Site Report

Kashif Mohammad

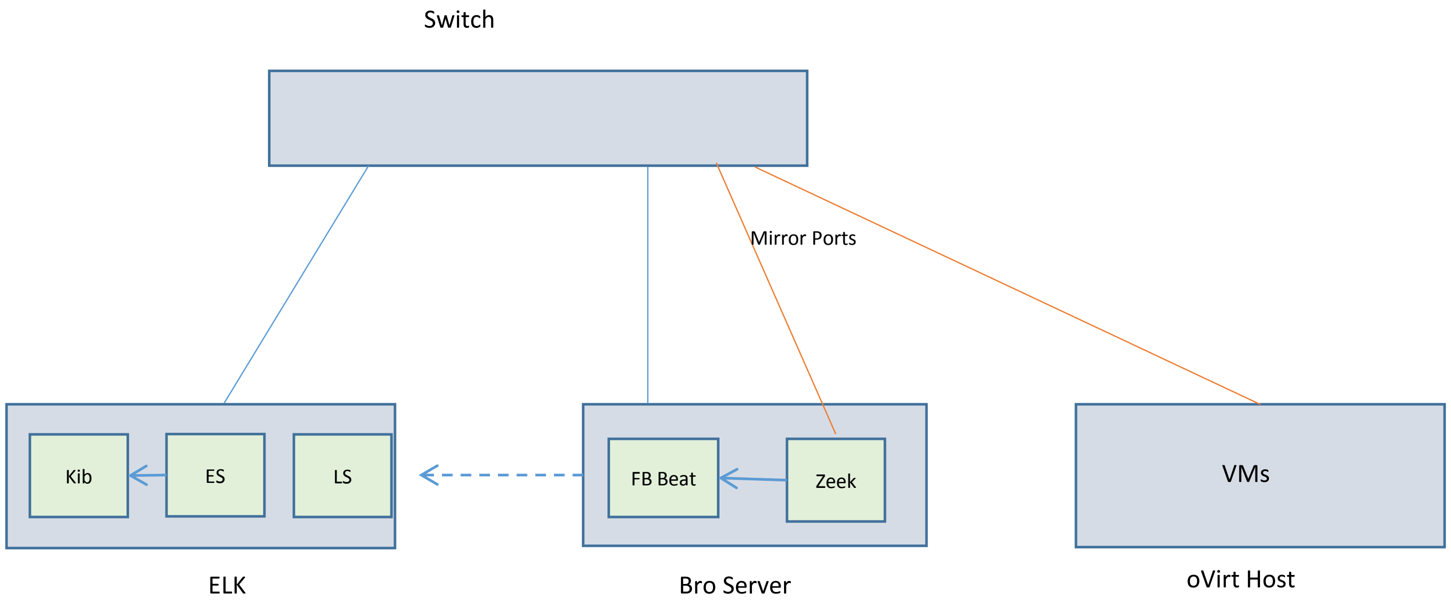
Department of Physics

University of Oxford

ZEEK and ELK

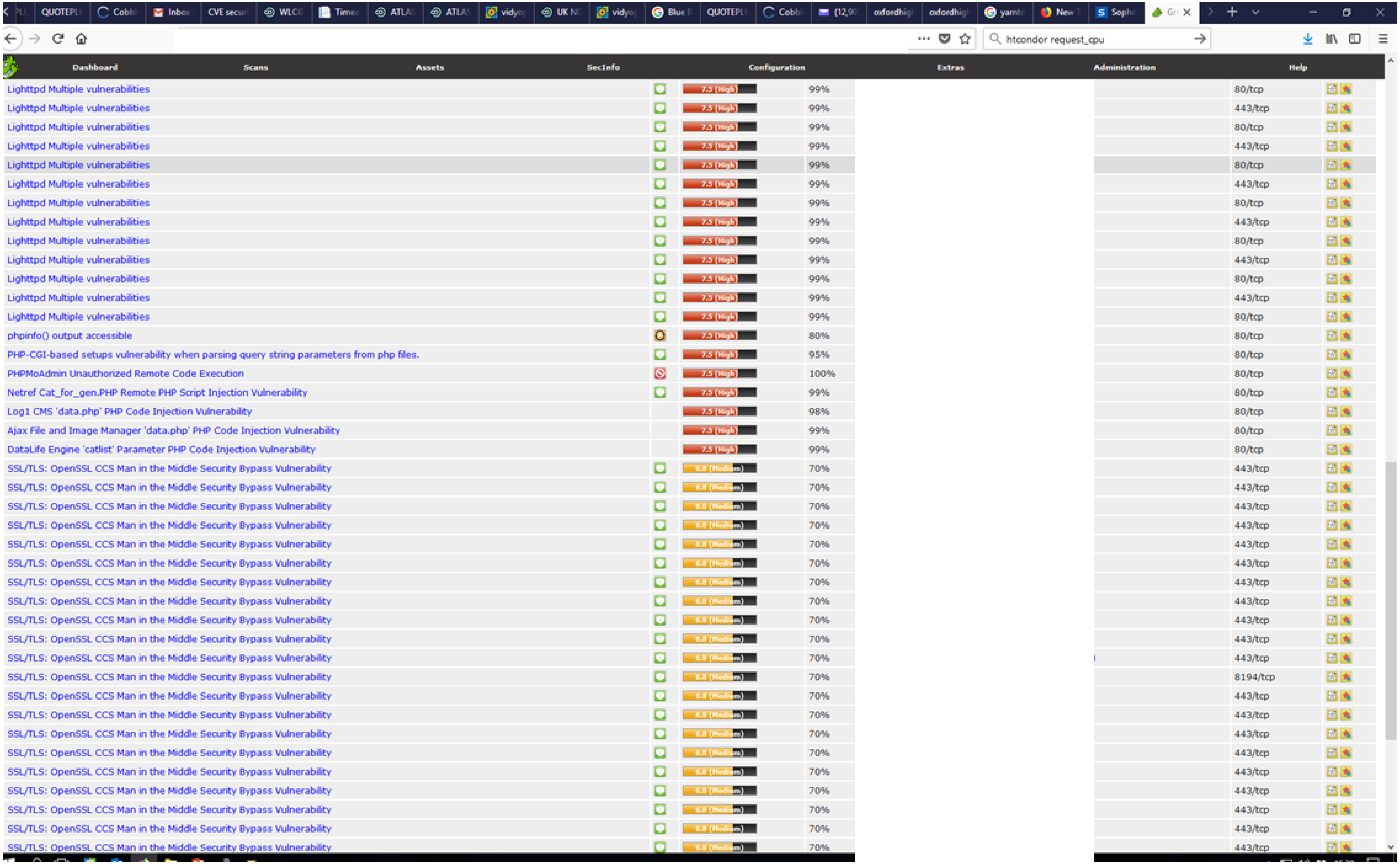
- Small setup of ZEEK and ELK
- Monitoring Grid Services through ZEEK
    - But not much interesting data
- Plan to monitor Physics department network
    - Waiting for network restructure
- Installed a MISP instance and long term plan is to integrate with ZEEK

ZEEK + ELK Setup



OpenVas

- Running OpenVas for Vulnerability Scanning
- Installed on top of Kali Linux
  - Mostly worked out of box
- We have quite a few vlans and subnets so scanning across network range takes too much time
- So running `nmap –sn <ip-range>` first and then feeding that list as input for openvas scan.
  - Much better



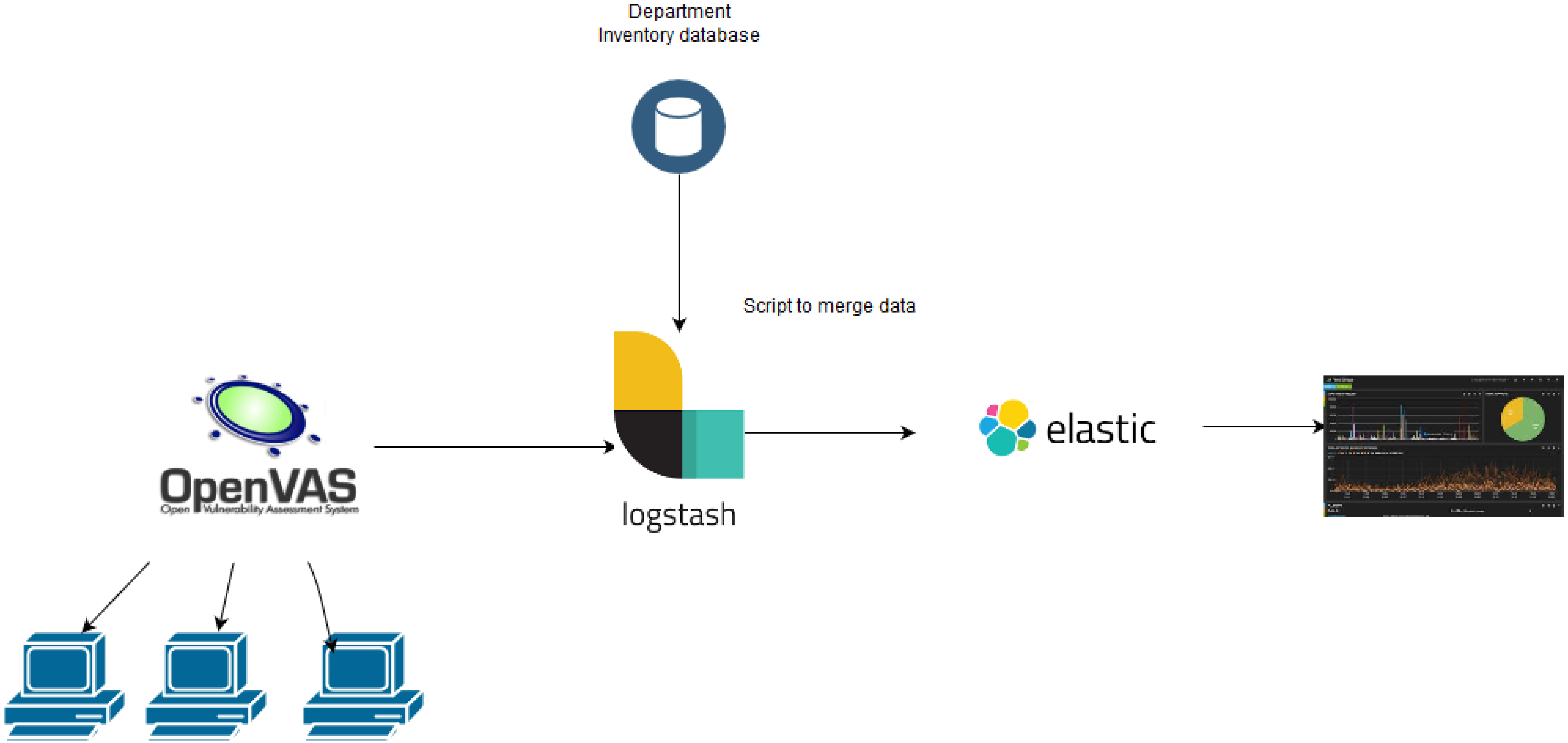
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	80/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	443/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	80/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	443/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	80/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	443/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	80/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	443/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	80/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	443/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	80/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	443/tcp
Lighttpd Multiple vulnerabilities	●	7.5 (High)	99%	80/tcp
phpinfo() output accessible	◎	7.5 (High)	80%	80/tcp
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	●	7.5 (High)	95%	80/tcp
PHPMoAdmin Unauthorized Remote Code Execution	⊘	7.5 (High)	100%	80/tcp
Netref Cat_for_gen.PHP Remote PHP Script Injection Vulnerability	●	7.5 (High)	99%	80/tcp
Log1 CMS 'data.php' PHP Code Injection Vulnerability		7.5 (High)	98%	80/tcp
Ajax File and Image Manager 'data.php' PHP Code Injection Vulnerability		7.5 (High)	99%	80/tcp
DataLife Engine 'catlist' Parameter PHP Code Injection Vulnerability		7.5 (High)	99%	80/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	8194/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	●	6.8 (Medium)	70%	443/tcp

OpenVas

- Quite satisfy with the tool
  - Completely free
  - Active mailing list
- Reporting is not very intuitive and can be difficult to navigate
  - 100 page PDF reports
- Fair number of false positives
- Can be unstable
  - Problem might be at my end

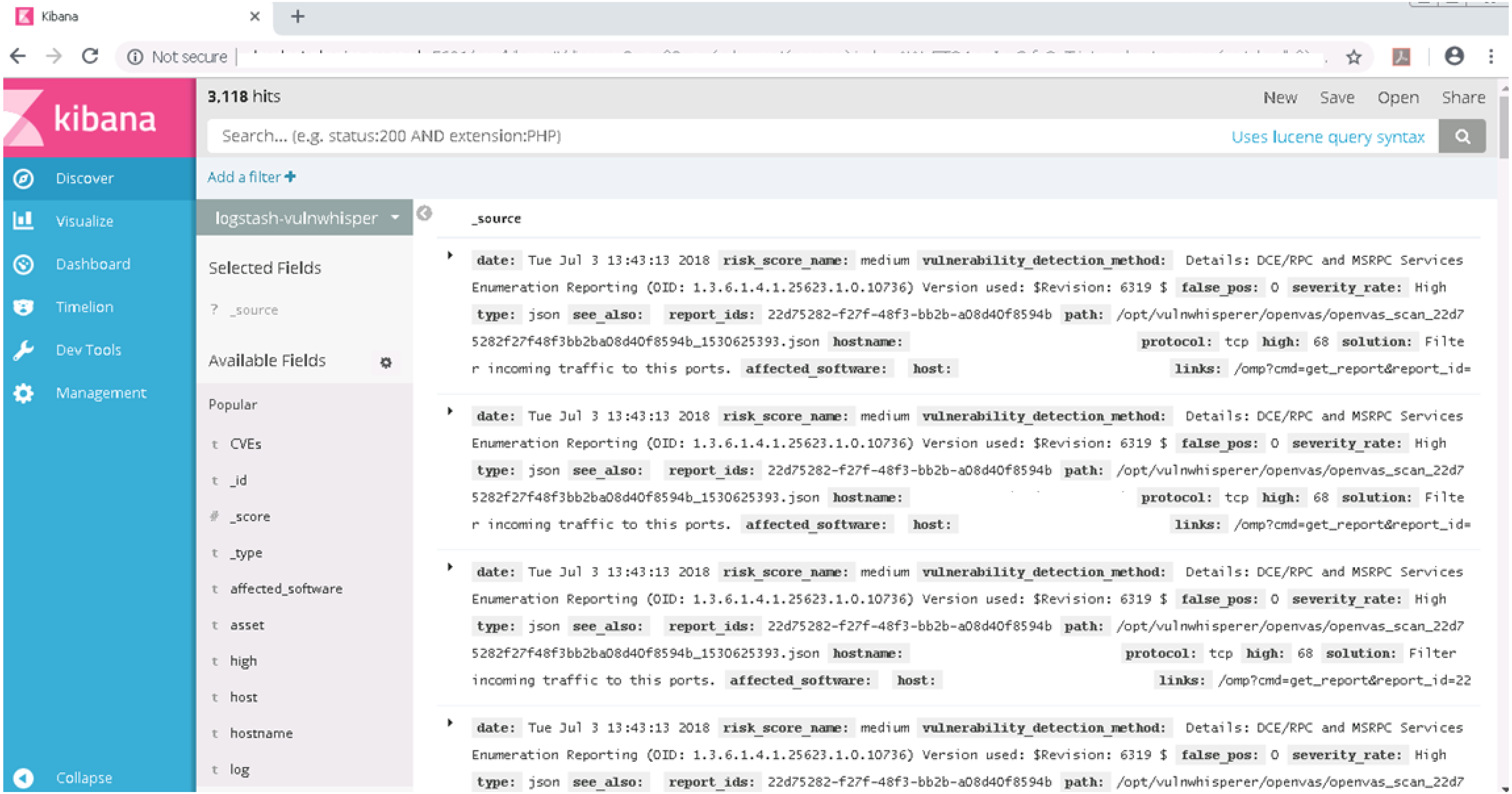
What We Want

- Classify nodes on basis of types
  - Servers, Desktop, DAQ, Switches, Network attached devices
- Classify on basis of ownership structures
  - Sub-department, web admin, desktop admin
- Classify on basis of data sensitivity
- Status over the time



Department
Inventory database

Script to merge data



3,118 hits

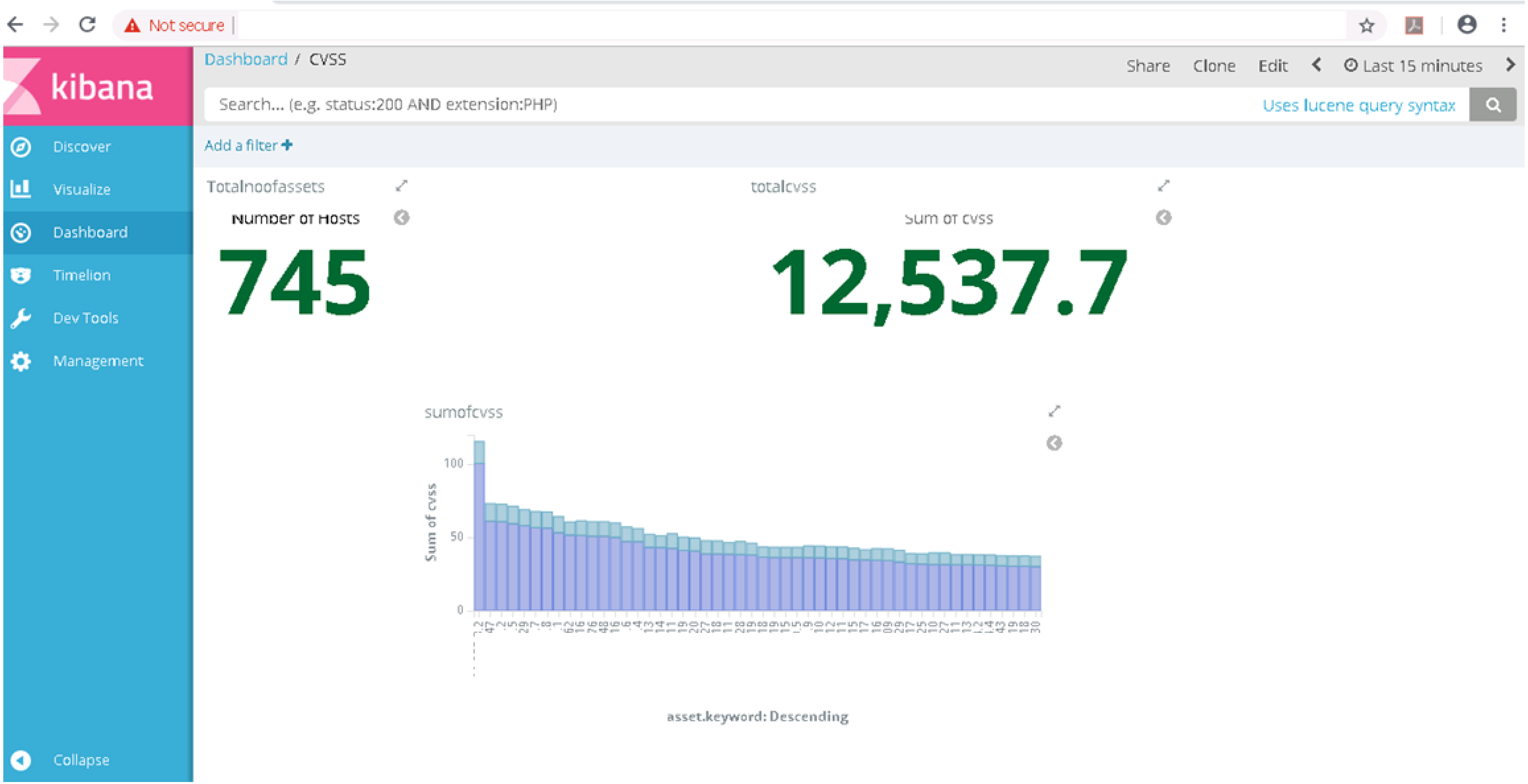
```
_source

date: Tue Jul 3 13:43:13 2018 risk_score_name: medium vulnerability_detection_method: Details: DCE/RPC and MSRPC Services
Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 6319 $ false_pos: 0 severity_rate: High
type: json see_also: report_ids: 22d75282-f27f-48f3-bb2b-a08d40f8594b path: /opt/vulnwhisperer/openvas/openvas_scan_22d7
5282f27f48f3bb2ba08d40f8594b_1530625393.json hostname:                 protocol: tcp high: 68 solution: Filte
r incoming traffic to this ports. affected_software: host:                 links: /omp?cmd=get_report&report_id=

date: Tue Jul 3 13:43:13 2018 risk_score_name: medium vulnerability_detection_method: Details: DCE/RPC and MSRPC Services
Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 6319 $ false_pos: 0 severity_rate: High
type: json see_also: report_ids: 22d75282-f27f-48f3-bb2b-a08d40f8594b path: /opt/vulnwhisperer/openvas/openvas_scan_22d7
5282f27f48f3bb2ba08d40f8594b_1530625393.json hostname:                 protocol: tcp high: 68 solution: Filte
r incoming traffic to this ports. affected_software: host:                 links: /omp?cmd=get_report&report_id=

date: Tue Jul 3 13:43:13 2018 risk_score_name: medium vulnerability_detection_method: Details: DCE/RPC and MSRPC Services
Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 6319 $ false_pos: 0 severity_rate: High
type: json see_also: report_ids: 22d75282-f27f-48f3-bb2b-a08d40f8594b path: /opt/vulnwhisperer/openvas/openvas_scan_22d7
5282f27f48f3bb2ba08d40f8594b_1530625393.json hostname:                 protocol: tcp high: 68 solution: Filter
incoming traffic to this ports. affected_software: host:                 links: /omp?cmd=get_report&report_id=22

date: Tue Jul 3 13:43:13 2018 risk_score_name: medium vulnerability_detection_method: Details: DCE/RPC and MSRPC Services
Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 6319 $ false_pos: 0 severity_rate: High
type: json see_also: report_ids: 22d75282-f27f-48f3-bb2b-a08d40f8594b path: /opt/vulnwhisperer/openvas/openvas_scan_22d7
```



Totalnoofassets

Number of Hosts

745

totalcvss

Sum of cvss

12,537.7