Name: Muhammad Usman Ali Sadiq

Cybersecurity

Task 1

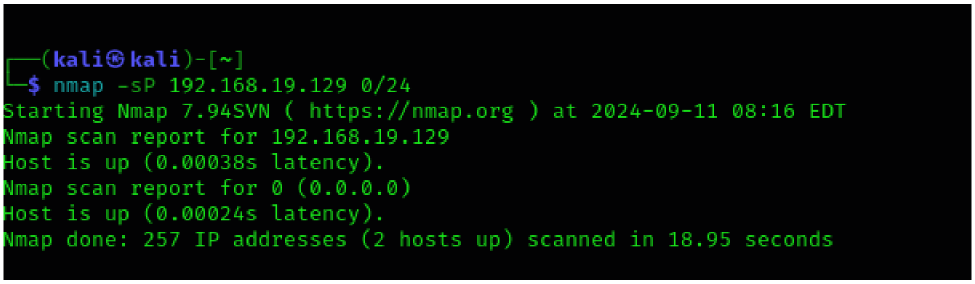
Conducting Security Audits

- **Conducting a risk assessment and identifying potential threats.**

Conduct a Risk Assessment

Identify Network Assets:

use **Nmap** to map the network



```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.19.129 0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 08:16 EDT
Nmap scan report for 192.168.19.129
Host is up (0.00038s latency).
Nmap scan report for 0 (0.0.0.0)
Host is up (0.00024s latency).
Nmap done: 257 IP addresses (2 hosts up) scanned in 18.95 seconds
```

This command scans and lists all devices on the local network.

Assess Threats:

For each asset, think about the possible threats.

- **Server**: Unauthorized access, SQL injection attacks.
- **Router**: Weak encryption, unpatched firmware vulnerabilities.
- **Workstations**: Malware, phishing attacks.

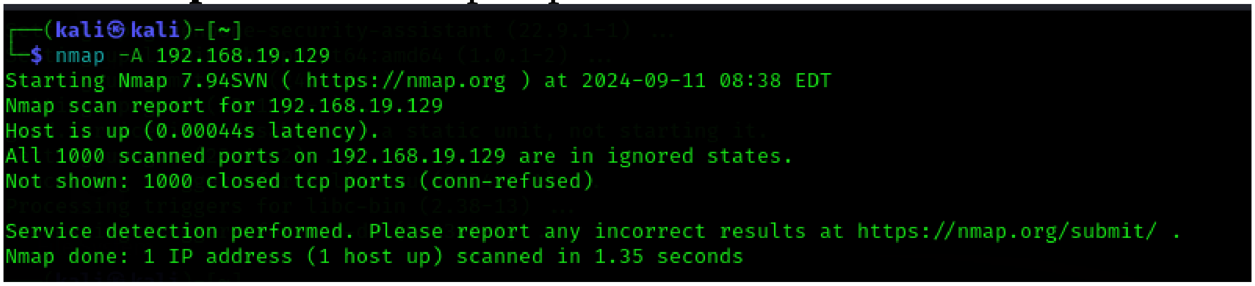
Risk Prioritization:

Use a simple risk matrix to prioritize threats based on their likelihood and impact.

➢ Use Tools to Scan for Vulnerabilities

Nmap for Network Scanning

Use **Nmap** to scan for open ports and services on the network

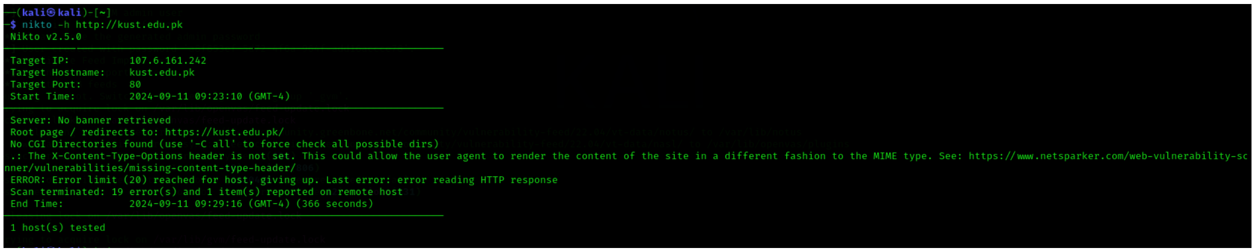


```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.19.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 08:38 EDT
Nmap scan report for 192.168.19.129
Host is up (0.00044s latency).
All 1000 scanned ports on 192.168.19.129 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

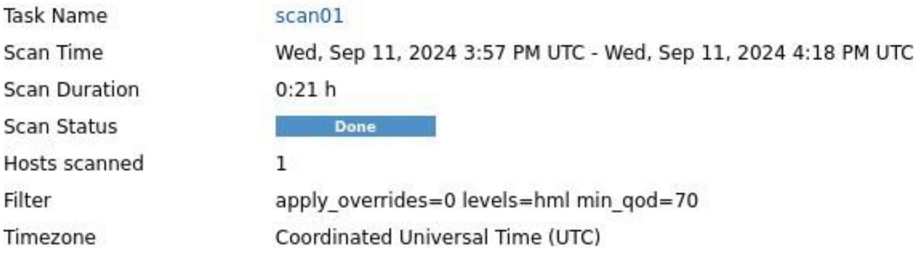
Nikto for Web Server Vulnerabilities

Use **Nikto** to scan web servers for vulnerabilities

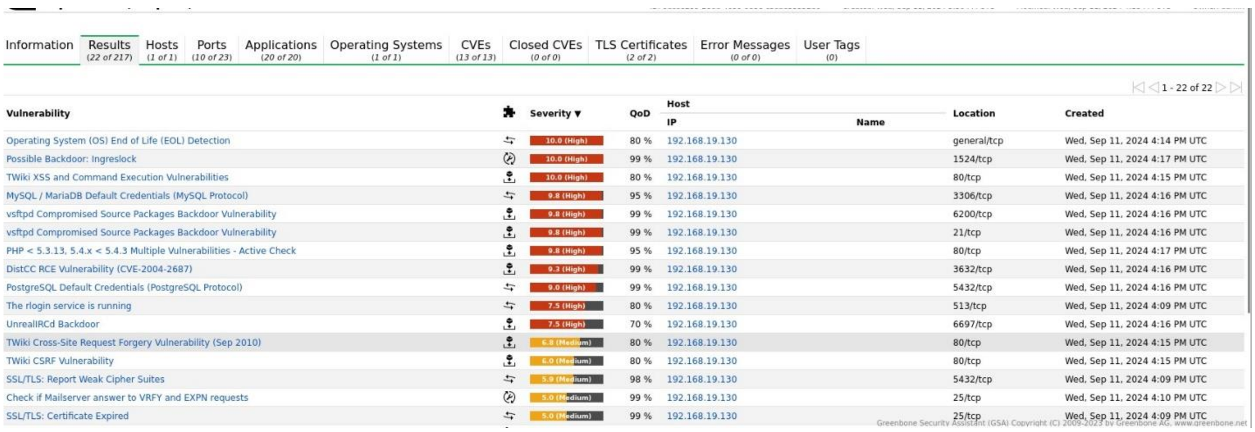


```
──(kali㉿kali)-[~]
─$ nikto -h http://kust.edu.pk
 Nikto v2.5.0
---------------------------------------------------------------------------
 Target IP:          107.6.161.242
 Target Hostname:    kust.edu.pk
 Target Port:        80
 Start Time:         2024-09-11 09:23:10 (GMT-4)
---------------------------------------------------------------------------
 Server: No banner retrieved
 Root page / redirects to: https://kust.edu.pk/
 No CGI Directories found (use '-C all' to force check all possible dirs)
 .: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-sc
nner/vulnerabilities/missing-content-type-header/
 ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
 Scan terminated: 19 error(s) and 1 item(s) reported on remote host
 End Time:           2024-09-11 09:29:16 (GMT-4) (366 seconds)
---------------------------------------------------------------------------
 1 host(s) tested
```

Openvas vulnerability scanning



Task Name	scan01
Scan Time	Wed, Sep 11, 2024 3:57 PM UTC - Wed, Sep 11, 2024 4:18 PM UTC
Scan Duration	0:21 h
Scan Status	Done
Hosts scanned	1
Filter	apply_overrides=0 levels=hml min_qod=70
Timezone	Coordinated Universal Time (UTC)

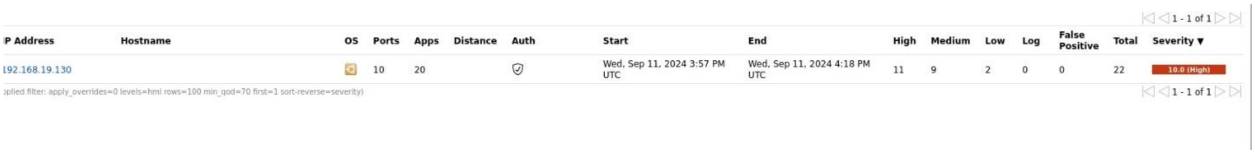


Information | Results (22 of 217) | Hosts (1 of 1) | Ports (10 of 23) | Applications (20 of 20) | Operating Systems (1 of 1) | CVEs (13 of 13) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (0 of 0) | User Tags (0)

1 - 22 of 22

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	192.168.19.130		general/tcp	Wed, Sep 11, 2024 4:14 PM UTC
Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.19.130		1524/tcp	Wed, Sep 11, 2024 4:17 PM UTC
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:15 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)		9.8 (High)	95 %	192.168.19.130		3306/tcp	Wed, Sep 11, 2024 4:16 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability		9.8 (High)	99 %	192.168.19.130		6200/tcp	Wed, Sep 11, 2024 4:16 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability		9.8 (High)	99 %	192.168.19.130		21/tcp	Wed, Sep 11, 2024 4:16 PM UTC
PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check		9.8 (High)	95 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:17 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)		9.3 (High)	99 %	192.168.19.130		3632/tcp	Wed, Sep 11, 2024 4:16 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)		9.0 (High)	99 %	192.168.19.130		5432/tcp	Wed, Sep 11, 2024 4:16 PM UTC
The rlogin service is running		7.5 (High)	80 %	192.168.19.130		513/tcp	Wed, Sep 11, 2024 4:09 PM UTC
UnrealIRCd Backdoor		7.5 (High)	70 %	192.168.19.130		6697/tcp	Wed, Sep 11, 2024 4:16 PM UTC
TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)		6.8 (Medium)	80 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:15 PM UTC
TWiki CSRF Vulnerability		6.0 (Medium)	80 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:15 PM UTC
SSL/TLS: Report Weak Cipher Suites		5.9 (Medium)	98 %	192.168.19.130		5432/tcp	Wed, Sep 11, 2024 4:09 PM UTC
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99 %	192.168.19.130		25/tcp	Wed, Sep 11, 2024 4:10 PM UTC
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	192.168.19.130		25/tcp	Wed, Sep 11, 2024 4:09 PM UTC

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

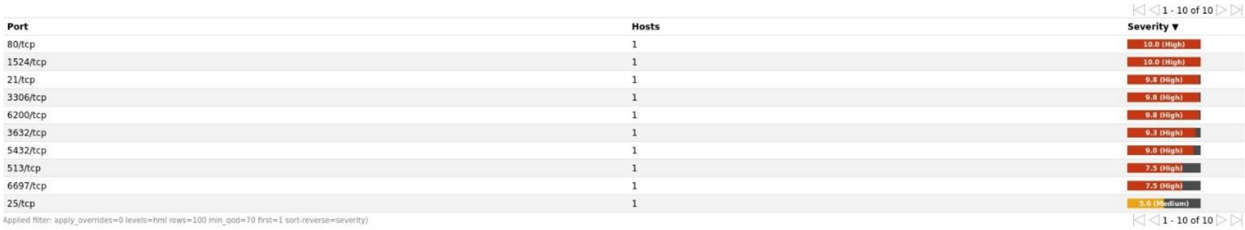


1 - 1 of 1

P Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▼
192.168.19.130			10	20			Wed, Sep 11, 2024 3:57 PM UTC	Wed, Sep 11, 2024 4:18 PM UTC	11	9	2	0	0	22	10.0 (High)

plied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 1 of 1



1 - 10 of 10

Port	Hosts	Severity ▼
80/tcp	1	10.0 (High)
1524/tcp	1	10.0 (High)
21/tcp	1	9.8 (High)
3306/tcp	1	9.8 (High)
6200/tcp	1	9.8 (High)
3632/tcp	1	9.3 (High)
5432/tcp	1	9.0 (High)
513/tcp	1	7.5 (High)
6697/tcp	1	7.5 (High)
25/tcp	1	5.0 (Medium)

Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 10 of 10

➢ Reviewing security policies and procedures.

Access Control Policy

- **Objective**: Ensure that only authorized personnel have access to specific systems and data.
- **Review:** Check if policies follow the principle of least privilege and enforce **multi-factor authentication (MFA)**.

Data Protection Policy

- **Objective**: Protect sensitive data from unauthorized access, breaches, or loss.
- **Review**: Assess encryption standards for data at rest and in transit, backup procedures, and data retention policies.

Incident Response Plan

- **Objective**: Define how to detect, respond to, and recover from security incidents.
- **Review**: Ensure there are clear steps for reporting, investigating, and mitigating incidents, along with regular drills.

Patch Management Policy

- **Objective**: Keep systems up-to-date and secure by regularly applying patches.
- **Review**: Confirm that the company has automated and timely patching processes for software, hardware, and operating systems.

Employee Training and Awareness

- **Objective**: Educate staff on security best practices, such as recognizing phishing attacks and handling sensitive information.
- **Review**: Check for mandatory cybersecurity awareness training and periodic refresher courses.

Acceptable Use Policy

- **Objective**: Outline how employees can use company IT resources.
- **Review**: Ensure it covers the use of devices, internet, email, and social media to minimize risks.

Weaknesses in Current Policies:

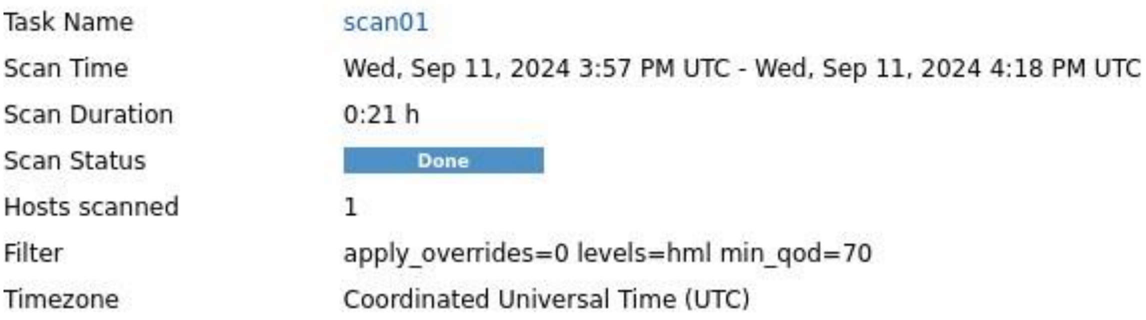
- Inconsistent password policies across departments.
- No multi-factor authentication (MFA) implemented.
- Lack of a comprehensive incident response plan.

Recommendations:

- Implement strict password policies.
- Enforce MFA across all systems.
- Develop and train staff on incident response procedures.

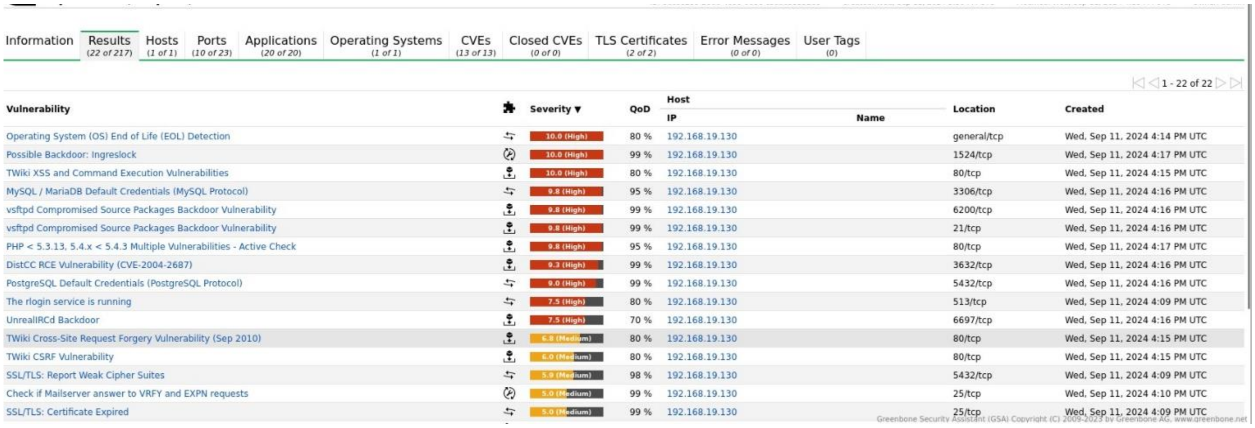
➢ Compiling a report with findings and recommendation

Vulnerability scanning information



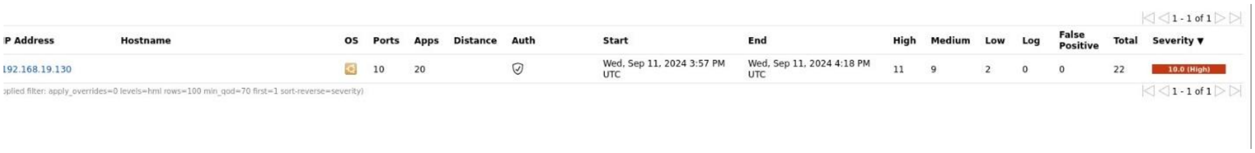
Task Name	scan01
Scan Time	Wed, Sep 11, 2024 3:57 PM UTC - Wed, Sep 11, 2024 4:18 PM UTC
Scan Duration	0:21 h
Scan Status	Done
Hosts scanned	1
Filter	apply_overrides=0 levels=hml min_qod=70
Timezone	Coordinated Universal Time (UTC)

Result:



Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Operating System (OS) End of Life (EOL) Detection	⇆	10.0 (High)	80 %	192.168.19.130		general/tcp	Wed, Sep 11, 2024 4:14 PM UTC
Possible Backdoor: Ingreslock	⊘	10.0 (High)	99 %	192.168.19.130		1524/tcp	Wed, Sep 11, 2024 4:17 PM UTC
TWiki XSS and Command Execution Vulnerabilities	⤓	10.0 (High)	80 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:15 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	⇆	9.8 (High)	95 %	192.168.19.130		3306/tcp	Wed, Sep 11, 2024 4:16 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	9.8 (High)	99 %	192.168.19.130		6200/tcp	Wed, Sep 11, 2024 4:16 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	9.8 (High)	99 %	192.168.19.130		21/tcp	Wed, Sep 11, 2024 4:16 PM UTC
PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	⤓	9.8 (High)	95 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:17 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	⤓	9.3 (High)	99 %	192.168.19.130		3632/tcp	Wed, Sep 11, 2024 4:16 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	⇆	9.0 (High)	99 %	192.168.19.130		5432/tcp	Wed, Sep 11, 2024 4:16 PM UTC
The rlogin service is running	⇆	7.5 (High)	80 %	192.168.19.130		513/tcp	Wed, Sep 11, 2024 4:09 PM UTC
UnrealIRCd Backdoor	⤓	7.5 (High)	70 %	192.168.19.130		6697/tcp	Wed, Sep 11, 2024 4:16 PM UTC
TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	⤓	6.8 (Medium)	80 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:15 PM UTC
TWiki CSRF Vulnerability	⤓	6.0 (Medium)	80 %	192.168.19.130		80/tcp	Wed, Sep 11, 2024 4:15 PM UTC
SSL/TLS: Report Weak Cipher Suites	⇆	5.9 (Medium)	98 %	192.168.19.130		5432/tcp	Wed, Sep 11, 2024 4:09 PM UTC
Check if Mailserver answer to VRFY and EXPN requests	⊘	5.0 (Medium)	99 %	192.168.19.130		25/tcp	Wed, Sep 11, 2024 4:10 PM UTC
SSL/TLS: Certificate Expired	⇆	5.0 (Medium)	99 %	192.168.19.130		25/tcp	Wed, Sep 11, 2024 4:09 PM UTC

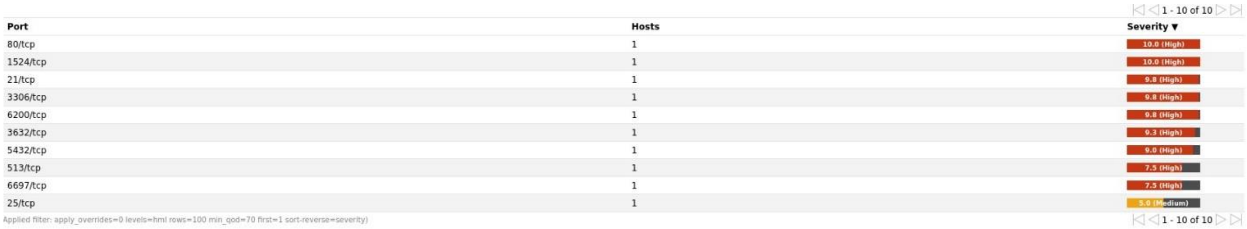
Host:



P Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▼
192.168.19.130			10	20		✓	Wed, Sep 11, 2024 3:57 PM UTC	Wed, Sep 11, 2024 4:18 PM UTC	11	9	2	0	0	22	10.0 (High)

pplied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

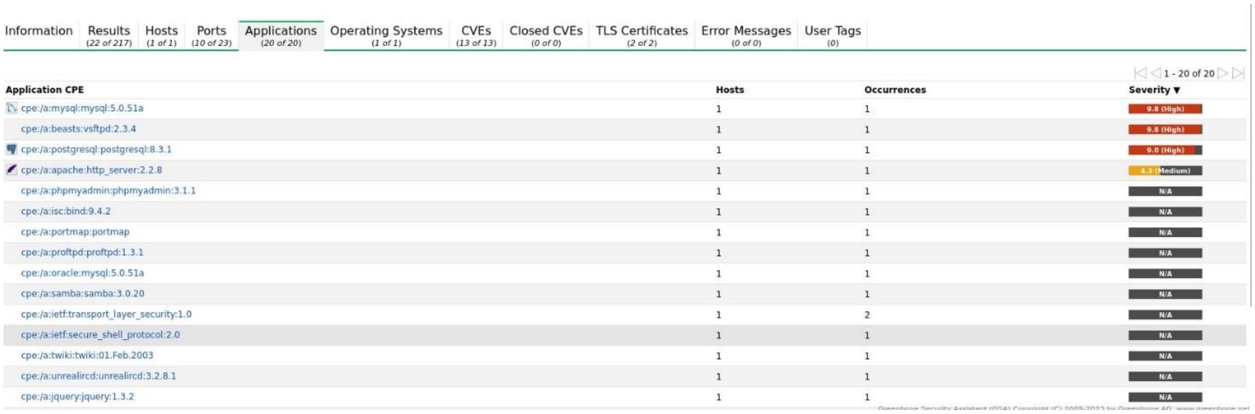
Ports:



Port	Hosts	Severity ▼
80/tcp	1	10.0 (High)
1524/tcp	1	10.0 (High)
21/tcp	1	9.8 (High)
3306/tcp	1	9.8 (High)
6200/tcp	1	9.8 (High)
3632/tcp	1	9.3 (High)
5432/tcp	1	9.0 (High)
513/tcp	1	7.5 (High)
6697/tcp	1	7.5 (High)
25/tcp	1	5.0 (Medium)

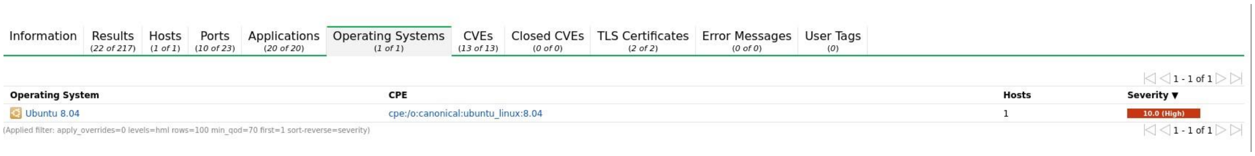
Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Application:



Application CPE	Hosts	Occurrences	Severity ▼
cpe:/a:mysql:mysql:5.0.51a	1	1	9.8 (High)
cpe:/a:beasts:vsftpd:2.3.4	1	1	9.8 (High)
cpe:/a:postgresql:postgresql:8.3.1	1	1	9.0 (High)
cpe:/a:apache:http_server:2.2.8	1	1	4.3 (Medium)
cpe:/a:phpmyadmin:phpmyadmin:3.1.1	1	1	N/A
cpe:/a:isc:bind:9.4.2	1	1	N/A
cpe:/a:portmap:portmap	1	1	N/A
cpe:/a:proftpd:proftpd:1.3.1	1	1	N/A
cpe:/a:oracle:mysql:5.0.51a	1	1	N/A
cpe:/a:samba:samba:3.0.20	1	1	N/A
cpe:/a:ietf:transport_layer_security:1.0	1	2	N/A
cpe:/a:ietf:secure_shell_protocol:2.0	1	1	N/A
cpe:/a:twiki:twiki:01.Feb.2003	1	1	N/A
cpe:/a:unrealircd:unrealircd:3.2.8.1	1	1	N/A
cpe:/a:jquery:jquery:1.3.2	1	1	N/A

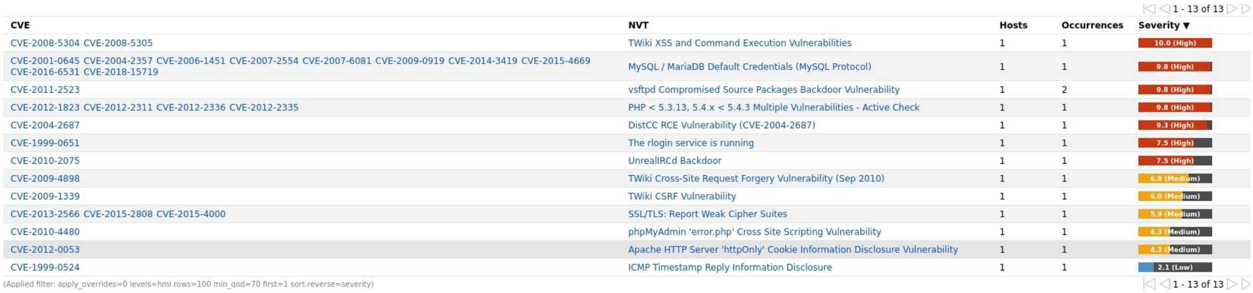
Operating System:



Operating System	CPE	Hosts	Severity ▼
Ubuntu 8.04	cpe:/o:canonical:ubuntu_linux:8.04	1	10.0 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

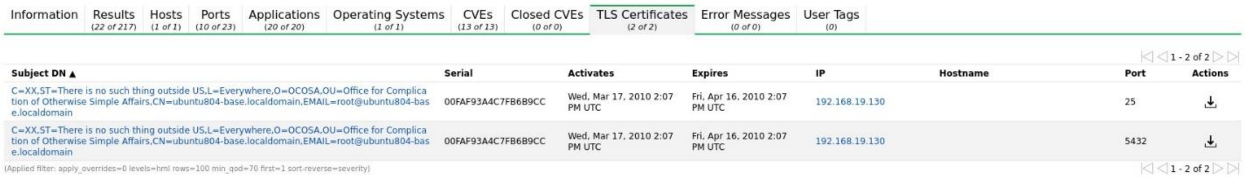
CVES:



CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2008-5304 CVE-2008-5305	TWiki XSS and Command Execution Vulnerabilities	1	1	10.0 (High)
CVE-2001-0645 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (High)
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	1	2	9.8 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	1	1	9.8 (High)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.3 (High)
CVE-1999-0651	The rlogin service is running	1	1	7.5 (High)
CVE-2010-2075	UnrealIRCd Backdoor	1	1	7.5 (High)
CVE-2009-4898	TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	1	1	6.8 (Medium)
CVE-2009-1339	TWiki CSRF Vulnerability	1	1	6.0 (Medium)
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites	1	1	5.9 (Medium)
CVE-2010-4480	phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	1	1	4.3 (Medium)
CVE-2012-0053	Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	1	1	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

TLS Certificate:



Subject DN ▲	Serial	Activates	Expires	IP	Hostname	Port	Actions
C=XX,ST=There is no such thing outside US,L=Everywhere,O=OCOSA,OU=Office for Complication of Otherwise Simple Affairs,CN=ubuntu804-base.localdomain,EMAIL=root@ubuntu804-base.localdomain	00FAF93A4C7FB6B9CC	Wed, Mar 17, 2010 2:07 PM UTC	Fri, Apr 16, 2010 2:07 PM UTC	192.168.19.130		25	⤓
C=XX,ST=There is no such thing outside US,L=Everywhere,O=OCOSA,OU=Office for Complication of Otherwise Simple Affairs,CN=ubuntu804-base.localdomain,EMAIL=root@ubuntu804-base.localdomain	00FAF93A4C7FB6B9CC	Wed, Mar 17, 2010 2:07 PM UTC	Fri, Apr 16, 2010 2:07 PM UTC	192.168.19.130		5432	⤓

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Severity: -

High

Recommendations

Patching and Updates:

- Patch high-severity vulnerabilities within .
- Regular software updates for all critical systems.

Access Controls:

- Review and update access controls, ensuring principle of least privilege.

Training:

- Provide cybersecurity awareness training for employees, focusing on phishing and social engineering attacks.