

Ex050

Gary Jones

Contents

Technical Report	2
Introduction	2
Finding: <i>Descriptive Name</i>	2
Risk Rating	2
Attack Narrative	2

Technical Report

Introduction

Finding: *Descriptive Name*

Risk Rating

Two risks were identified. The first was a backdoor command found in the vsftpd 2.3.4 software which is a major risk and the second is a local privilege escalation software present in the Apache 2.4.17 software which is a medium risk.

Attack Narrative

Utilizing the nmap tool www.artstailor.com was probed and 4 ports were found to be open (see figures 1 and 2). When the OS was probed the results were inconclusive (see figure 2). These results were found by probing with TCP.

When nmap was used to probe www.artstailor.com with UDP the only open port found with 21 (see figure 3). Between the two types of scan UDP took longer than TCP and resulted in fewer observations.

While working in groups our team observed that some members had port 40 appear in their probe while others did not. This led the team to investigate further into this port (see figures 4 and 5) a response was observed coming from it yielding a key value: KEY007-9sGDcP6yOz9NqfkXEmX43A==

Utilizing nmap and searchsploit our team was able to identify two exploits (see figure 6). These exploits are with a backdoor present in the vsftpd 2.3.4 code and a local privilege escalation present in the Apache 2.4.17 code.

```

(kali@kali)-[~]
└─$ nmap -sT www.artstailor.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 20:07 EDT
Nmap scan report for www.artstailor.com (217.70.184.38)
Host is up (0.00022s latency).
rDNS record for 217.70.184.38: ns.artstailor.com
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds

```

Figure 1:

```

(kali@kali)-[~]
└─$ sudo nmap -sT -O www.artstailor.com
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 20:14 EDT
Nmap scan report for www.artstailor.com (217.70.184.38)
Host is up (0.00053s latency).
rDNS record for 217.70.184.38: ns.artstailor.com
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91E=4%D=9/29%OT=21%CT=1%CU=33826%PV=N%DS=2%DC=I%G=Y%TM=6155016
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%
OS:DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=5)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.61 seconds

```

Figure 2:

The screenshot shows a network traffic analysis tool interface. On the left, a packet capture table is visible with columns for No., Time, Source, Destination, Protocol, and Len. The main window displays the output of an nmap scan on 217.70.184.38, including a table of open ports and OS detection details.

No.	Time	Source	Destination	Protocol	Len
2032	15.488547939	217.70.184.38	172.24.0.10	TCP	60
2033	15.488547966	217.70.184.38	172.24.0.10	TCP	60
2035	15.589150827	217.70.184.38	172.24.0.10	TCP	60
2036	15.589593405	217.70.184.38	172.24.0.10	TCP	60
2041	15.709576951	217.70.184.38	172.24.0.10	TCP	60
2044	15.889714479	217.70.184.38	172.24.0.10	TCP	60
2047	15.906431924	217.70.184.38	172.24.0.10	TCP	60
2050	16.009824151	217.70.184.38	172.24.0.10	TCP	60
2050	16.009824151	217.70.184.38	172.24.0.10	TCP	60

The terminal window shows the following output:

```

rg/submit/ -
Mmap done: 1 IP address (1 host up) scanned in 23.62 seconds
(kali@kali)-[~]
└─$ nmap -sT -O www.artstailor.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 20:17 EDT
Nmap scan report for www.artstailor.com (217.70.184.38)
Host is up (0.00065s latency).
rDNS record for 217.70.184.38: ns.artstailor.com
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91E=4%D=9/29%OT=21%CT=1%CU=33826%PV=N%DS=2%DC=I%G=Y%TM=6155016
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%
OS:DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=5)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.59 seconds

```

Figure 3:

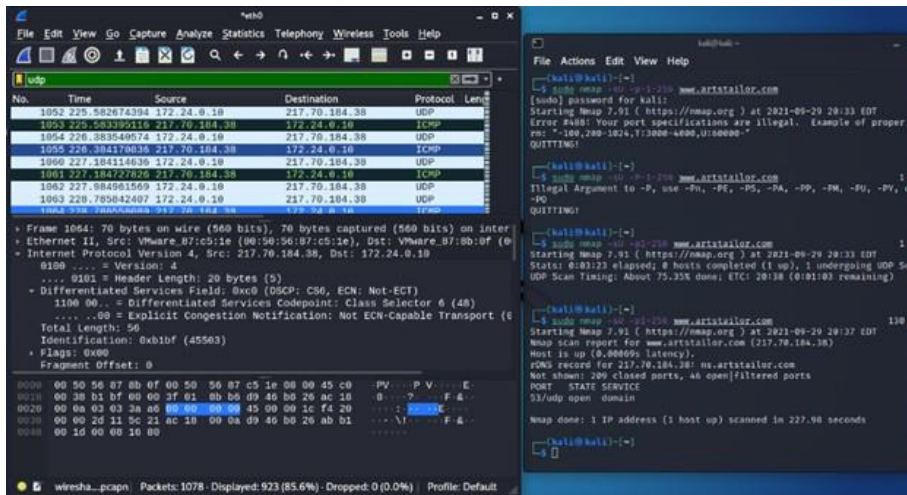


Figure 4:

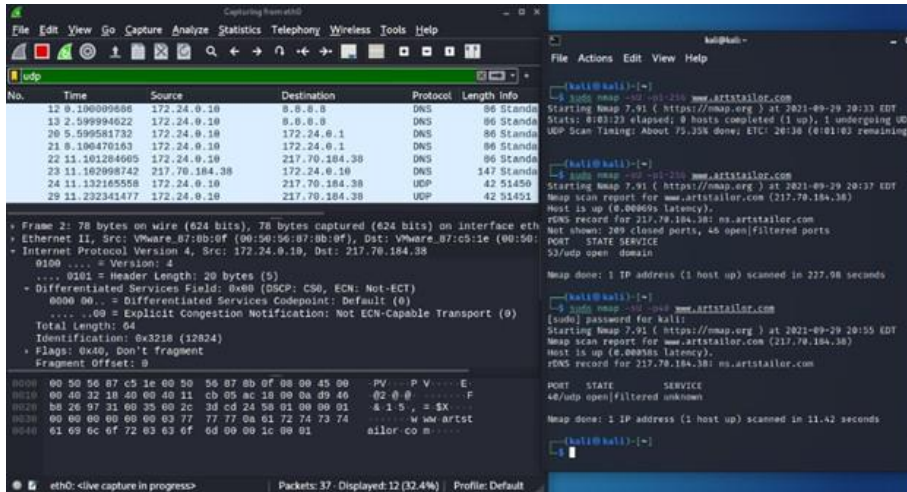


Figure 5:

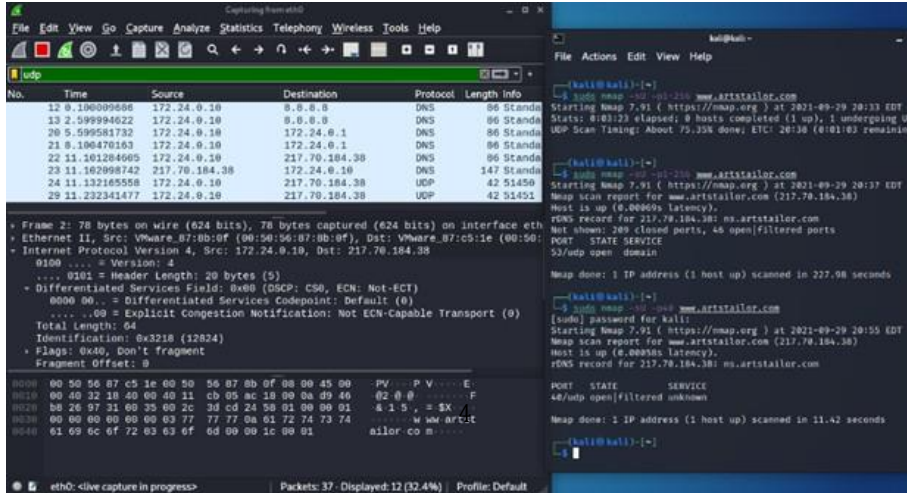


Figure 6: