

Forum:[Hack Forums](#)

Thread: [Stuck on local network access win 10 need help!](#)

T1kBg - January 13, 2022, 5:55 pm

Hello ! I'm trying to find a way to access 3 windows 10 machines on a local network. No physical access. I try bind_tcp attack try smb .. no NULL shares .. trying brute force on RDP but the password and username that shows are not the real ones... trying MITf but nothing ...open ports .. 135;149;445;808;3389 I'm new to this so take it easy with me :)

linkinpork - January 13, 2022, 11:27 pm

(Jan 13, 2022 06:55 PM)T1kBg Wrote: [\[CITE\]](#) ...open ports .. 135;149;445;808;3389 I'm new to this so take it easy with me :)

Try this nmap/zenmap argument:

Code -sV -p- -T4 --script vulners <TARGET IP ADDRESS>

Put all effort into enumeration stage and attack surface mapping until you find a proper attack vector. If you want structure in your attack, check out this post: [RE: Website hacking](#)

T1kBg - January 14, 2022, 12:09 am

well i've go new ports... 10x for the heads up :)

Nmap scan report for 192.168.0.117

Host is up (0.044s latency).

Not shown: 65519 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

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

445/tcp	open	microsoft-ds?	
---------	------	---------------	--

808/tcp	open	mc-nmf	.NET Message Framing
---------	------	--------	----------------------

5040/tcp	open	unknown	
----------	------	---------	--

7070/tcp	open	ssl/realserver?	
----------	------	-----------------	--

7680/tcp	open	pando-pub?	
----------	------	------------	--

8197/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
----------	------	------	---

_http-server-header: Microsoft-HTTPAPI/2.0

8666/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
----------	------	------	---

_http-server-header: Microsoft-HTTPAPI/2.0

49664/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49665/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49666/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49667/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49675/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49677/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49679/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

MAC Address: (ASRock Incorporation)

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

linkinpork - January 14, 2022, 12:31 am

(Jan 14, 2022 01:09 AM)T1kBg Wrote: [\[CITE\]](#) well i've go new ports... 10x for the heads up :)

Nmap scan report for 192.168.0.117

snip

You have SMBv3 on port 139 and 445. Here's something to help you with that:

<https://www.hackingarticles.in/a-little-guide-to-smb-enumeration/>

It might also help if you checked out the UDP ports, not just the TCP ones. It will definitely take longer though, so I suggest you do it in a separate window:

Code -sV -sU -T4 -v <TARGET IP ADDRESS>

EDIT: It really helps to learn how to speak SMB. It's similar to speaking FTP, with some difference in authentication. Here's a cheatsheet:

<https://www.willhackforsushi.com/sec504/SMB-Access-from-Linux.pdf>

T1kBg - January 14, 2022, 1:02 am

I try this all ready but nothing... i get no Null Session or

```
+- $ smbmap -H 192.168.0.114
```

```
[!] Authentication error on 192.168.0.114
```

and stuck on entering root password... :(

Trying brute force on RDP but my laptop is showing 3568 days to finish :D

trying from msfconsole bind_tcp attack and i get sessions is dead

linkinpork - January 14, 2022, 1:33 am

(Jan 14, 2022 02:02 AM)T1kBg Wrote: [\[CITE\]](#) I try this all ready but nothing... i get no Null Session or

```
+- $ smbmap -H 192.168.0.114
```

```
[!] Authentication error on 192.168.0.114
```

and stuck on entering root password... :(

Trying brute force on RDP but my laptop is showing 3568 days to finish :D

trying from msfconsole bind_tcp attack and i get sessions is dead

You're exploiting already :(That's like, one of the last parts. Keep enumerating until you're very sure it's vulnerable. Use scanners, fuzzers, banner grabbers, whatever.

Relevant:

EDIT:

Here's a resource you might like. Check the list under "Active Recon Tools":

<https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/>

For perspective, many long-term breaches done by hacker groups take 200 to 300 days before being completely contained. Your typical script only takes seconds to verify shell. You have all the time in the world :)

Marcus Lauren - January 15, 2022, 6:55 pm

Thats a good suggestion. Many breaches do take a lot of time before they actually get into the computers.Keep bruteforcing.

PS : The cheatsheet wouldnt work if the PC owner isnt native english speaker , as the password could be in english but with their native language meaning.

Why isnt MITM working? Did you try scanning their router open ports as well? You can perhaps bruteforce into it and could launch MITM

T1kBg - *January 18, 2022, 7:29 am*

The mitmf attack faild because inside the network are 3 miners and i get flooded .. i have access to the router minera and everything else except the pc's Is there any tipe of way that i can get some information from the miners or a printer?