Qualys. Community Edition

Scan Results

December 21, 2023

Report Summary	
User Name:	Khadijah Watkins
Login Name:	crena6kw
Company:	log
User Role:	Manager
Address:	44 freshmont st
State:	Hawaii
Zip:	89142
Country:	United States of America
Created:	12/21/2023 at 04:07:30 (GMT)
Launch Date:	12/21/2023 at 03:29:40 (GMT)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1703129381.35037
Scanner Appliances:	kdee (Scanner 12.16.55-1, Vulnerability Signatures 2.5.940-4)
Duration:	00:00:04
Title:	basicvm - 20231221
Asset Groups:	-
IPs:	192.168.0.4
Excluded IPs:	-
Options Profile:	basicnetscan

Summary of Vulnerabilities

Vulnerabilities Total	20

Security Risk (Avg)	2.0

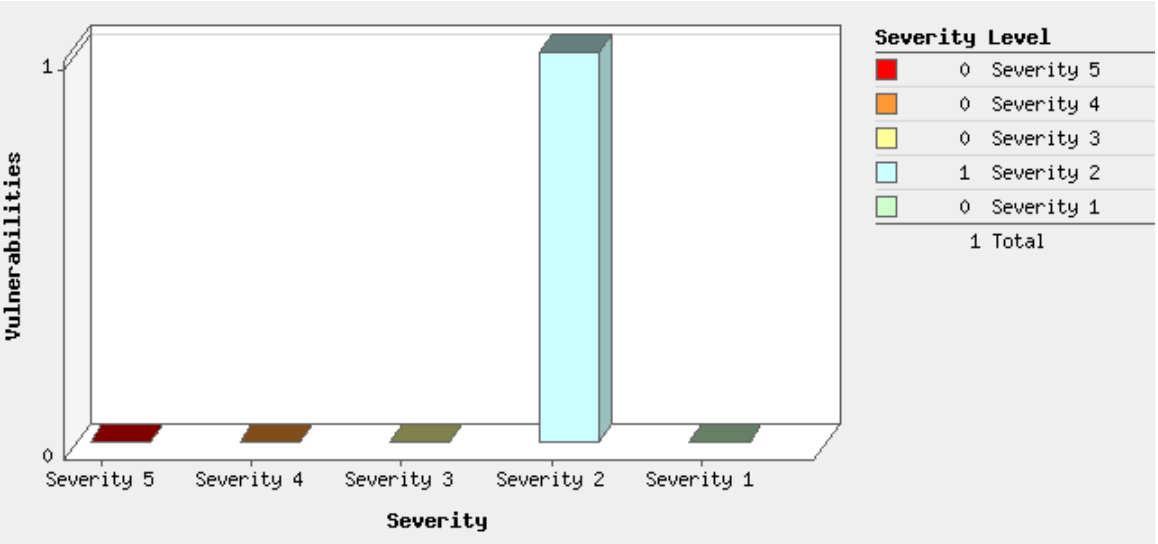
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	1	1
2	1	0	3	4
1	0	0	15	15
Total	1	0	19	20

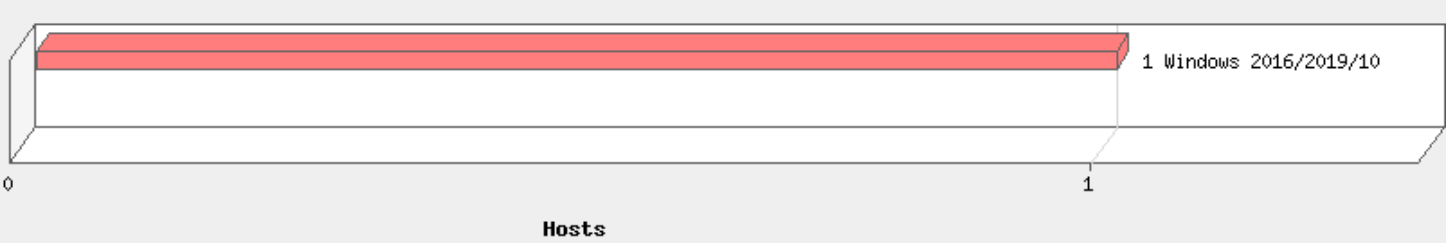
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
TCP/IP	0	0	7	7
Information gathering	0	0	6	6
SMB / NETBIOS	1	0	4	5
Windows	0	0	1	1
Hardware	0	0	1	1
Total	1	0	19	20

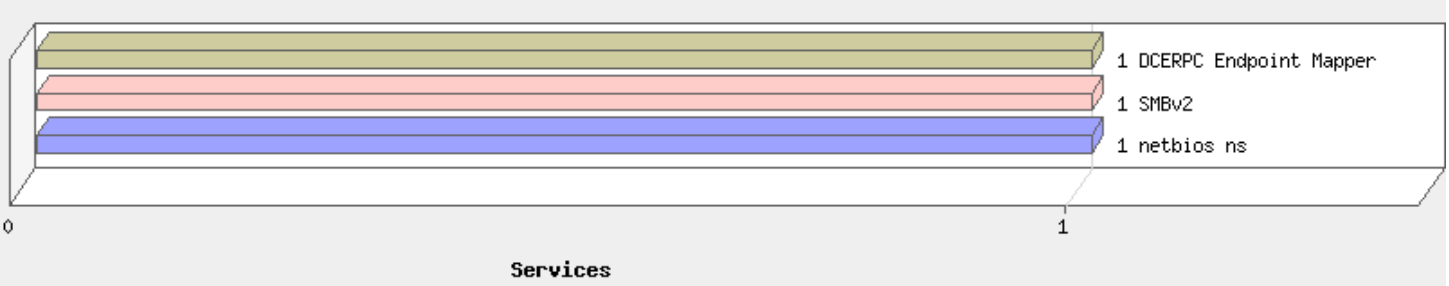
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

192.168.0.4 (win10, WIN10) Windows 2016/2019/10

Vulnerabilities (1)

2 NetBIOS Name Accessible

QID:	70000
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2009
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:

Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:

If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WIN10

Information Gathered (19)

3 NetBIOS Bindings Information

QID:	70004
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following bindings were detected on this computer. Bindings have many purposes. They reflect such things as users logged-in, registration of a user name, registration of a service in a domain, and registering of a NetBIOS name.

IMPACT:

Unauthorized users can use this information in further attacks against the host. A list of logged-in users on the target host/network can potentially be used to launch social engineering attacks.

SOLUTION:

This service uses the UDP and TCP port 137. Typically, this port should not be accessible to external networks, and should be firewalled.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Service	NetBIOS Suffix
WIN10	File Server Service	0x20
WIN10	Workstation Service	0x0
WORKGROUP	Domain Name	0x0
WORKGROUP	Browser Service Elections	0x1e
WORKGROUP	Master Browser	0x1d
.._MSBROWSE__.	Master Browser	0x1

2 Operating System Detected

QID:	45017
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/18/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016/2019/10	NTLMSSP	
Windows 10	TCP/IP Fingerprint	U7119:135

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Microsoft Scheduler Control Service	1.0				\PIPE\atsvc
Microsoft Security Account Manager	1.0	49664			\pipe\lsass
Microsoft Service Control Service	2.0	49670			
Microsoft Spool Subsystem	1.0	49669			
Microsoft Task Scheduler	1.0				\PIPE\atsvc
Ngc Pop Key Service	1.0	49664			\pipe\lsass
KeyIso	2.0	49664			\pipe\lsass
(Unknown Service)	1.0	49665			\PIPE\InitShutdown
(Unknown Service)	1.0				\PIPE\InitShutdown
Event log TCPIP	1.0	49666			\pipe\eventlog
(Unknown Service)	1.0	49667			\PIPE\atsvc
(Unknown Service)	2.0				\PIPE\atsvc
(Unknown Service)	1.0	49669			
DfsDs service	1.0				\PIPE\wkssvc
Remote Fw APIs	1.0	54847			
Vpn APIs	1.0				\PIPE\ROUTER

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

 1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
192.168.0.4	No registered hostname

1 Network Adapter MAC Address

QID:	43007
Category:	Hardware
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

It is possible to obtain the MAC address information of the network adapters on the target system. Various sources such as SNMP and NetBIOS provide such information. This vulnerability test attempts to gather and report on this information in a table format.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Method	MAC Address	Vendor
NBTSTAT	08:00:27:4F:9D:04	CADMUS COMPUTER SYSTEMS

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The

Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 294 seconds

Start time: Thu, Dec 21 2023, 02:59:15 GMT

End time: Thu, Dec 21 2023, 03:04:09 GMT

 1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/27/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
win10	NTLM DNS
WIN10	NTLM NetBIOS

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/22/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:

N/A

SOLUTION:

For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SMB Version 2 detected on TCP port 445.

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:01:22
TCP	445	0:01:22
UDP	137	0:00:56
UDP	138	0:00:07
UDP	500	0:00:12
UDP	1900	0:00:12

 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled

Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
500	isakmp	isakmp	unknown
1900	unknown	unknown	unknown

 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/20/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	

445	microsoft-ds	Microsoft-DS	SMBv2

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	02:31:40 GMT
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1041	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 40423	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 12346	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7000	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1807	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable
Unreachable (type=3 code=3)	UDP Port 40422	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 135	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 12345	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 54321	Port Unreachable

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/21/2005

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WIN10

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1347698335 with a standard deviation of 979316831. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(10734 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 41 milli seconds

1 NetBIOS Workgroup Name Detected

QID:	82062
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/02/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS workgroup or domain name for this system has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WORKGROUP

Appendix

Hosts Scanned (IP)

192.168.0.4

Target distribution across scanner appliances

kdee : 192.168.0.4

Options Profile

basicnetscan

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Purge old host data when OS changes:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco/Network SSH:	Disabled
Unix Least Privilege Authentication:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Sybase:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled

Neo4j:	Disabled
NGINX:	Disabled
Infoblox:	Disabled
BIND:	Disabled
Cisco_APIC:	Disabled
Overall Performance:	Normal
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.

Severity	Level	Description
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.