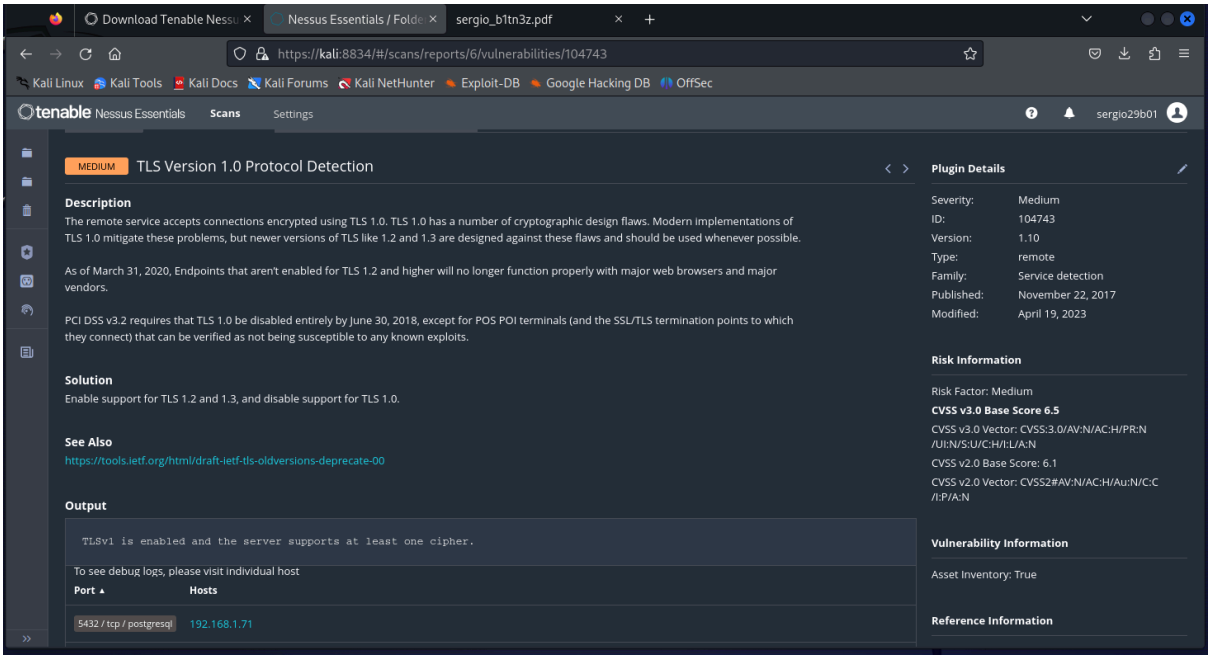
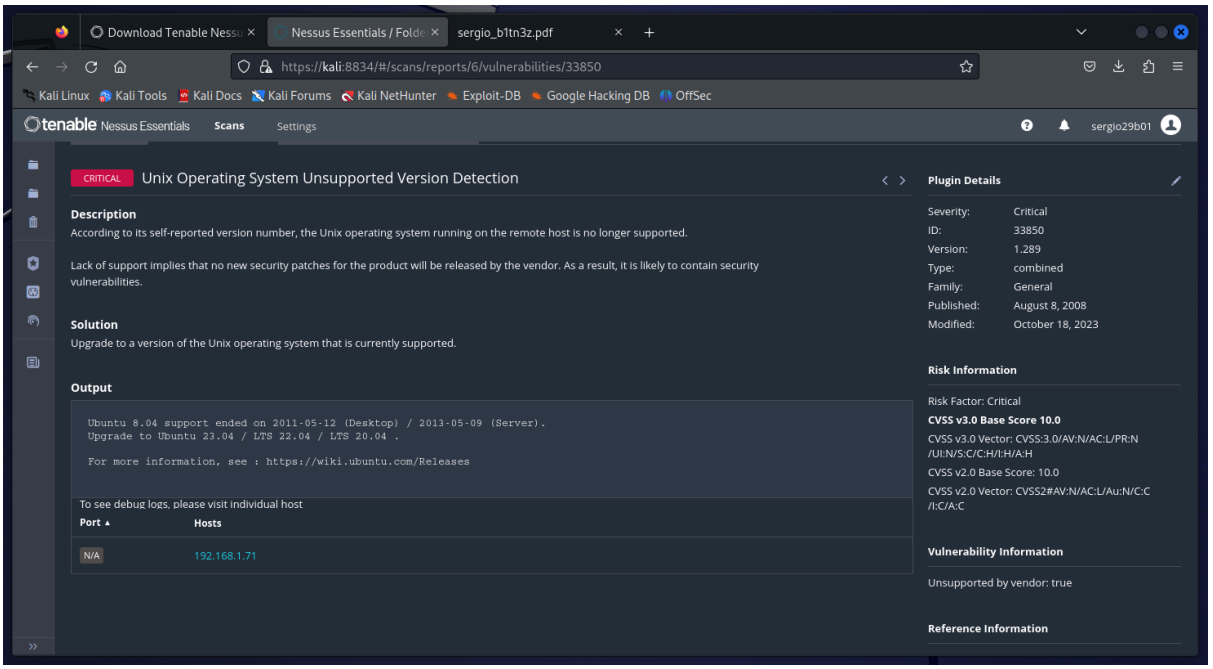
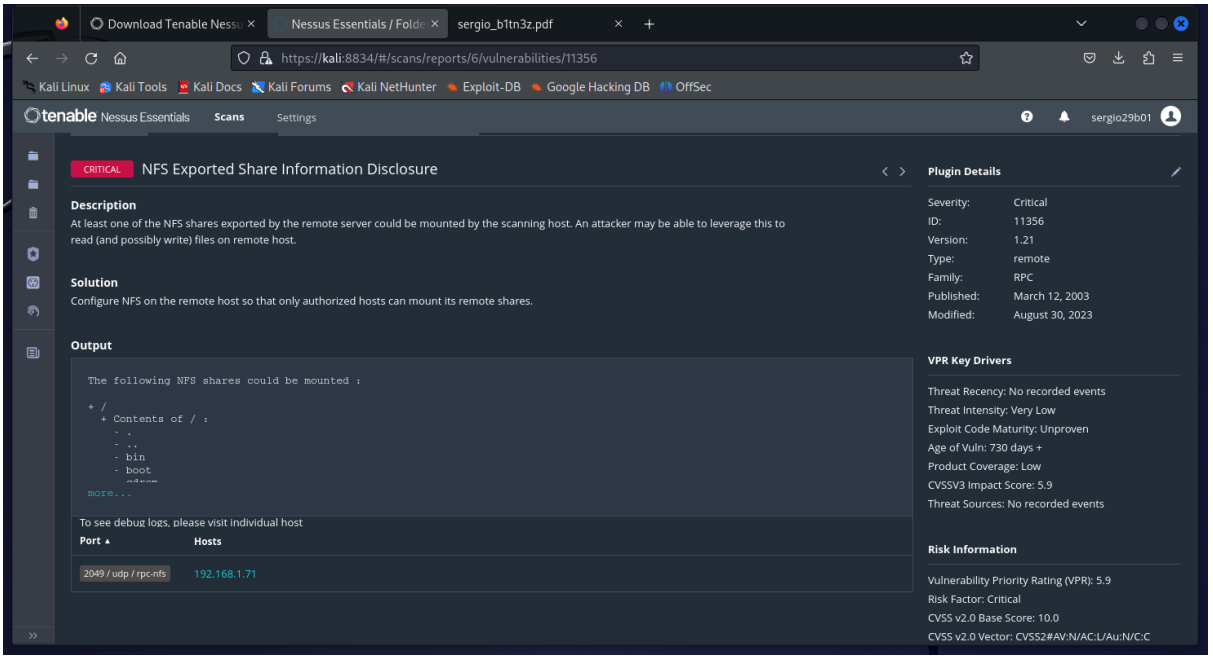

Download Tenable Nessu
Nessus Essentials / Folde
sergio_b1tn3z.pdf
https://kali:8834/#/scans/reports/6/vulnerabilities/104743
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials Scans Settings
sergio29b01
MEDIUM
TLS Version 1.0 Protocol Detection
Description
The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.
Solution
Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
See Also
https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
Output
TLSv1 is enabled and the server supports at least one cipher.
To see debug logs, please visit individual host
Port
Hosts
5432 / tcp / postgresql
192.168.1.71
Plugin Details
Severity: Medium
ID: 104743
Version: 1.10
Type: remote
Family: Service detection
Published: November 22, 2017
Modified: April 19, 2023
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v2.0 Base Score: 6.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N
Vulnerability Information
Asset Inventory: True
Reference Information


Download Tenable Nessu
Nessus Essentials / Folde
sergio_b1tn3z.pdf
https://kali:8834/#/scans/reports/6/vulnerabilities/33850
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials Scans Settings
sergio29b01
CRITICAL
Unix Operating System Unsupported Version Detection
Description
According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Solution
Upgrade to a version of the Unix operating system that is currently supported.
Output
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .
For more information, see : https://wiki.ubuntu.com/Releases
To see debug logs, please visit individual host
Port
Hosts
N/A
192.168.1.71
Plugin Details
Severity: Critical
ID: 33850
Version: 1.289
Type: combined
Family: General
Published: August 8, 2008
Modified: October 18, 2023
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Vulnerability Information
Unsupported by vendor: true
Reference Information


Download Tenable Nessu
Nessus Essentials / Folde
sergio_b1tn3z.pdf
https://kali:8834/#/scans/reports/6/vulnerabilities/11356
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
tenable Nessus Essentials
Scans
Settings
sergio29b01
CRITICAL
NFS Exported Share Information Disclosure
Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.
Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
Output
The following NFS shares could be mounted :
+ /
+ Contents of / :
- .
- ..
- bin
- boot
more...
To see debug logs, please visit individual host
Port
Hosts
2049 / udp / rpc-nfs
192.168.1.71
Plugin Details
Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C