Hacking with Wireshark

Presenter: Stan Overgauw
Organization: Rabobank Red Team

Who am I?

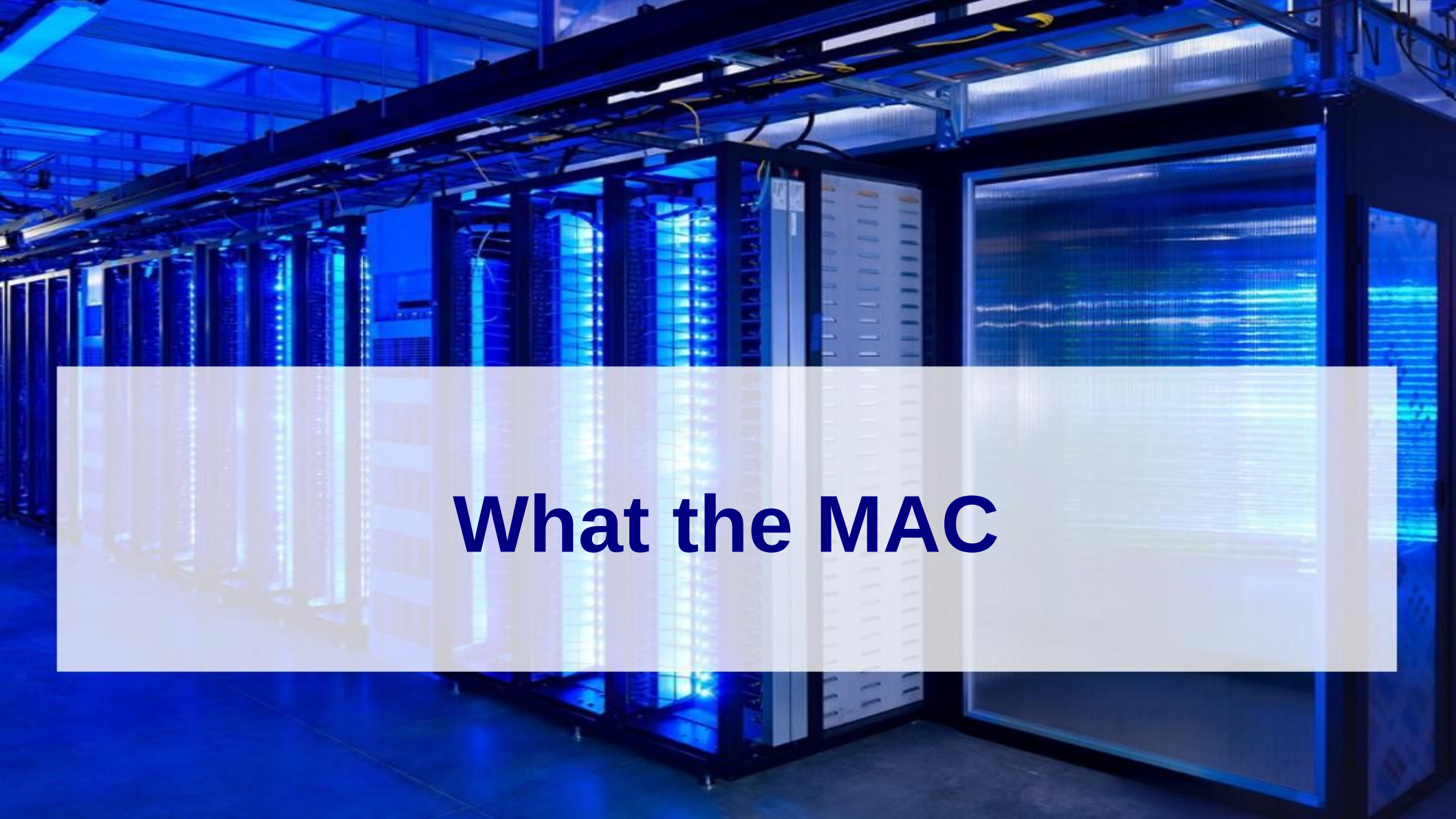
- Red Teamer
- Ethical Hacker
- 25
- 3+ years at Rabobank Red Team
- What is Red Teaming?

Red teaming?

A red team goes a step further, and adds physical penetration, social engineering, and an element of surprise. The blue team is given no advance warning of a red team, and will treat it as a real intrusion. A red-team assessment is similar to a penetration test, but is more targeted. The goal is to test the organization's detection and response capabilities. The red team will try to get in and access sensitive information in any way possible, as quietly as possible.

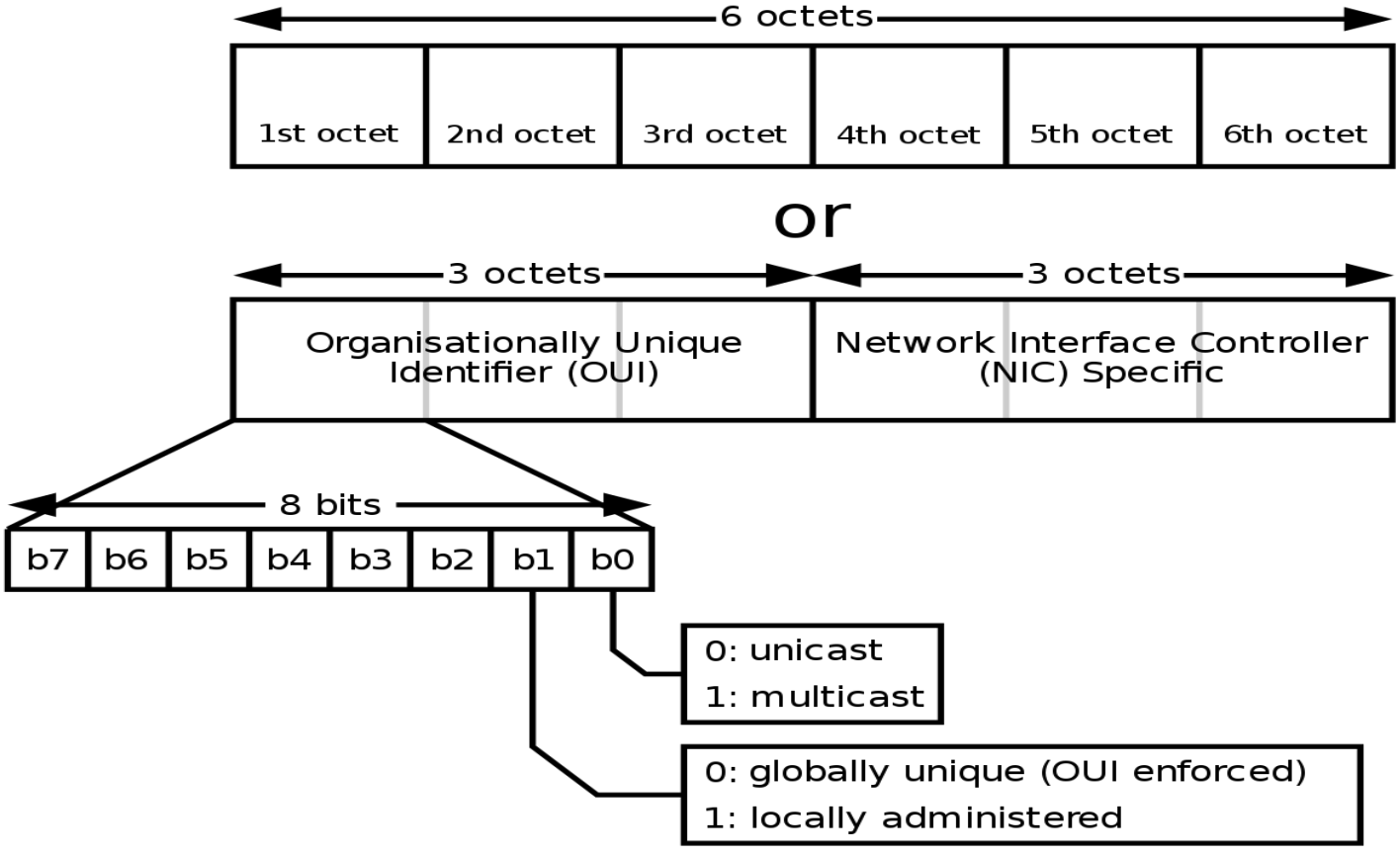
TODO:

- Social engineering based on MAC Address
- Vulnerability hunting with LLDP
- Why SSL/TLS offloading can be a bad idea



What the MAC

What a mac can tell us



What a mac can tell us

Ex:

48-73-97-85-c7-69 → New H3c Tech Co, Ltd

Sells “Full-Scenario Finance Cloud Solution” based on H3Cloud OS → CVE-2019-12193

Or: 84:39:8F:23:24:19 →Fortinet, Inc → CVE-2022-42475 → Unauthenticated RCE on FortiOs VPN

Can you figure this one out:

64:51:77:34:77:39

57:67:58:63:51:0A

Switch to https://

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Articles

External Links :

NVD Website

CWE Web Site

Fortinet : Vulnerability Statistics

Products (242) Vulnerabilities (497) Search for products of Fortinet CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

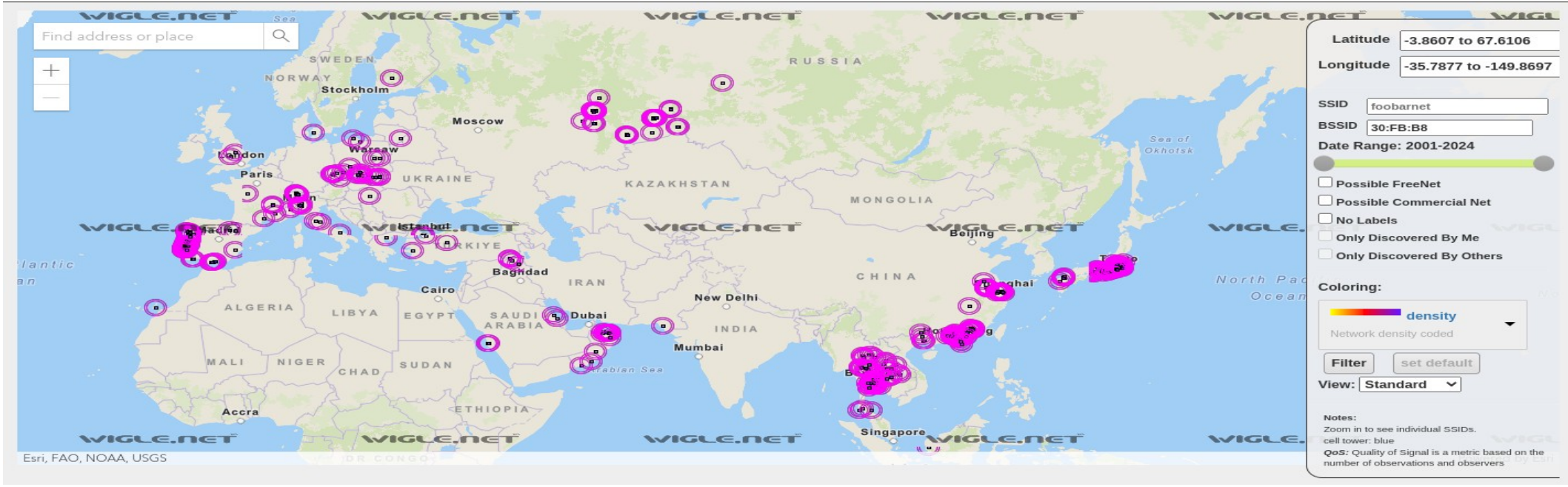
Vulnerability Feeds & Widgets

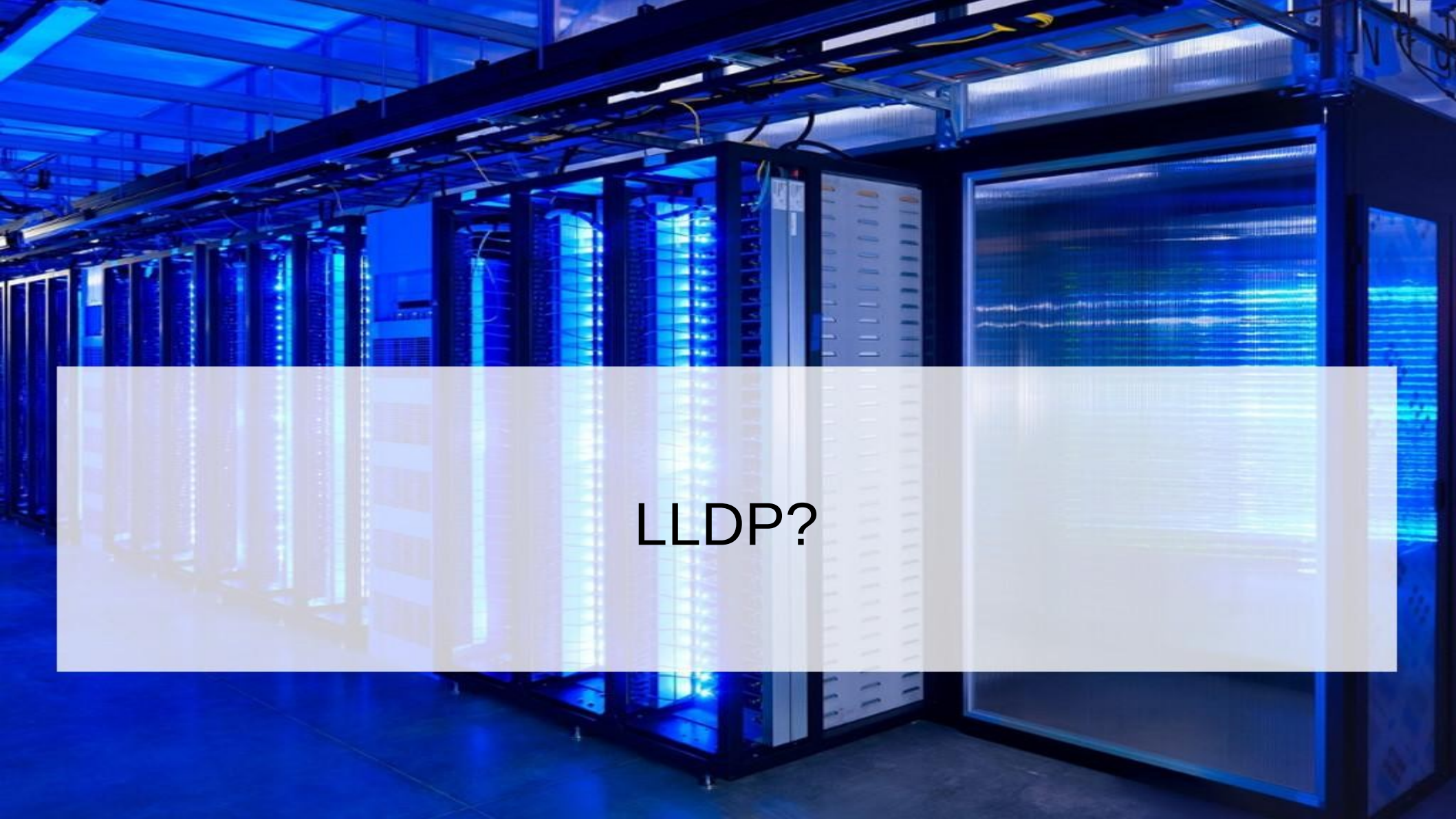
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2005	6	1								4		1			
2006	2	1								1					
2008	1		1												
2009	2		1							1					
2012	18									17					
2013	1														
2014	14	1	1				8		1		1	2	1		
2015	28	1	2	1			10			1	4	1			
2016	17		2	1			6	1			3	1	1		
2017	39	1	15				16				8	3	1		
2018	20		3				7			1	3		1		1
2019	37	1	15	2			8	1		1	4				
2020	45	2	2	1			13				3	4	1		
2021	121	9	38	15		6	15	5	1	8	4	3	1		
2022	104	1	32	4		7	16	7		6	4	2			
2023	42	1	16	8			5	5	2						
Total	497	19	128	32		13	104	19	4	40	34	17	6		1
% Of All		3.8	25.8	6.4	0.0	2.6	20.9	3.8	0.8	8.0	6.8	3.4	1.2	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

What a mac can tell us





LLDP?

LLDP

Demo?

LLDP

```
▾ Frame 15: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface enp0s20f0u2u1, id 0
    Section number: 1
  ▸ Interface id: 0 (enp0s20f0u2u1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 21, 2023 15:33:35.948787851 CET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1676990015.948787851 seconds
    [Time delta from previous captured frame: 1.010365738 seconds]
    [Time delta from previous displayed frame: 1.010365738 seconds]
    [Time since reference or first frame: 51.533352872 seconds]
    Frame Number: 15
    Frame Length: 97 bytes (776 bits)
    Capture Length: 97 bytes (776 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:lldp]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
▾ Ethernet II, Src: Ubiquiti_27:61:4f (e0:63:da:27:61:4f), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
  ▸ Destination: LLDP_Multicast (01:80:c2:00:00:0e)
  ▸ Source: Ubiquiti_27:61:4f (e0:63:da:27:61:4f)
    Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)
    Trailer: 040000
▾ Link Layer Discovery Protocol
  ▸ Chassis Subtype = MAC address, Id: e0:63:da:27:61:4e
  ▸ Port Subtype = Locally assigned, Id: Port 2
  ▸ Time To Live = 120 sec
  ▸ Port Description = Port 2
  ▸ System Name = Switch
  ▸ System Description = US-8-60W, 5.64.8.13083, Linux 3.6.5
  ▸ Capabilities
  ▸ End of LLDPDU
```

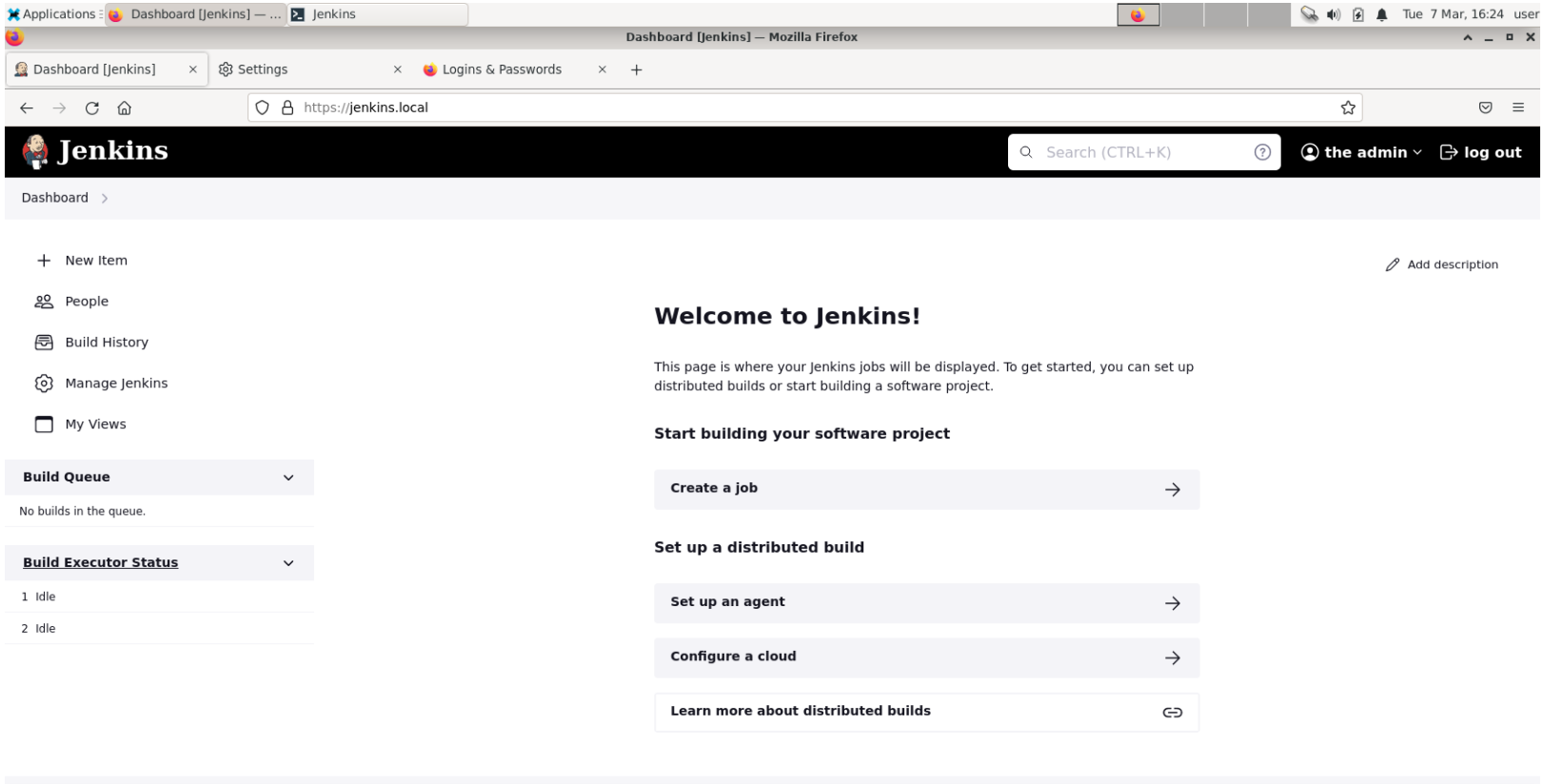
US-8-60W, 5.64.8.13083, Linux 3.6.5

SSL/TLS offloading

Demo

- Server < http > Loadbalancer < https > client
- Loadbalancer setup at 5pm on a Friday while WFH
-

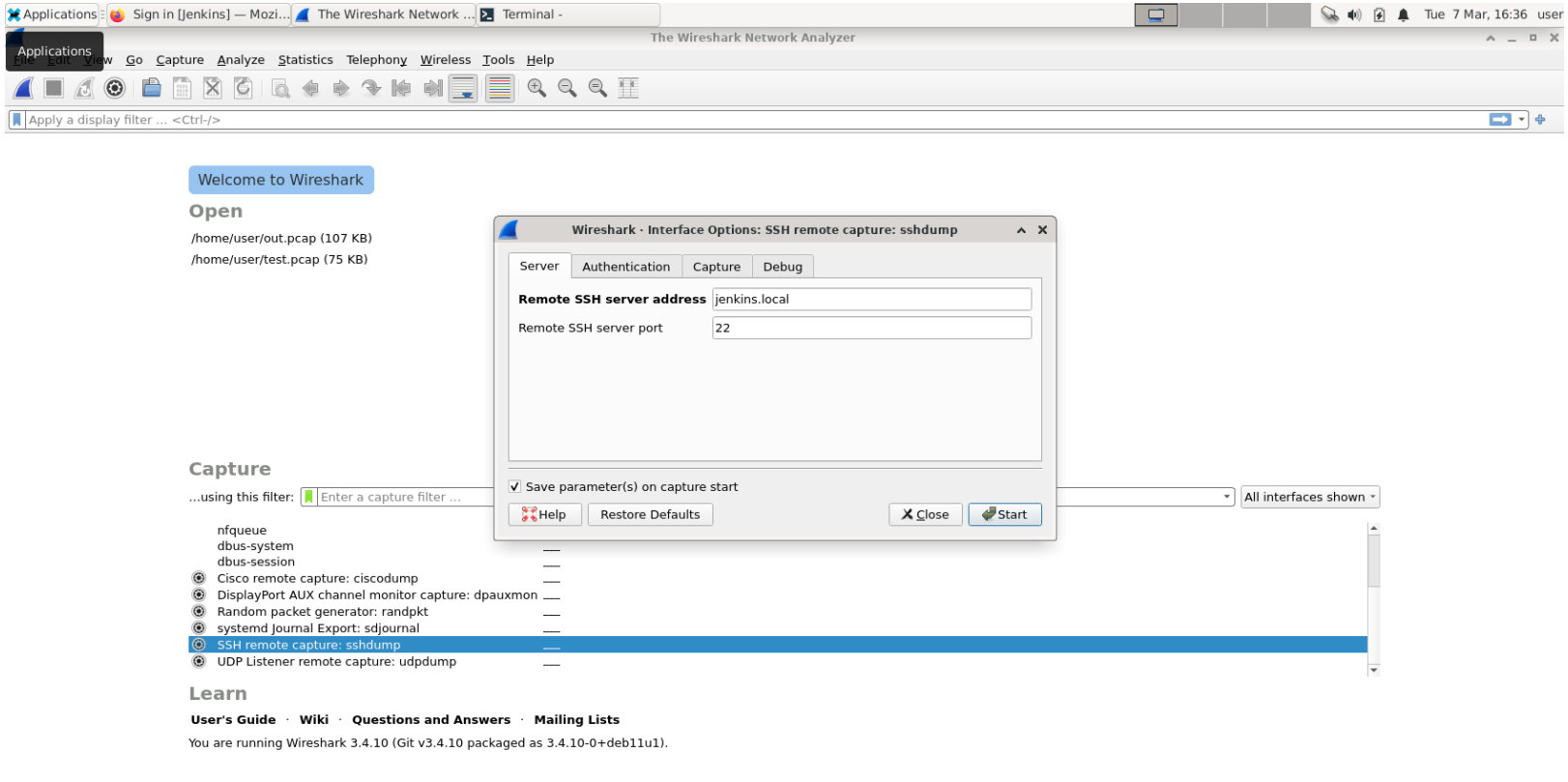
Demo



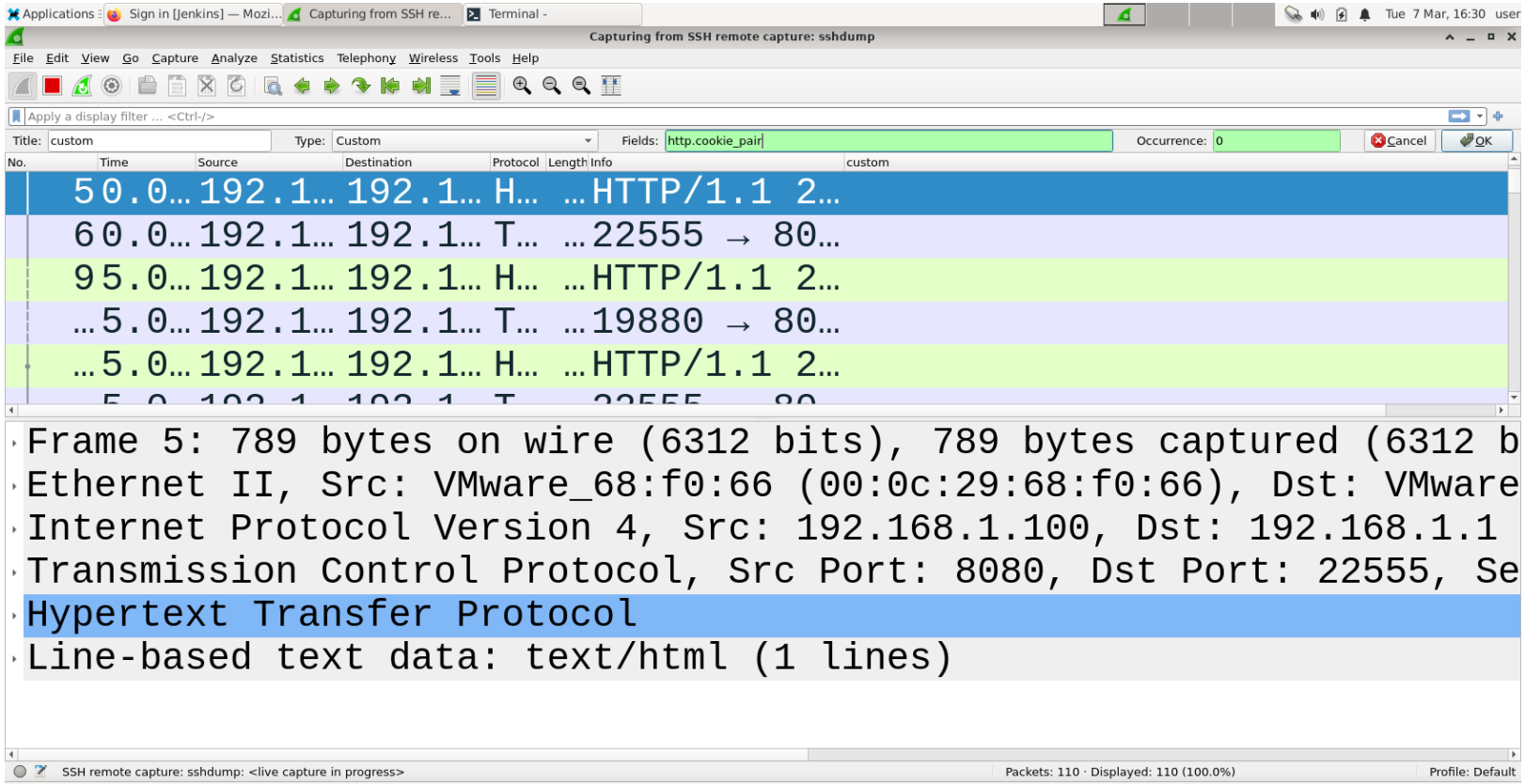
I AM THE SERVER

```
Desktop$ ssh admin@jenkins.local
Password for admin@pfSense.home.arpa:
VMware Virtual Machine - Netgate Device ID: 1c42bf11e8ae1fe29384

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.16.141.129/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

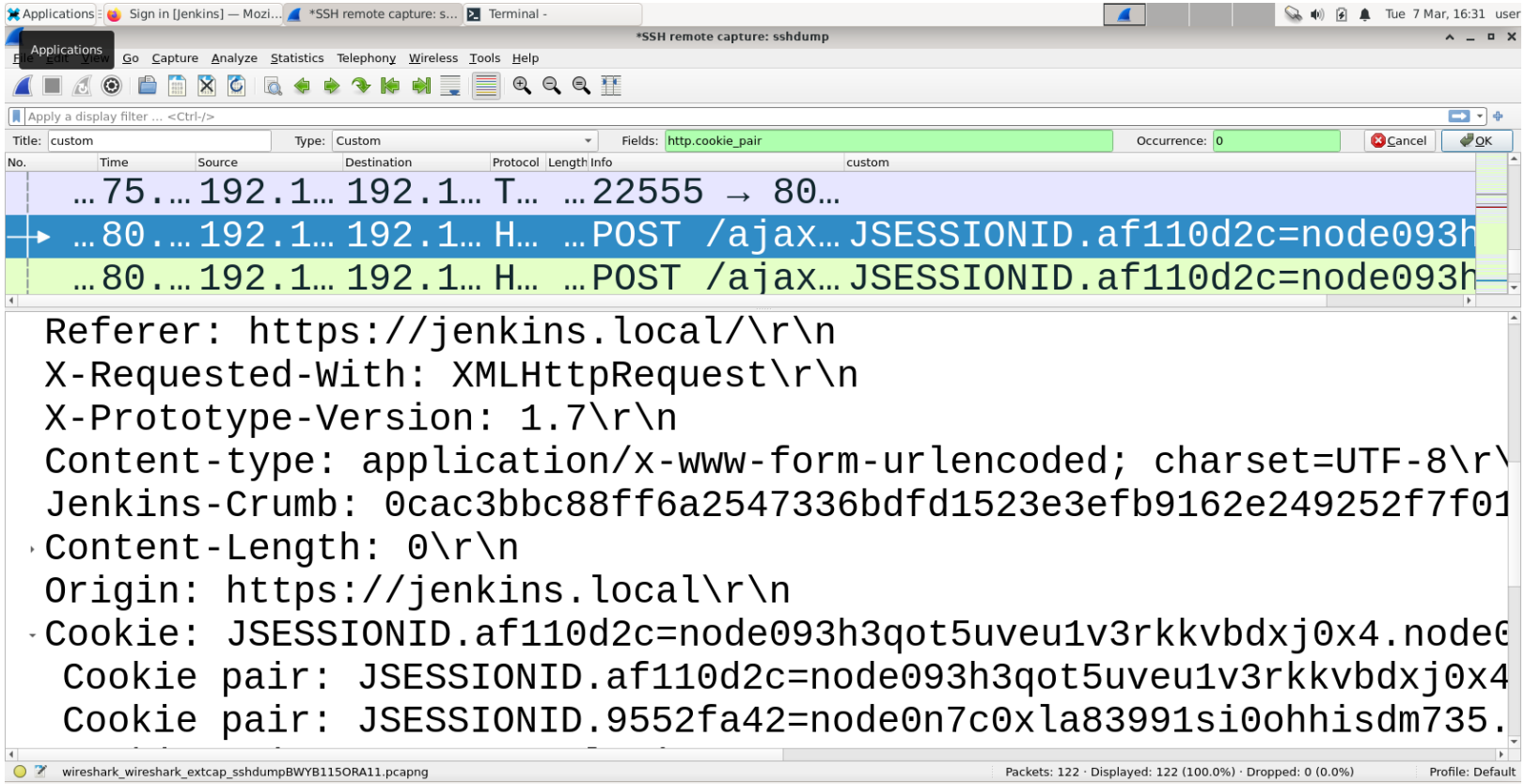
I AM THE HACKER



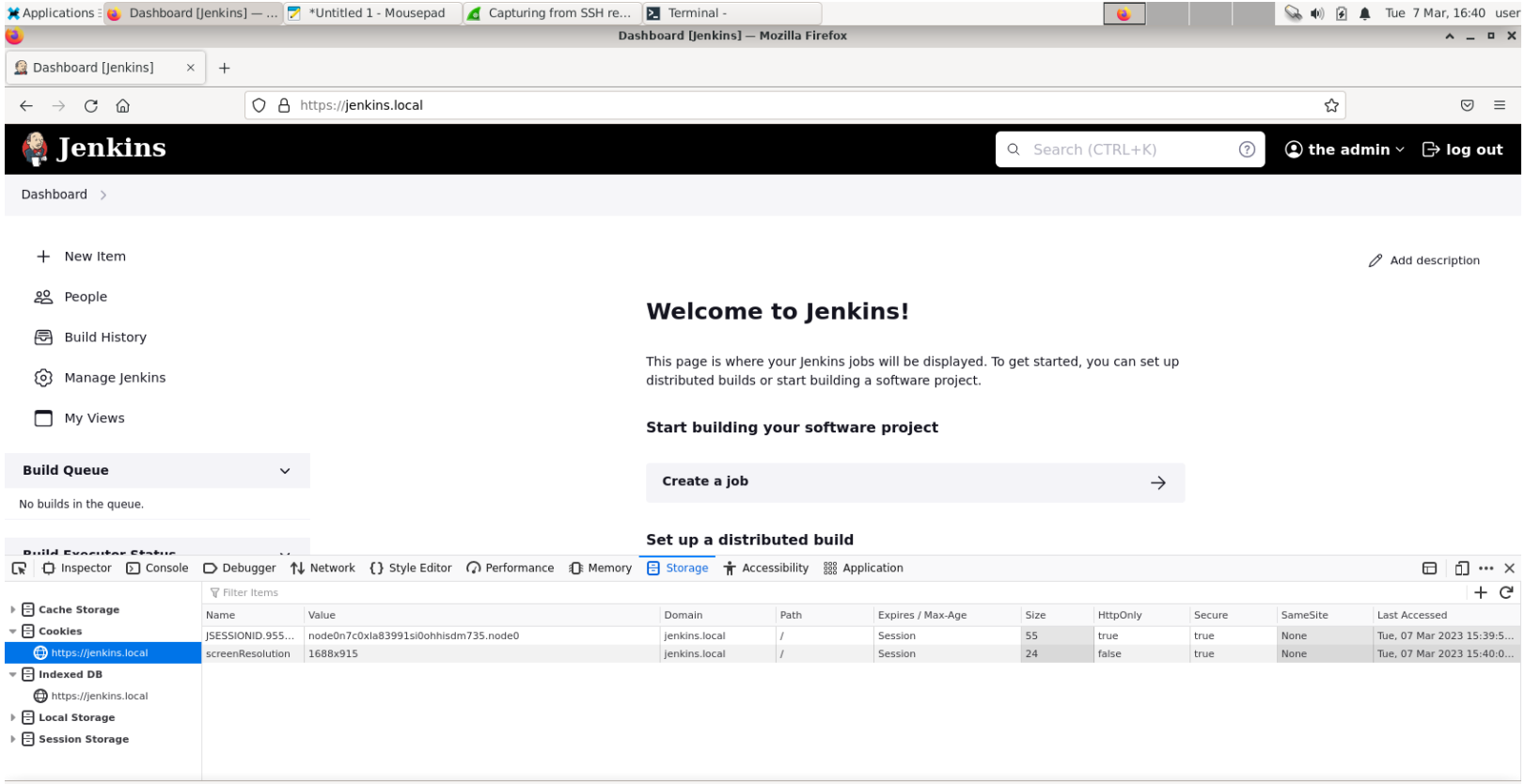
I AM THE HACKER



I AM THE HACKER



I AM THE HACKER



I AM THE HACKER

DONT USE SUDO WITH TCPDUMP/TSHARK !!!!1111!!!!1111!!!!!111!!1!1!!!!

dumping to multiple files

```
-- Create a file named by_ip/''ip_addess''.cap with all ip traffic of each ip host. (tsha
-- Dump files are created for both source and destination hosts
function createDir (dirname)
    -- this will print out an error if the directory already exists, but that's fine
    os.execute("mkdir " .. dirname)
end

```

-z *postrotate-command*

Used in conjunction with the **-C** or **-G** options, this will make *tcpdump* run " *postrotate-command file* " where *file* is the savefile being closed after each rotation. For example, specifying **-z gzip** or **-z bzip2** will compress each savefile using gzip or bzip2.

Note that tcpdump will run the command in parallel to the capture, using the lowest priority so that this doesn't disturb the capture process.

And in case you would like to use a command that itself takes flags or different arguments, you can always write a shell script that will take the savefile name as the only argument, make the flags & arguments arrangements and execute the command that you want.

Questions?

Stan Overgauw
stan.overgauw@rabobank.nl