



**www.SecPoint.com**

**00:24:02 2 Apr 2011 Central European Time**

**Scan of:  
Local net 26 april 2011**

**Confidential**

**© SecPoint ® 1999-2011**

# ***Table of Contents***

Front page . . . . .	1
Table of Contents . . . . .	2
Introduction . . . . .	3
Vulnerability details . . . . .	4
Analysis for host 192.168.1.20 . . . . .	5
Executive Summary . . . . .	5
Identified Ports and Services . . . . .	7
Traceroute . . . . .	8
Version Banner identified . . . . .	9
Summary of vulnerabilities found . . . . .	10

## ***Introduction***

This report is the result of an "online vulnerability assessment scan", performed using the "**SecPoint® Penetrator**".

This document has been compiled and arranged to provide a quick and easy-to-understand report to simplify the task of securing computer systems and IT equipment connected to the Internet.

System vulnerabilities are categorised under one of three headings: **High risk, Medium risk or Low risk.**

A detailed explanation of each category of vulnerability can be found under the heading of "**Vulnerability Details**".

An **Executive Summary** has been compiled specifically for a management level review. This summary contains both written and graphic details based upon the results of the scanner. These results include such information as "when the scan was performed", "who performed the scan", and the amount of system vulnerabilities found in each category.

The **Executive Summary** also includes a conclusion reporting the "overall security level" of the tested system.

Details and names of vulnerabilities discovered are found under the heading of "**Summary of vulnerabilities found**". This is followed by individual descriptions for fixing each found vulnerability.

Where possible, a **Bugtraq ID** and/or **CVE** is present verifying the existence of the discovered vulnerabilities.

**Bugtraq ID is the official Securityfocus.com ID; Also known as bugtraq.**  
**CVE is the official CVE Mitre list.**

**Every system vulnerability discovered is supplied with a possible remedy.**

## ***Vulnerability details***

### **Vulnerabilities categorised**

#### **High Risk Vulnerability Information**

When a high risk vulnerability is identified, it means that it is possible for an intruder to penetrate and compromise the system fully and/or gain access to highly sensitive system information. This in turn could lead to theft or loss of private and sensitive data.

#### **Medium Risk Vulnerability Information**

When a medium Risk vulnerability is identified, it means that an intruder can gain access to system information that could lead to more specific attacks and possibly a full system compromise. This in turn could lead to theft of loss of private or sensitive data.

#### **Low Risk Vulnerability Information**

When a low risk vulnerability is identified, it generally means that an intruder can gain access to system information that can aid and lead to more specific attacks resulting in the theft or loss of private and sensitive data.

# ***Analysis for host 192.168.1.20***

## ***Executive Summary***

### **General information**

Scan was performed for:	www.SecPoint.com
Scan of IP number:	192.168.1.20
Scan was started at:	00:24:02 2 Apr 2011 Central European Time
Scan ended at:	01:15:26 2 Apr 2011 Central European Time
Duration:	00:51:24 Minutes
Performed by:	SecPoint® Penetrator 8.6.5.25

**Overall Security Level: Cat 1 (Critical level)**

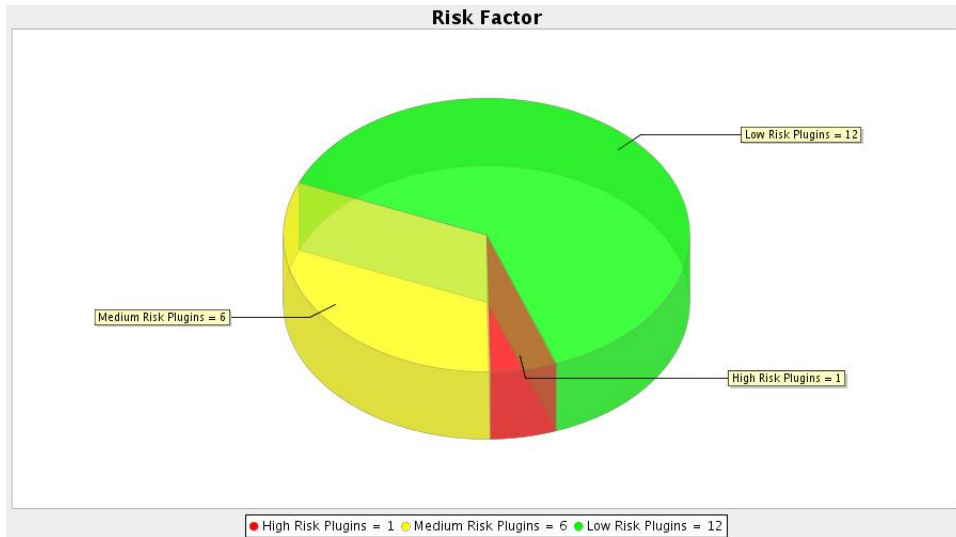
### **Vulnerabilities**

19 potential vulnerabilities identified.

The vulnerabilities divide in the following way:

### **Conclusion**

SecPoint® Penetrator has determined that your system security level is dangerously low. It is possible for intruders to fully penetrate the system which can result in loss of private and sensitive data. It is recommended that you take immediate action to improve the security level.



## Identified Ports and Services

The following "Ports and Services" could be identified remotely over the Internet.

Port	Protocol	Service
21	tcp	File Transfer [Control]
135	tcp	DCE endpoint resolution
139	tcp	NETBIOS Session Service
445	tcp	Microsoft-DS
912	tcp	APEX relay-relay service
3261	tcp	winShadow
3260	tcp	iSCSI port
3389	tcp	MS WBT Server
137	udp	
123	udp	

## ***Traceroute***

This is the result of a traceroute from the SecPoint® Penetrator system to the target IP address:

traceroute to 192.168.1.20 (192.168.1.20), 15 hops max, 60 byte packets

1 192.168.1.20 (192.168.1.20) 0.427 ms 0.390 ms 0.292 ms

## ***Version Banner identified***

The following Service Version Banner outputs were readable remotely over the internet. It is highly recommended to reconfigure these banners with bogus or no information at all.

**Alco Version Banner: [2JStarWind Alcohol Edition iSCSI Target v12.1 (Build 20091211, Win32);Copyright (c) StarWind Software 2003-2009. All rights reserved.;;**

### **Recommended solution**

It is highly adviceable to configure this output to return bogus or no information at all. If you have already done that please ignore this warning.

Port: 3261/tcp

**Ftp Version Banner: 220 VMware Authentication Daemon Version 1.0, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC ,**

### **Recommended solution**

It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Port: 912/tcp

**Ftp Version Banner: 220-FileZilla Server version 0.9.34 beta;220-written by Tim Kosse (Tim.Kosse@gmx.de)**

### **Recommended solution**

It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Port: 21/tcp

## ***Summary of vulnerabilities found***

### **Vulnerabilities found:**

#### **High risk vulnerabilities**

- NetBIOS Registry Accessible

#### **Medium risk vulnerabilities**

- Default Administrator Account Identified
- Default Guest Account Identified
- NetBIOS User Name Retrieval #1
- Netbios NULL Session possible No password set
- Windows Terminal Services
- winShadow Server Port / Alcohol120

#### **Low risk vulnerabilities**

- All Protocols Tested
- It is possible to obtain remote NetBIOS name table.
- MAC address obtained via NetBIOS
- NetBIOS service listening 137 UDP
- NetBIOS service listening 139 TCP
- NetBIOS service listening 445 UDP
- Ntpd Service found PORT 123 TCP
- Remote system answers to PING command
- Remote system time via NetBIOS.
- System Time Revealed via. ICMP TimeStamp
- System type guessed via remote FTP Server Check #2
- Windows XP Identified on the remote System

## **NetBIOS Registry Accessible**

**Risk: High**

**SecPoint ID: 2577**

### **Impact**

It is possible on the remote system to access the Windows Registry via the NetBIOS service. An attacker can by this gain sensitive information from the target system.

### **Recommended solution**

It is recommended to block incoming traffic to the NetBIOS service running on the UDP ports 135,136,137,139,445 TCP ports 135,136,137,139,445.

## Default Administrator Account Identified

**Risk: Medium**

**SecPoint ID: 1773**

**CVE: CAN-1999-0585**

### Impact

The default Windows Administrator account has been found to be Administrator on this host. In more secure network environments, companies ensure that the Administrator username is changed to LocalAdmin, CompanyAdmin, or other names that are not easy to guess. Brute force attacks can be launched via POP3, NetBIOS or other access services to compromise the Administrator account.

### Recommended solution

It is recommended that the Administrator account username is changed by following these steps  
WINDOWS

-

- 1 Load User Manager from Administrative Tools under the Control-Panel
- 2 Select the Administrator account
- 3 Select Rename option from under the User menu

## Default Guest Account Identified

**Risk: Medium**

**SecPoint ID: 1773**

**CVE: CAN-1999-0585**

### Impact

The default Windows Guest account has been found to be active on this host. In more secure network environments, companies ensure that the Guest account is deactivated or deleted entirely. Brute force attacks can be launched via. POP3, NetBIOS or other access services to compromise the Guest account.

### Recommended solution

It is recommended that the Guest account is changed by following these steps  
WINDOWS

-

- 1 Load User Manager from Administrative Tools under the Control-Panel
- 2 Select the Guest account
- 3 Either rename, delete, or deactivate the account by using the relevant options

## NetBIOS User Name Retrieval #1

**Risk: Medium**

**SecPoint ID: 1772**

### Impact

It is possible to query NetBIOS Windows file sharing services running on The identified TCP port to gain a list of and other NetBIOS information. Determined attackers can use this information to launch effective brute-force attacks against shared resources.

### Recommended solution

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via the identified TCP port. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.

### Vulnerability output / evidence

Administrator

ASPNET

BitDefenderComm

Guest

HelpAssistant

null

SecPoint

SUPPORT\_388945a0

\_\_vmware\_user\_\_

## **Netbios NULL Session possible No password set**

**Risk: Medium**

**SecPoint ID: 2349**

### **Impact**

It is possible on the remote netbios system to connect with no valid user name or password. This can allow any attacker to connect to your system.

### **Recommended solution**

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.

## Windows Terminal Services

**Risk: Medium**

**SecPoint ID: 2390**

**Bugtraq ID: 3541**

**Bugtraq ID: 4464**

**CVE: CAN-2002-0444**

**CVE: CVE-2001-0860**

**Port: 3389/tcp**

### Impact

The Terminal Services has been found running. Terminal Services is used to remotely obtain a graphical login interface. If an attacker has gained a valid login and password the attacker can be able to use this service to gain further access on the remote system. The identified service is also known to a remote Denial of Service vulnerability.

### Recommended solution

Either disable the Terminal Services from Start->Control-Panel->Administrative Tools->Service and find it and set it to disable and or block incoming TCP traffic to the identified port. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.

### Vulnerability output / evidence

Please note in this check we only relied on the presence of the found port.

## winShadow Server Port / Alcohol120

**Risk: Medium**

**SecPoint ID: 4086**

**Bugtraq ID: 8719**

**Bugtraq ID: 8720**

**Port: 3261/tcp**

### Impact

The identified port found on the remote system is known to be the OmniCom winShadow Server port. This service is known to be subject to a remote Buffer overflow vulnerability. This can allow an attacker to execute arbitrary code on the target system and or crash the service.

### Recommended solution

Please upgrade to the latest version of this software from <http://www.omnicomtech.com/> and there click on Download. Further more it is recommended to only allow incoming traffic to trusted ip addresses. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.

### Vulnerability output / evidence

Please note in this check we only relied on the presence of the found port.

## All Protocols Tested

**Risk: Low**

**SecPoint ID: 8311**

### Impact

This check probes all ports for their real protocols. If all matches as it should be please ignore this check.

### Recommended solution

If there is found known services on unknown ports it is recommended to properly test those ports.

### Vulnerability output / evidence

Protocol on 192.168.1.20:135/tcp matches netbios-session

Protocol on 192.168.1.20:139/tcp matches netbios-session

Protocol on 192.168.1.20:445/tcp matches ms-ds

Protocol on 192.168.1.20:912/tcp matches vmware-authd

Protocol on 192.168.1.20:912/tcp matches ftp

## It is possible to obtain remote NetBIOS name table.

**Risk: Low**

**SecPoint ID: 1770**

### Impact

Attackers can use this information to base other attacks on.

### Recommended solution

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.

### Vulnerability output / evidence

Name	Service	Type
SECPOINT-DELL	Workstation Service	
WORKGROUP	Domain Name	
SECPOINT-DELL	File Server Service	
WORKGROUP	Browser Service Elections	

## MAC address obtained via NetBIOS

**Risk: Low**

**SecPoint ID: 1771**

### Impact

It is possible on the remote target via NetBIOS to retrieve the MAC address. The MAC address is the physical address on the netcard. An attacker can use this number to spoof on the attackers own netcard and do hacks which will look like to be done with your netcard.

### Recommended solution

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.

### Vulnerability output / evidence

MAC Address: 00-01-03-be-5e-7b

## NetBIOS service listening 137 UDP

**Risk: Low**

**SecPoint ID: 1990**

**Port: 137/udp**

### Impact

The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.

### Recommended solution

#### WINDOWS

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presence of the identified port. Some systems are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.

### Vulnerability output / evidence

Please note in this check we only relied on the presence of the found port.

## NetBIOS service listening 139 TCP

**Risk: Low**

**SecPoint ID: 1990**

**Port: 139/tcp**

### Impact

The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.

### Recommended solution

#### WINDOWS

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presence of the identified port. Some systems are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.

### Vulnerability output / evidence

Please note in this check we only relied on the presence of the found port.

## NetBIOS service listening 445 UDP

**Risk: Low**

**SecPoint ID: 1990**

**Port: 445/tcp**

### Impact

The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.

### Recommended solution

#### WINDOWS

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. Further more to stop the listening on TCP and UDP port 445 in Regedit please goto:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters And in the TransportBindName remove the "\Device\" value. It can also be done by opening the Network and Dial-Up Connections applet and there select Advanced and Advanced Settings. There deselecting File And Printer Sharing for Microsoft Networks. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.

### Vulnerability output / evidence

Please note in this check we only relied on the presence of the found port.

## **Ntpd Service found PORT 123 TCP**

**Risk: Low**

**SecPoint ID: 25**

**Bugtraq ID: 2491**

**Bugtraq ID: 2540**

**CVE: CVE-2001-0414**

**Port: 123/udp**

### **Impact**

The Ntpd service is normally listening on TCP or UDP port 123. This service is used for time/date synchronozation. Severale remotely buffer overflows is known to exist in this service.

### **Recommended solution**

If you do not use this service block incoming TCP/tcp traffic to port 123 and or upgrade to the latest version of your Ntpd service. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.

### **Vulnerability output / evidence**

Please note in this check we only relied on the presence of the found port.

## Remote system answers to PING command

**Risk: Low**

**SecPoint ID: 2853**

### Impact

The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.

### Recommended solution

It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .

### Vulnerability output / evidence

64 octets from 192.168.1.20: icmp\_seq=0 ttl=128 time=0.5 ms

## Remote system time via NetBIOS.

**Risk: Low**

**SecPoint ID: 1707**

### Impact

Attackers can misuse this time information to bypass timebased intrusion detection. \*NOTE\* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.

### Recommended solution

Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) ->

Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.

### Vulnerability output / evidence

Sat Apr 2 00:45:42 2011 Timezone is UTC+2.0

## System Time Revealed via. ICMP TimeStamp

**Risk: Low**

**SecPoint ID: 1746**

**CVE: CAN-1999-0524**

### Impact

By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be 15:04:40. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). \*NOTE\* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.

### Recommended solution

At network-level this traffic should be rejected both inbound and outbound.

#### UNIX/FIREWALL

ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly.

#### WINDOWS

This can be a hard option to set at the current time and it is therefore recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.

## **System type guessed via remote FTP Server Check #2**

**Risk: Low**

**SecPoint ID: 7351**

**Port: 21/tcp**

### **Impact**

It is possible on the remote FTP Server to request a SYST command that revealed the operating system running. An attacker can use this information to base other attacks on.

### **Recommended solution**

It is recommended to disable the SYST command in your FTP Server if it is allowed. If it is not allowed please contact your vendor for a workaround or a new version of the ftp software.

### **Vulnerability output / evidence**

215 UNIX emulated by FileZilla

## Windows XP Identified on the remote System

**Risk: Low**

**SecPoint ID: 3234**

### Impact

It is possible to identify the remote system to be Windows XP via the NetBIOS services. An attacker can use this information to base other attacks on.

### Recommended solution

It is recommended to block incoming traffic to the NetBIOS service running on the UDP ports 135,136,137,139,445 TCP ports 135,136,137,139,445

### Vulnerability output / evidence

Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]