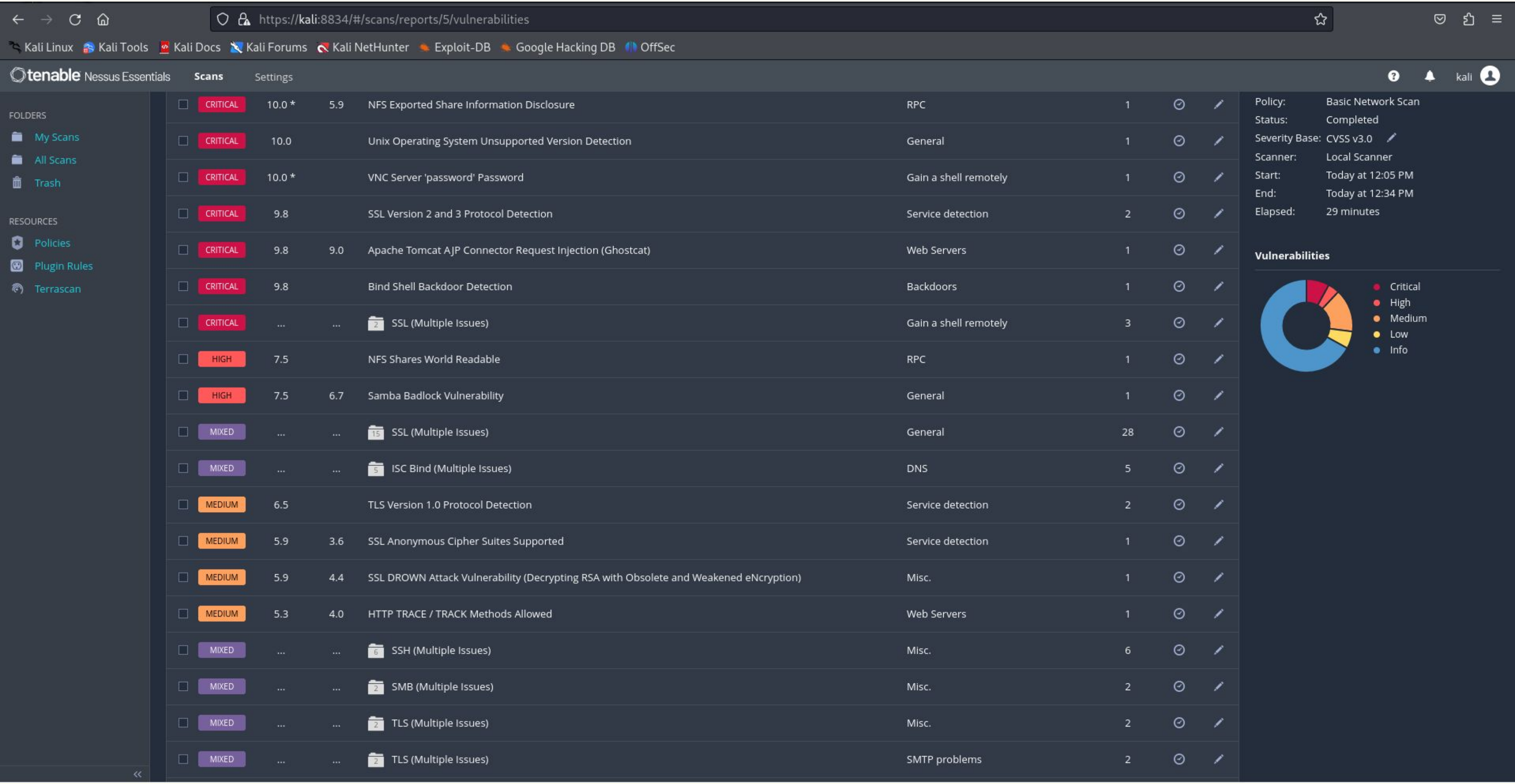
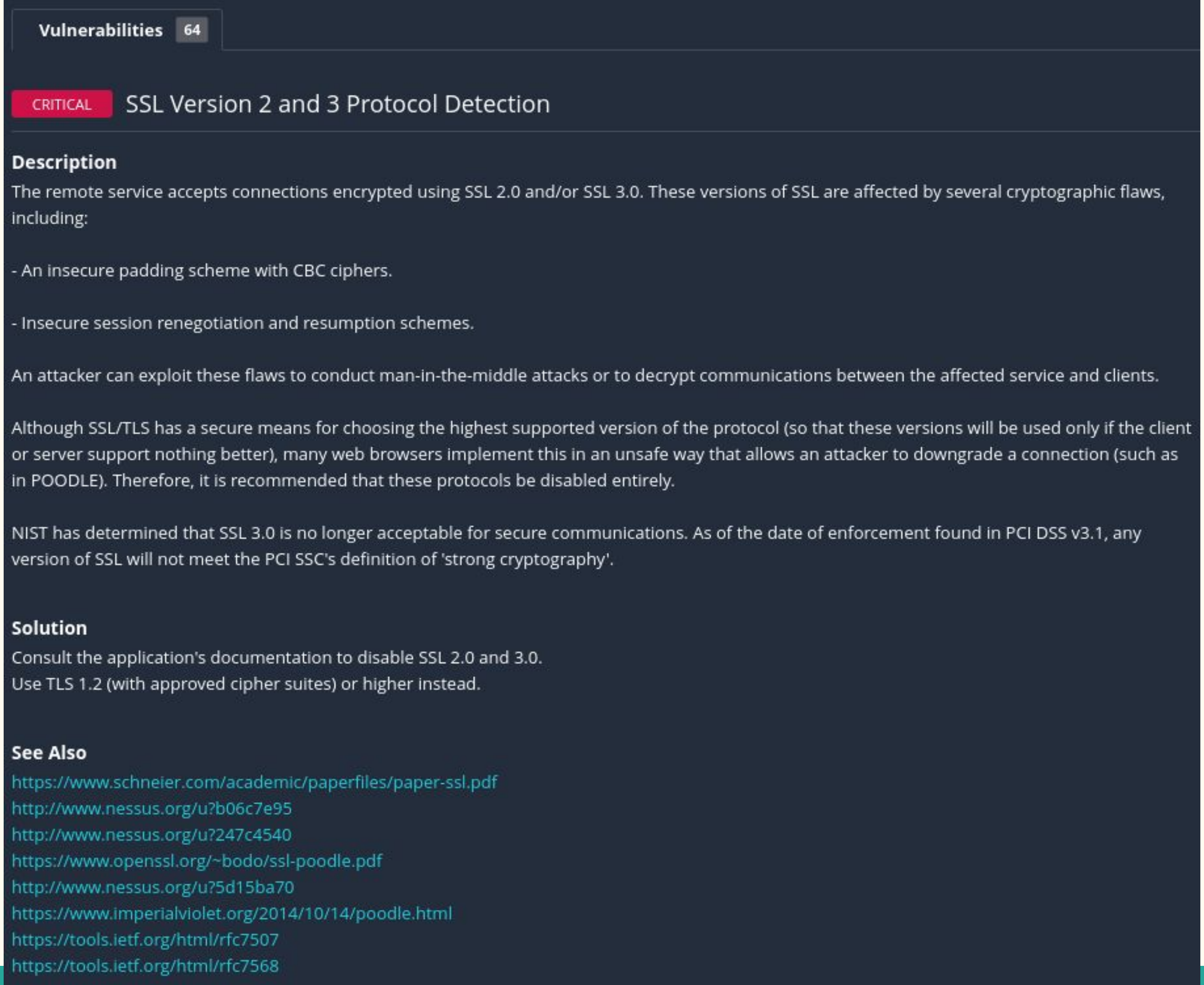
S5-L5



□	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
□	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
□	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
□	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
□	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
□	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
□	CRITICAL	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
□	HIGH	7.5		NFS Shares World Readable	RPC	1
□	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
□	MIXED	...	...	15 SSL (Multiple Issues)	General	28
□	MIXED	...	...	5 ISC Bind (Multiple Issues)	DNS	5
□	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
□	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1
□	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
□	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
□	MIXED	...	...	6 SSH (Multiple Issues)	Misc.	6
□	MIXED	...	...	2 SMB (Multiple Issues)	Misc.	2
□	MIXED	...	...	2 TLS (Multiple Issues)	Misc.	2
□	MIXED	...	...	2 TLS (Multiple Issues)	SMTP problems	2

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:05 PM
End:	Today at 12:34 PM
Elapsed:	29 minutes



SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

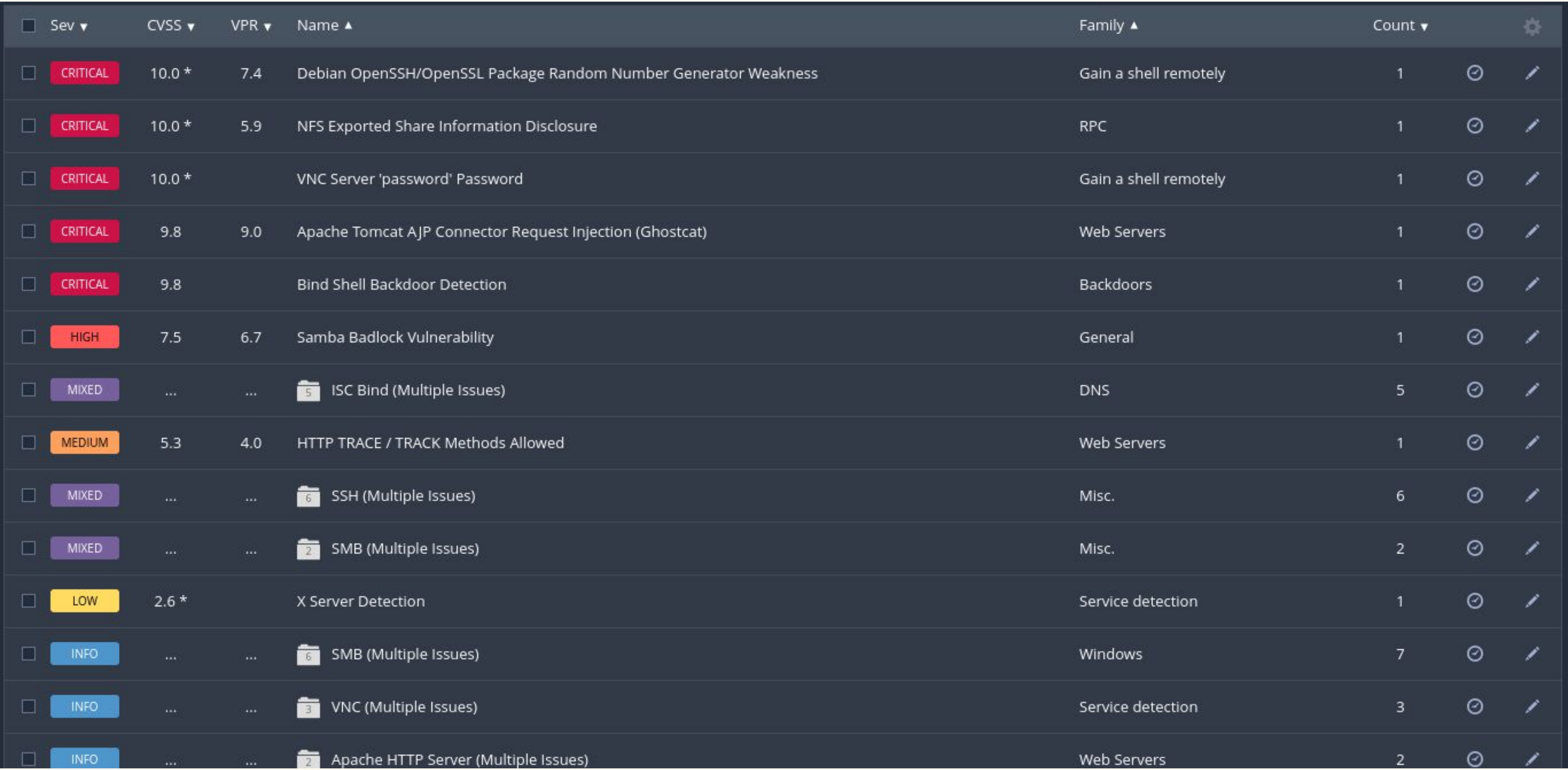
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568



□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾		⚙
□	CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1	✓	✎
□	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	✓	✎
□	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	✓	✎
□	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	✓	✎
□	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	✓	✎
□	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	✓	✎
□	MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5	✓	✎
□	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	✓	✎
□	MIXED	...	...	SSH (Multiple Issues)	Misc.	6	✓	✎
□	MIXED	...	...	SMB (Multiple Issues)	Misc.	2	✓	✎
□	LOW	2.6 *		X Server Detection	Service detection	1	✓	✎
□	INFO	...	...	SMB (Multiple Issues)	Windows	7	✓	✎
□	INFO	...	...	VNC (Multiple Issues)	Service detection	3	✓	✎
□	INFO	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2	✓	✎