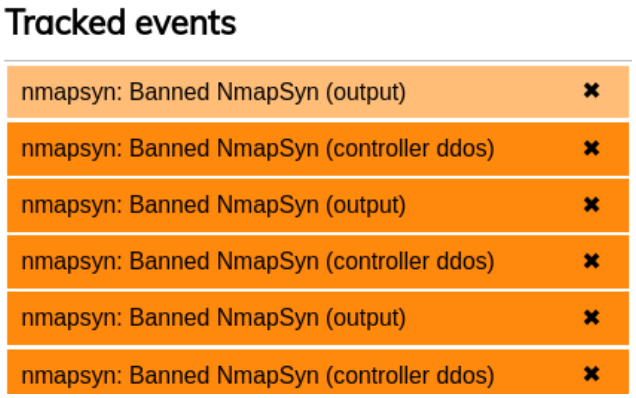
- Scanning completed in less than a second
- Reported open ports can be used to perform further exploitation

ISF in action – nmap module enabled

root@ue2:~# time nmap -Pn -v -p- 192.168.143.215 -n -T5 -e eth1
Starting Nmap 7.80 (https://nmap.org) at 2020-10-06 21:04 CEST
Initiating SYN Stealth Scan at 21:04
Scanning 192.168.143.215 [65535 ports]
SYN Stealth Scan Timing: About 0.92% done
*SYN Stealth Scan Timing: About 1.83% done; ETC: 22:00 (**0:54:30 remaining**)*
...Stopped...
real 2m19,767s

- No open ports reported
- About 1 hour for the same activity





Papers published - nmapsyn module

- Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech [et al.] : SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System, in: ARES 2018 Proceedings of the 13th International Conference on Availability, Reliability and Security / Doerr Christian, Schrittwieser Sebastian, Weippl Edgar (eds.), 2018, ISBN 978-1-4503-6448-5, pp. 1-10, DOI:10.1145/3230833.3233248
- Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech [et al.] : Network Threats Mitigation Using Software-Defined Networking for the 5G Internet of Radio Light System, in: Security and Communication Networks, vol. 2019, 2019, pp. 1-22, DOI:10.1155/2019/4930908

dhcpstarv module

- DHCP is one of the most ubiquitous services.
- An attacker can exhaust pool of available addresses – new users/devices cannot connect to the network.
- Can be annoying, but also dangerous.
- This is a type of DoS – Denial of Service attack.
- Our module successfully protect the DHCP server by using an algorithm developed for IoRL project.
- **Paper published:**
- Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech [et al.] : Network Threats Mitigation Using Software-Defined Networking for the 5G Internet of Radio Light System, in: Security and Communication Networks, vol. 2019, 2019, pp. 1-22, DOI:10.1155/2019/4930908

sniffdetdns module

- Eavesdropping is usually one of the first phases of network reconnaissance performed by an attacker.
- The aim is to discover network topology, services, protocols that are in use, but also capture unsecured credentials or other sensitive data.
- Two detection methods proposed, one utilizing AI
- **Papers published:**
- Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech [et al.] : Sniffing Detection within the Network, in: Proceedings of the 14th International Conference on Availability, Reliability and Security - Ares 2019, ICPS, 2019, ISBN 978-1-4503-7164-3, pp. 1-8, DOI:10.1145/3339252.3341494
- Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech [et al.] : Sniffing Detection within the Network, in: Proceedings of the 14th International Conference on Availability, Reliability and Security - Ares 2019, ICPS, 2019, ISBN 978-1-4503-7164-3, pp. 1-8, DOI:10.1145/3339252.3341494

arpfilter and ipfilter modules

- Simple modules allowing filtering ARP requests and IP packets with invalid IP source address
- Valid network addresses are provided using dashboard
- Rogue devices may not be able to exploit such network

„Extra” modules – 6 month extension

- Firewall – implemented withing SDN, allows to filter traffic based 3 and 4 OSI layers. Network elements can be protected and separated each other. Can be further utilized by other modules, if developed.
- Suricata – well-known open-source Intrusion Detection System can be used to monitor traffic within the network and report malicious activities. Additionally, an operator can ban such traffic easily in the Dashboard.

„Extra” modules – 6 month extension

- SDN as next-generation network, provides many benefits.
- It is a core of cloud computing and modern data-centers.
- New design of managing the network.
- Provides new elements that can be exploited.
- Module within ISF can countermeasure DoS attacks to SDN-specific infrastructure.
- **Paper published:**
- Nowakowski Piotr, Żórawski Piotr, Cabaj Krzysztof [et al.] : Distributed packet inspection for network security purposes in software-defined networking environments, in: ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, ISBN 978-1-4503-8833-7, pp. 1-7, Article number:106, DOI:10.1145/3407023.3409210

Summary

- WUT provided required security modules for the IoRL project
- Additional modules were developed and implemented during 6 months extension
- Dashboard is integrated with IoRL location service

Acknowledgement and disclaimer

- This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 761992, project IoRL.

- This presentation reflects the author's view, only, and the Commission is not responsible for any use that may be made of the information provided.

Thank you for your attention

m.gregorczyk@tele.pw.edu.pl and IoRL-contact@5g-ppp.eu

https://iorl.5g-ppp.eu/

IoRL partners

EURESCOM

Brunel University London

COBHAM

isep
École d'ingénieurs du numérique

MostlyTek

issymedia
Communication & Innovation

bre

Fraunhofer IIS

VIOTECH

arçelik

RunEL
NGMT-Next Generation Mobile Technology

HIT
מכון טכנולוגי חולון
Holon Institute of Technology

ferrovial
agroman

OLEDCOMM

LEADPCOM

IINESA
FACS
飞乐音响

centro de innovación de infraestructuras inteligentes