Host Vulnerabilities Report

Hostname:	WIN2008UPDATE
IP Address:	10.128.133.20
Submit by:	admin
Generated Time:	Oct. 2, 2018, 1:25 p.m.

Table Of Contents

Host Detailed Information

Information

Submit by:	admin
Created Date:	Sept. 10, 2018, 3:31 a.m.
Updated Date:	Sept. 10, 2018, 3:31 a.m.
Hostname: WIN2008UPDATE	**Ip Address:** 10.128.133.20
OS: Windows Server 2008 R2 (Service Pack 1, Server, SQL Server, [++])	**Version:** NA#

Description:

NA#

Running Service

| Service	Network Port	Description
loc-srv	135	
netbios-ssn	139	
microsoft-ds	445	
ms-term-service	3389	
vnc	5900	
unknown	49153	
unknown	49154	
http	80	
unknown	49155	
unknown	49152	
netbios-ns	137	

Table 1: Running Services of Host

Vulnerabilities

Overview

In this section, this report contains overview information that includes statistics by running services (in graph-1) and current categorized vulnerabilities (in graph-2) into groups:

- **High Risk** - Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access (e.g. administrator, root) to the machine over a remote connection.
- **Medium Risk** - The vulnerability discovered on the system can directly lead to an attacker gaining non-privileged access (e.g. standard user) to the machine over a remote connection.
- **Low Risk** - The vulnerability discovered on the system provides enticement data to the attacker that may be used to launch a more informed attack against the target environment. In addition, the vulnerability may indirectly lead to an attacker gaining some form of access to the machine over a remote connection.
- **Informational Risk** - A finding on the system that provides data to an attacker that is of lesser value to an attacker than the enticement data provided by a low risk vulnerability.
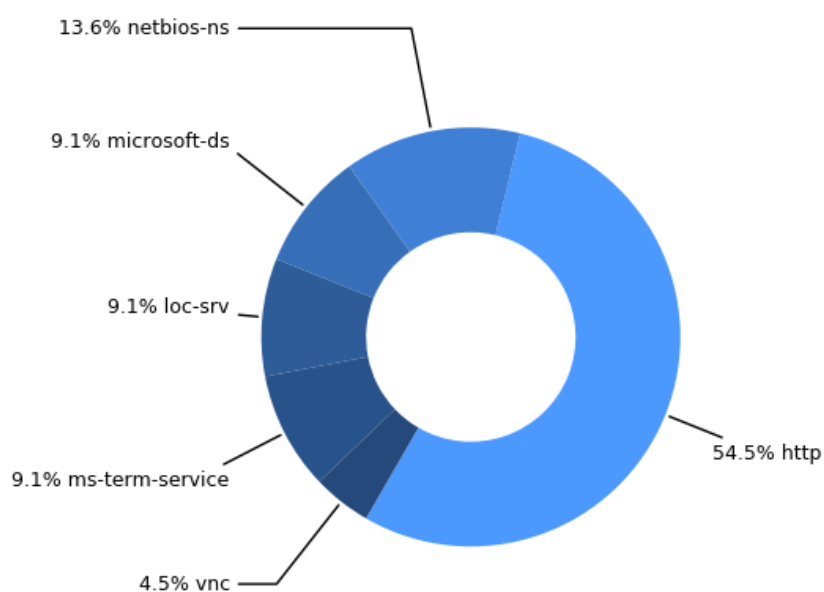
Graph 1: Vulnerabilities statistic by services
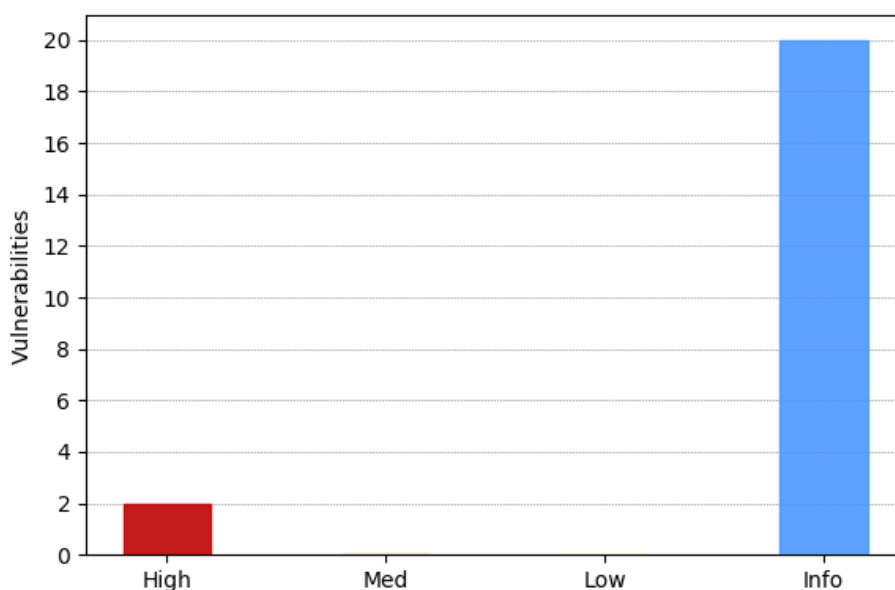
Graph 2: Current Vulnerabilities of Host

Scan History

In this section, the report contains scan history of host. It includes scan frequency and brief information of involved scan tasks.
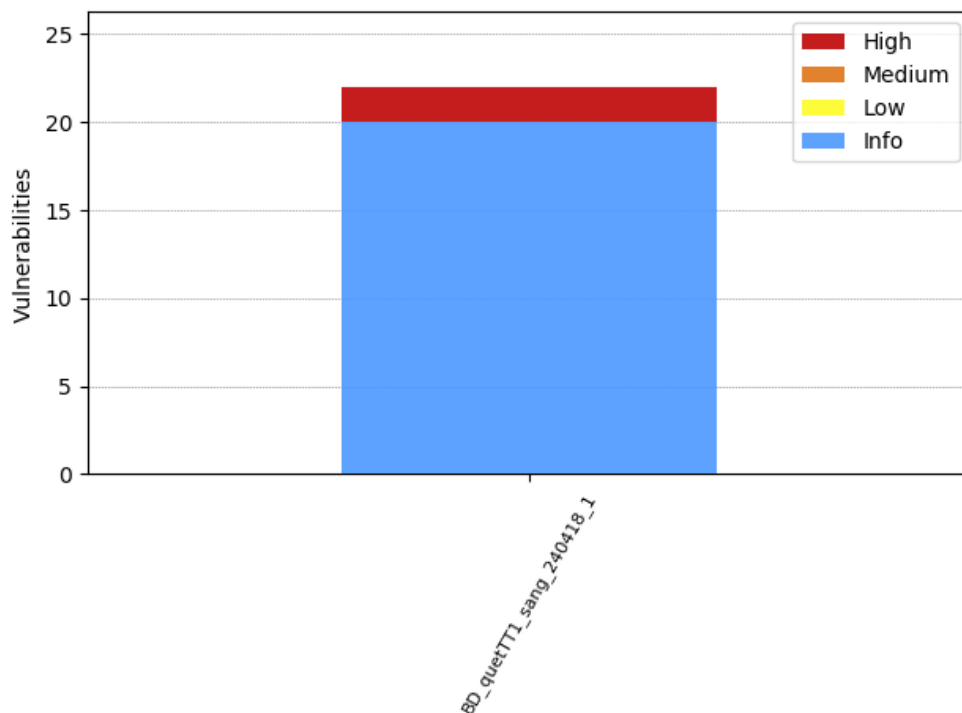
Graph 3: Scan History Statistic of Host

Scan History:

Scan Task	Start Time	Finished Time	Vulnerabilities			
			High	Med	Low	Info
BD_quetTT1_sang_240418_1	April 24, 2018, 4:30 a.m.	April 24, 2018, 5:44 a.m.	2	0	0	20

Table 2: Scan History of Host

Current Vulnerabilities In Detail

(MS15-034) Microsoft Windows HTTP.sys Remote Code Execution (3042553)

Vulnerbility:		(MS15-034) Microsoft Windows HTTP.sys Remote Code Execution (3042553)	
Level Risk:		10.0	
Service:	http	**CVE:**	CVE-2015-1635

Observation:

A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw occurs when HTTP.sys improperly parses specially crafted HTTP requests. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

Recommendation:

The vendor has released an update to address this issue. https://technet.microsoft.com/library/security/MS15-034 Superseded patch information: The patches for the following products are superseded by patches provided in: MS17-006 - March, 2017 Security Monthly Quality Rollup for Windows 8.1 (KB4012216): KB4012216- March, 2017 Security Monthly Quality Rollup for Windows 8.1 for x64-based Systems (KB4012216): KB4012216- March, 2017 Security Monthly Quality Rollup for Windows Server 2012 R2 (KB4012216): KB4012216 https://technet.microsoft.com/library/security/MS17-006

Description:

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

(MS17-010) Security Update for Windows SMB Server (4013389)

Vulnerbility:		(MS17-010) Security Update for Windows SMB Server (4013389)	
Level Risk:		9.0	
Service:	microsoft-ds	**CVE:**	CVE-2017-0143

Observation:

Microsoft Windows is an industry-standard operating system. Multiple vulnerabilities are present in some versions of Microsoft Windows. The flaws lie in the way the Microsoft Server Message Block 1.0 (SMBv1) server handles requests. Successful exploitation could allow an attacker to execute arbitrary remote code or to obtain sensitive information. Exploitation requires the malicious user to send a specially crafted packet to a SMBv1 server. Microsoft has released MS17-010 to address this issue. The target appears to be missing this patch.

Recommendation:

The vendor has released an update to address these issues. https://technet.microsoft.com/library/security/MS17-010 https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Description:

Multiple vulnerabilities are present in some versions of Microsoft Windows.

Microsoft Windows IIS ASP.NET Version Detection

Vulnerbility: Microsoft Windows IIS ASP.NET Version Detection
Level Risk: 0.0
Service: http   **CVE:**   -

Observation:
Microsoft IIS ASP.NET is a software service for applications designed to run under Microsoft Windows. The server is running the Microsoft Windows IIS ASP.NET service, and the version information was obtained.

Recommendation:
Ensure that the ASP.NET service is allowed to be running on the host.

Description:
The server is running the Microsoft Windows IIS ASP.NET service, and the version information was obtained.

Microsoft IIS Server Extensions Enumerated

Vulnerbility: Microsoft IIS Server Extensions Enumerated
Level Risk: 0.0
Service: http   **CVE:**   -

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS server extensions were enumerated on the host.

Recommendation:
Ensure that Microsoft IIS complies with organizational policy.

Description:
Microsoft Internet Information Services (IIS) extensions were enumerated on the host.

LSASS RPC Interface Detected

Vulnerbility: LSASS RPC Interface Detected
Level Risk: 0.0
Service: loc-srv   **CVE:**   -

Observation:
LSASS RPC Interface Detected.

Recommendation:
It is recommended to block the following ports at the network perimeter: 135/TCP,UDP,137/UDP, 138/TCP,UDP, 139/TCP,UDP 445/TCP,UDP, 593/TCP, 1025/TCP, 1026/TCP.

Description:
LSASS RPC Interface Detected.

NetBIOS Null Session Enabled

Vulnerbility:		NetBIOS Null Session Enabled	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:

A NetBIOS null session allows users to connect to a host remotely with no username and password and perform a limited set of administrative tasks. Null sessions allow the remote user to gather information such as: 1. List users 2. List groups 3. List shares (including hidden shares) 4. Policies (such as minimum password length, etc.) While the enumerated information is not an immediate risk, much of the information can be leveraged to launch an attack to gain user or administrative privilege. All steps should be taken to eliminate the vulnerability and/or reduce the information available to the attacker. This check only attempts to establish a NetBIOS null session with the host. It does not attempt to determine what information is accessible with the null session.

Recommendation:

Disable or restrict null session access to network shares. For Windows operating systems, the configuration steps may vary based on the type of operating system and Domain or Local Security policies. Contact the operating system vendor for hardening steps specific to the operating system and setup environment. For Unix Samba based server, make sure that samba's configuration parameter "guest ok" is set to "no" and set the "restrict anonymous" parameter. Workaround: Block access to TCP port 139 (NetBIOS) and TCP port 445 using a firewallNote: Blocking access for MVM to both TCP ports 139 and 445 will also block MVM's credential based scans. This should only be done if credential based scans are not needed.

Description:

NetBIOS Null sessions are enabled on the host.

Microsoft Windows Terminal Service

Vulnerbility:		Microsoft Windows Terminal Service	
Level Risk:		0.0	
Service:	ms-term-service	**CVE:**	CVE-MAP-NOMATCH

Observation:

Terminal Services allows the remote, full-access administration of any server running Microsoft Windows. This service is optional, and can be disabled at any time. If an attacker gains a valid username and password, he can use this service to gain further access on the remote host. Windows XP uses Terminal Services to provide additional functionality such as Fast User Switch, and Remote Assistance. Vulnerable Systems: Microsoft Windows 2000, NT, XP, 2003

Recommendation:

Disable Terminal Services if not in use. Ensure that account policies for Terminal Server users is as restrictive as possible. To disable Terminal Services: For Windows 2000 and NT1. Click Start > Settings > Control Panel. 2. Double click Add/Remove programs. 3. In the Add/Remove programs window, click Add/Remove Windows Components. 4. Scroll down and click Terminal Services. Then click Next twice to remove it.

Description:

Microsoft Windows Terminal service has been detected on the target host.

Microsoft IIS Host Name Setting Enumerated

Vulnerbility:		Microsoft IIS Host Name Setting Enumerated	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:

Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS "Use Host Header Name" setting is disabled on the host.

Recommendation:

Ensure that Microsoft IIS complies with the corporate policy. Note: It is advised to enable "Use Host Header Name" setting.

Description:

Microsoft Internet Information Services (IIS) "Use Host Header Name" setting is disabled on the host.

Microsoft IIS Basic Authentication Scheme Disabled

Vulnerbility:		Microsoft IIS Basic Authentication Scheme Disabled	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:

Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS Basic Authentication scheme is disabled on the host.

Recommendation:

Ensure that Microsoft IIS complies with the corporate policy.

Description:

Microsoft Internet Information Services (IIS) Basic Authentication scheme is disabled on the host.

VNC Server Detected

Vulnerbility:		VNC Server Detected	
Level Risk:		0.0	
Service:	vnc	**CVE:**	CVE-MAP-NOMATCH

Observation:

An open VNC connection will allow an attacker to obtain sensitive information about the host and possibly gain access to the system.

Recommendation:

A VNC Server application was detected. The affected system should be examined to determine which VNC application is installed. Once determined, it should be removed unless being used for legitimate business purposes. To uninstall VNC for Windows NT/2000/XP: ----- To uninstall using the Add/Remove Programs control panel: 1. Go to the Start menu, select Settings and then Control Panel. 2. Double-click the Add/Remove Programs icon. 3. Select VNC. 4. Click the Add/Remove button.

Description:

A VNC server has been detected on the host.

Microsoft IIS NTLM Authentication Disabled

Vulnerbility: Microsoft IIS NTLM Authentication Disabled
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS NTLM Authentication is disabled on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: It is advised to enforce NTLM authentication for Microsoft IIS.

Description:
Microsoft Internet Information Services (IIS) NTLM Authentication is disabled on the host.

Microsoft IIS Server Detected

Vulnerbility: Microsoft IIS Server Detected
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS was detected on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: Conceal the IIS Server status by modifying the banner.

Description:
Microsoft Internet Information Services (IIS) was detected on the host.

Microsoft IIS Anonymous Access Enabled

Vulnerbility: Microsoft IIS Anonymous Access Enabled
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS anonymous access is enabled.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy.

Description:
Microsoft Internet Information Services (IIS) anonymous access is enabled.

Microsoft Terminal Service Has Not Been Configured Network Level Authentication

Vulnerbility:		Microsoft Terminal Service Has Not Been Configured Network Level Authentication	
Level Risk:		0.0	
Service:	ms-term-service	**CVE:**	-

Observation:

The target is running Microsoft Terminal Service and the Terminal Service has not been configured Network Level Authentication. Network Level Authentication provides better security than previous authentication approach.

Recommendation:

Consider to configure the Terminal Service to use Network Level Authentication if possible.More details could be found at: http://technet.microsoft.com/en-us/library/cc732713.aspx

Description:

The target is running Microsoft Terminal Service and the Terminal Service has not been configured Network Level Authentication.

NetBIOS NBTSTAT -A

Vulnerbility:		NetBIOS NBTSTAT -A	
Level Risk:		0.0	
Service:	netbios-ns	**CVE:**	CVE-MAP-NOMATCH

Observation:

All Microsoft Windows platforms include support for the NetBIOS network protocol stack. The NetBIOS protocol provides the underlying support for Microsoft Windows file and resource sharing. One component of all Microsoft Windows NetBIOS implementations is the NetBIOS Name Service.The NetBIOS Name Service listens for name service requests on UDP port 137. It can be queried to retrieve a listing of currently logged in user accounts and groups. In addition, the MAC address for the network interface over which the query is performed is included in the response to a nbtstat -A request. The DOS nbtstat command can be used to perform this operation. To do so, open a DOS command prompt and run the following command: nbtstat -A target_system Where target_system is the IP address or hostname of the target system.

Recommendation:

Disable the NetBIOS Name Service to prevent access to NBTSTAT -A informationWorkaround: Block access to UDP port 137 using a firewall. Contact the operating system vendor for hardening steps specific to the operating system.

Description:

It is possible to retrieve NetBIOS Name Service information.

Microsoft ASP.NET HTTP Handlers Enumeration

Vulnerbility: Microsoft ASP.NET HTTP Handlers Enumeration

Level Risk: 0.0

Service: http   **CVE:**   -

Observation:

Microsoft .NET is a Software Framework for applications designed to run under Microsoft Windows. HTTP handlers in ASP .NET are used for processing different kinds of file types(file extensions). A list of file extensions handled by the ASP.NET server was obtained.

Recommendation:

Ensure that the list of file extension handlers found on the ASP.NET server is allowed by policy.

Description:

A list of file extensions handled by the ASP.NET server was obtained.

Web Server HTTP Protocol Version Detected

Vulnerbility: Web Server HTTP Protocol Version Detected

Level Risk: 0.0

Service: http   **CVE:**   -

Observation:

Web servers are widely used to serve static and dynamic content and render it in the client's browser. HTTP protocol version was obtained from the host through web server.

Recommendation:

Ensure that web server complies with organizational policy.

Description:

HTTP protocol version was obtained from the host through web server.

NetBIOS Names Information Accessible

Vulnerbility: NetBIOS Names Information Accessible

Level Risk: 0.0

Service: netbios-ns   **CVE:**   -

Observation:

Microsoft NetBIOS is a service developed to communicate with different computers over a local network.Microsoft NetBIOS names information was detected on the host.

Recommendation:

Ensure that Microsoft NetBIOS complies with organizational policies.

Description:

Microsoft NetBIOS names information was detected on the host.

Microsoft Remote Procedure Call Service Detected

Vulnerbility: Microsoft Remote Procedure Call Service Detected

Level Risk: 0.0

Service: loc-srv   **CVE:**   -

Observation:

Microsoft Remote Procedure Call Service (MSRPC) service is the DCE RPC mechanism implemented by Microsoft. It supports inheritance of interfaces, Unicode strings and implicit handles. Microsoft Remote Procedure Call Service was detected on the host.

Recommendation:

Ensure that MSRPC complies with organizational policy.

Description:

Microsoft Remote Procedure Call Service was detected on the host.

Microsoft ASP.NET State Service Detected

Vulnerbility: Microsoft ASP.NET State Service Detected

Level Risk: 0.0

Service: http   **CVE:**   -

Observation:

The Microsoft ASP.NET State Service is used to manage session state on computerMicrosoft ASP.NET State Service was detected on the host.

Recommendation:

Ensure that Microsoft ASP.NET State service complies with corporate policy.

Description:

Microsoft ASP.NET State Service was detected on the host.

NetBIOS Bindings Information Detected

Vulnerbility: NetBIOS Bindings Information Detected

Level Risk: 0.0

Service: netbios-ns   **CVE:**   -

Observation:

NetBIOS is a service which allows different computers to communicate with each other over a local area network.NetBIOS bindings information was detected on the host.

Recommendation:

Ensure that NetBIOS service complies with organizational policies.

Description:

NetBIOS bindings information was detected on the host.

Hidden WWW Server Name Detected

Vulnerbility:	Hidden WWW Server Name Detected
Level Risk:	0.0
Service: http	**CVE:** -

Observation:

WWW server is a computer application for delivering web based contents using HTTPHidden WWW server name detected. Web server name can be hidden as a security measure.

Recommendation:

Ensure that web server complies with corporate policy.

Description:

Hidden WWW server name detected.