KGB - PenToolBox

Date et Heure: 15/05/2024 22:10:02
Réseau Scanné: 192.168.1.29

Discovered Targets
192.168.1.29

Vulnérabilités Découvertes:

IP	CVE	Description	Sévérité
192.168.1.29	CVE-2008-5304	TWiki XSS and Command Execution Vulnerabilities	High
192.168.1.29	CVE-1999-0618	The rexec service is running	High
192.168.1.29	CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	High
192.168.1.29	CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	High
192.168.1.29	CVE-2001-0645	MySQL / MariaDB Default Credentials (MySQL Protocole)	High
192.168.1.29	CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	High
192.168.1.29	CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	High
192.168.1.29	CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	High
192.168.1.29	CVE-2010-2075	UnrealIRCd Backdoor	High
192.168.1.29	CVE-1999-0501	FTP Brute Force Logins Reporting	High
192.168.1.29	CVE-2012-1823	PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	High
192.168.1.29	CVE-2014-0224	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	High

IP	CVE	Description	Sévérité
192.168.1.29	CVE-2011-0411	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	Medium
192.168.1.29	CVE-2009-4898	TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	Medium
192.168.1.29	CVE-1999-0497	Anonymous FTP Login Reporting	Medium
192.168.1.29	CVE-2018-20212	TWiki < 6.1.0 XSS Vulnerability	Medium
192.168.1.29	CVE-2012-6708	jQuery < 1.9.0 XSS Vulnerability	Medium
192.168.1.29	CVE-2009-1339	TWiki Cross-Site Request Forgery Vulnerability	Medium
192.168.1.29	CVE-2013-2566	SSL/TLS: Report Weak Cipher Suites	Medium
192.168.1.29	CVE-2016-0800	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocole Detection	Medium
192.168.1.29	CVE-2016-0800	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocole Detection	Medium
192.168.1.29	CVE-2003-1567	HTTP Debugging Methods (TRACE/TRACK) Enabled	Medium
192.168.1.29	CVE-2008-0149	phpinfo() Output Reporting (HTTP)	Medium
192.168.1.29	CVE-2011-1473	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	Medium
192.168.1.29	CVE-2011-1473	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	Medium
192.168.1.29	CVE-2005-0283	QWikiwiki directory traversal vulnerability	Medium
192.168.1.29	CVE-1999-0678	/doc directory browsable	Medium
192.168.1.29	CVE-2011-3389	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocole Detection	Medium
192.168.1.29	CVE-2012-0053	Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability	Medium
192.168.1.29	CVE-2010-4480	phpMyAdmin error.php Cross Site Scripting Vulnerability	Medium
192.168.1.29	CVE-2011-4969	jQuery < 1.6.3 XSS Vulnerability	Medium
192.168.1.29	CVE-2011-3389	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocole Detection	Medium
192.168.1.29	CVE-2015-0204	SSL/TLS: RSA Temporary Key Handling RSA_EXPORT Downgrade Issue (FREAK)	Medium
192.168.1.29	CVE-2015-4000	SSL/TLS: DHE_EXPORT Man in the Middle Security Bypass Vulnerability (LogJam)	Low
192.168.1.29	CVE-2014-3566	SSL/TLS: SSLv3 Protocole CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	Low
192.168.1.29	CVE-2014-3566	SSL/TLS: SSLv3 Protocole CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	Low

Exploitation - Evaluation des Vulnérabilités

Résultat de l'attaque Hydra :

PORT	PROTOCOL	IP	LOGIN	PASSWORD
21	ftp	192.168.1.29	ftp	123456
21	ftp	192.168.1.29	ftp	password
21	ftp	192.168.1.29	ftp	12345678
21	ftp	192.168.1.29	ftp	qwerty
21	ftp	192.168.1.29	ftp	123456789
21	ftp	192.168.1.29	ftp	12345
21	ftp	192.168.1.29	ftp	1234567
21	ftp	192.168.1.29	ftp	dragon
21	ftp	192.168.1.29	ftp	1234
21	ftp	192.168.1.29	ftp	111111