

# Nessus Report

Nessus Scan Report

Sat, 29 Oct 2016 05:40:30 CLST

# Table Of Contents

Hosts Summary (Executive).....	3
•192.168.87.129.....	4

# Hosts Summary (Executive)

## Summary

Critical	High	Medium	Low	Info	Total
2	4	6	2	29	43

## Details

Severity	Plugin Id	Name
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (unauthenticated check)
Critical (10.0)	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (unauthenticated check)
High (9.3)	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unauthenticated check)
High (7.5)	10481	MySQL Unpassworded Account Check
High (7.5)	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (unauthenticated check)
High (7.5)	34460	Unsupported Web Server Detection
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	45517	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (unauthenticated check)
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (3.3)	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10719	MySQL Server Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10884	Network Time Protocol (NTP) Server Detection

Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11424	WebDAV Detection
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	66173	RDP Screenshot
Info	66334	Patch Report