

Nessus Report

DATE	31-10-2023
TEAM ID	4.1
PROJECT NAME	NETWORK ANOMALY DETECTION

MENTOR : P MANOJ

Team Members :

C DEVAKI NANDAN REDDY

S NIHAL AHMED

192.168.1.205					
Summary					
Critical	High	Medium	Low	Info	Total
31	150	30	2	0	213
Details					
Severity	Plugin Id	Name			

Critical (10.0)	11790	MS03-026 / MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (823980 / 824146)
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980)
Critical (10.0)	11835 check)	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	11888	MS03-043: Buffer Overrun in Messenger Service (828035)
Critical (10.0)	11921	MS03-049: Buffer Overflow in the Workstation Service (828749)
Critical (10.0)	12052	MS04-007: ASN.1 parsing vulnerability (828028)
Critical (10.0)	12205	MS04-011: Microsoft Hotfix (credentialed check) (835732)
Critical (10.0)	12206	MS04-012: Microsoft Hotfix (credentialed check) (828741)
Critical (10.0)	15456	MS04-031: Vulnerability in NetDDE Could Allow Code Execution (841533)
Critical (10.0)	18483	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
Critical (10.0)	19402	MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
Critical (10.0)	19406	MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0)	19407	MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)
Critical (10.0)	19408	MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)
Critical (10.0)	19999	MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)
Critical (10.0)	20004	MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)
Critical (10.0)	21193	MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)
Critical (10.0)	21692	MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege (914389)
Critical (10.0)	22182 (921883)	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)
Critical (10.0)		
Critical (10.0)		

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

Critical (10.0)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)	22183 (920683)	MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution
	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (unauthenticated check)
	23646	MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution (924270)
	24340	MS07-016: Cumulative Security Update for Internet Explorer (928090)
High (9.3)	29893	MS08-001: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)
	34476	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644)
	35361	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)
	39344	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)
	39348	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)
43063		MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)
44422		MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)
	10861	MS02-005: MSIE 5.01 5.5 6.0 Cumulative Patch (890923)
11878		MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution (823559)
11887		MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control (826232)
	11928	MS03-044: Buffer Overrun in Windows Help (825119)
	13642	MS04-024: Buffer overrun in Windows Shell (839645)
	15457	MS04-032: Security Update for Microsoft Windows (840987)
	15460	MS04-037: Vulnerability in Windows Shell (841356)
16123		MS05-001: HTML Help Code Execution (890175)
16124		MS05-002: Cursor and Icon Format Handling Code Execution (891711)
	16324	MS05-008: Vulnerability in Windows Shell (890047)
	16326	MS05-011: Vulnerability in SMB may allow remote code execution (885250)
16329		MS05-013: Vulnerability in the DHTML Editing Component may allow code execution (891781)
18215		MS05-024: Vulnerability in Web View Could Allow Code Execution (894320)
	18482	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution (896358)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)

High (9.3)	25884	MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829)
	25886	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)
	26017 (938827)	MS07-051: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)
	26961	MS07-055: Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution (923810)
High (9.3)	26962 (941202)	MS07-056: Cumulative Security Update for Outlook Express and Windows Mail (941202)
	26963	MS07-057: Cumulative Security Update for Internet Explorer (939653)
	29308	MS07-064: Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)
	29313	MS07-069: Cumulative Security Update for Internet Explorer (942615)
	31042	MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)
	31044	MS08-010: Cumulative Security Update for Internet Explorer (944533)
	31794	MS08-021: Vulnerabilities in GDI Could Allow Remote Code Execution (948590)
	31797	MS08-024: Cumulative Security Update for Internet Explorer (947864)
	32312	MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)
	33133	MS08-031: Cumulative Security Update for Internet Explorer (950759)
	33135	MS08-033: Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)
	33874	MS08-045: Cumulative Security Update for Internet Explorer (953838)
	33875	MS08-046: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)
	34403	MS08-058: Microsoft Internet Explorer Multiple Vulnerabilities (956390)
	35070	MS08-071: Vulnerabilities in GDI+ Could Allow Remote Code Execution (956802)
	35072	MS08-073: Microsoft Internet Explorer Multiple Vulnerabilities (958215)
	35221	MS08-078: Microsoft Internet Explorer Security Update (960714)
	35822	MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)
	35823	MS09-007: Vulnerability in SChannel Could Allow Spoofing (960225)
	36151	MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)
	36152	MS09-014: Cumulative Security Update for Internet Explorer (963027)

22536	MS06-063: Vulnerability in Server Service Could Allow Denial of Service (923414)
23643	MS06-066: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (923980)
23645	MS06-068: Vulnerability in Microsoft Agent Could Remote Code Execution (920213)
23838	MS06-078: Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689/925398)
35075	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)
39342	MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)
11885	MS03-045: Buffer Overrun in the ListBox and in the ComboBox (824141)
13637	MS04-019: Utility Manager Could Allow Code Execution (842526)
15963	MS04-044: Vulnerabilities in Windows Kernel and LSASS (885835)
19403	MS05-040: Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)
20298	MS05-055: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (908523)

High (7.5)

High (7.5)

High (7.5)

High (7.5)

High (7.5)

High (7.5)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

High (7.2)

Medium (6.9)

Medium (6.9)	25025	MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)
Medium (6.8)	29894	MS08-002: Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)
Medium (6.8)	31798	MS08-025: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)
Medium (6.8)	34406	MS08-061: Microsoft Windows Kernel Multiple Privilege Elevation (954211)
	36150	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)
	39347	MS09-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)
	46839	MS10-032: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)
	44421	MS10-011: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)
	46844	MS10-037: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)
	11990	MS04-003: MDAC Buffer Overflow (832483)
	21687	MS06-023: Vulnerability in Microsoft JScript Could Allow Remote Code Execution (917344)
	23835	MS06-076: Cumulative Security Update for Outlook Express (923694) 31039 MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)
	43061	MS09-069: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)
	22028	MS06-034: Vulnerability in Microsoft IIS using ASP Could Allow Remote Code Execution (917537)
	45511	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)
	44425	MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)
	45508	MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)
	22186	MS06-044: Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (917008)
	31793	MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)
	33441	MS08-037: Vulnerabilities in DNS Could Allow Spoofing (953230)
	33877	MS08-048: Security Update for Outlook Express and Windows Mail (951066)
	21211	MS06-014: Vulnerability in MDAC Could Allow Code Execution (911562)

Medium (6.8)

Medium (6.8)

Medium (6.5)

Medium (6.4)

Medium (6.2)

Medium (6.2)

Medium (6.0)

Medium (5.8)

Medium (5.8)

Medium (5.4)

Medium (5.1)

Medium (5.1)

Medium (5.1)

Medium (5.1)

Medium (5.1)

Medium (5.1)

Medium (5.1)

Medium (5.1)

Medium (5.1)

Medium (5.0)

Medium (4.3)
Low (3.3)
Low (2.6)
Medium (4.6)

	21212	MS06-015: Vulnerabilities in Windows Explorer Could Allow Remote Code Execution (908531)
	21213	MS06-016: Vulnerability in Outlook Express Could Allow Remote Code Execution (911567)
	22187	MS06-045: Vulnerability in Windows Explorer Could Allow Remote Code Execution (921398)
(950760)	33134	MS08-032: Cumulative Security Update of ActiveX Kill Bits
39622		MS09-032: Cumulative Security Update of ActiveX Kill Bits (973346)
42111		MS09-055: Cumulative Security Update of ActiveX Kill Bits (973525)
44418		MS10-008: Cumulative Security Update of ActiveX Kill Bits (978262)
46841		MS10-034: Cumulative Security Update of ActiveX Kill Bits (980195)
12267		MS04-016: Vulnerability in DirectPlay Could Allow Denial of Service (839643)
19998		MS05-045: Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)
21693		MS06-031: Vulnerability in RPC Mutual Authentication Could Allow Spoofing (917736)
42112		MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)
19405		MS05-042: Vulnerability in Kerberos Could Allow Denial of Service, Information Disclosure and Spoofing (899587)
18485		MS05-032: Vulnerability in Microsoft Agent Could Allow Spoofing (890046)
16299		MS03-034: NetBIOS Name Service Reply Information Leakage (824105) (credentialed check)
22333		MS06-053: Vulnerability in Indexing Service Could Allow Cross-Site Scripting (920685)