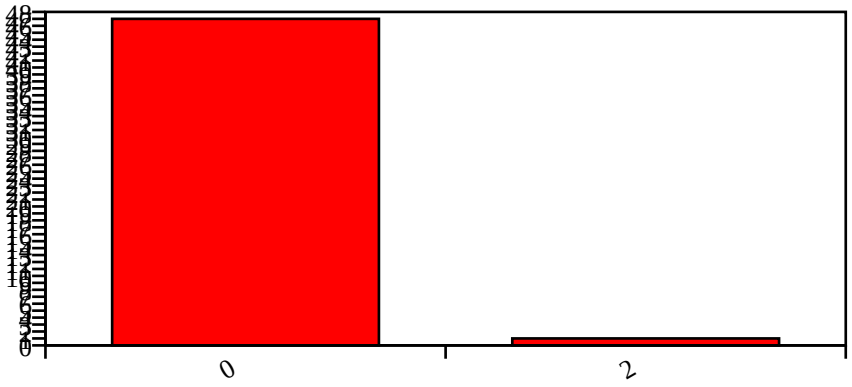
JosiaBasicNetwork

Scan Start: None

Scan End: None

Executive Summary

Severity Level	Count
0	47
2	1



Detailed Report

Assets Information

Asset IP	Hostname	Operating System	MAC Address
10.147.160.11	JOSIAH-DELL	Microsoft Windows 7 Professional	A0:CE:C8:C5:80:FB

Vulnerability Details

us to log into it or some other problem occurred.
se using the credentials that have been provided.
ote that these are only the alternate hostnames for vhosts discovered on a web server.
ardware and software products found on a host.
nformation available from the scan.
r, general-purpose computer, etc).
It is also possible sometimes to guess the version of the operating system.
e registered by IEEE.
hen consolidates the MAC addresses into a single, unique, and uniform list.
so be reachable through SOAP requests.
so be reachable through SOAP requests.
e-middle attacks against the SMB server.
receives a 'HELP' request.
st is running VMware Server, ESX Server, or GSX Server.
st is running VMware Server, ESX Server, or GSX Server.
t receives an HTTP request.
t receives an HTTP request.

request to port 139 or 445.
remote host can sometimes be computed.
erating system type and exact version, its hostname, and the list of services it is running. as Nessus.
BIOS or DNS. It is enabled by default on modern Windows versions.
arily intended for home networks. An attacker could potentially leverage this to discover your network architecture.
at affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that
quest to port 139 or 445.
ntials do not have administrative privileges. l or not. This is the method Microsoft recommends to determine if a patch has been applied. when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).
abled on the remote host or can not be connected to with the supplied credentials.
g virtualization software, a VPN client, or has multiple network interfaces.
alled target. o leave unclosed connections on the remote target, if the network is loaded.
alled target. o leave unclosed connections on the remote target, if the network is loaded.
alled target. o leave unclosed connections on the remote target, if the network is loaded.
alled target. o leave unclosed connections on the remote target, if the network is loaded.
alled target. o leave unclosed connections on the remote target, if the network is loaded.
alled target. o leave unclosed connections on the remote target, if the network is loaded.
alled target. o leave unclosed connections on the remote target, if the network is loaded.

g into it using one of the following accounts :
r 445. Note that this plugin requires SMB1 to be enabled on the host.
SMB requests. te a report.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
his information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
access to files, printers, etc between nodes on a network.
access to files, printers, etc between nodes on a network.