

David Murillo Santiago
Professor Munoz
7 Dec 2024
IS3523

Lab 4: Attack Analysis

In this lab, I was provided with a packet capture and two copies of captured event logs and asked to identify what attacks, if any, had occurred.

I was provided a packet capture from July 8th 2017 taken between the minutes of 2:09 pm to 2:13 pm, from a Windows device. In total, 2364 packets were captured.

Time	
First packet:	2017-07-08 14:09:32
Last packet:	2017-07-08 14:13:45
Elapsed:	00:04:12
Capture	
Hardware:	Unknown
OS:	64-bit Windows 7 Service Pack 1, build 7601
Application:	Dumpcap 1.10.3 (SVN Rev 53022 from /trunk-1.10)
Interfaces	
Interface	<u>Dropped packets</u>
\Device\NPF_{AA48AEC9-CEF5-43EC-B3F1-25D52CAE7321}	Unknown
Statistics	
<u>Measurement</u>	<u>Captured</u>
Packets	2364
Time span, s	252.934
Average pps	9.3
Average packet size, B	813
Bytes	1921245
Average bytes/s	7595
Average bits/s	60 k

Total packets captured.

Of the 2364, approximately 91% of the packets originate from conversations between the devices with the IP addresses of 192.168.134.129 and 192.168.134.132. The concentration of traffic between the two local devices is unusually dense in comparison to the surrounding traffic. Therefore revealing the need for further investigation of the conversations between the .132 and .129 devices.

Ethernet - 13	IPv4 - 8	IPv6 - 4	TCP - 155	UDP - 35		
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B
192.168.134.1	192.168.134.255	7	735 bytes	5	7	735 bytes
192.168.134.1	239.255.255.250	8	2 kB	6	8	2 kB
192.168.134.2	192.168.134.132	15	2 kB	0	9	1 kB
192.168.134.129	192.168.134.132	2,158	2 MB	4	1,573	2 MB
192.168.134.158	65.55.158.118	11	1 kB	7	11	1 kB

Dense traffic between the .129 and .132 devices.

The majority of the traffic between the two devices originates from the .129 device, meaning that 192.168.132.129 was the source address for most of the traffic, initiating 66% of the packets in the packet capture. The unusually high amount of traffic generated by the .129 address is abnormal and suggests that the device may be compromised and targeting the .132 device.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	2284				0.0090	100%	6.2800	8.051
fe80::ffff:ffff:ffffe	11				0.0000	0.48%	0.0100	71.983
192.168.134.2	28				0.0001	1.23%	0.0200	7.988
192.168.134.158	66				0.0003	2.89%	0.0700	4.711
192.168.134.132	591				0.0023	25.88%	0.9000	8.051
192.168.134.129	1573				0.0062	68.87%	5.3800	8.051
192.168.134.1	15				0.0001	0.66%	0.0100	13.203
Destination IPv4 Addresses	2284				0.0090	100%	6.2800	8.051
ff02::2	11				0.0000	0.48%	0.0100	71.983
239.255.255.250	8				0.0000	0.35%	0.0100	23.850
224.0.0.252	16				0.0001	0.70%	0.0200	69.962
224.0.0.22	31				0.0001	1.36%	0.0600	4.711
192.168.134.255	7				0.0000	0.31%	0.0100	13.203
192.168.134.2	25				0.0001	1.09%	0.0200	7.985
192.168.134.158	19				0.0001	0.83%	0.0200	7.988
192.168.134.132	1582				0.0063	69.26%	5.3800	8.051
192.168.134.129	585				0.0023	25.61%	0.9000	8.051

IPv4 Statistics - Source and Destination Addresses

To better my understanding of the packet capture, I analyzed the pcap with Snort. To do so, I used the following command:

```
Snort -c C:\Users\Administrator\Desktop\Snort\etc\snort.conf -r
C:\Users\Administrator\Downloads\ExtraHop.pcap -A console >
C:\Users\Administrator\Desktop\DMSDMS
```

Snort generated 2 types of alerts: “Consecutive TCP small segments exceeding threshold” and “TCP Port Scan – Attempted Information Leak”. Breaking these alerts down, I discovered that the “TCP small segments exceeding threshold” alert is generated when Snort detects a sequence of TCP packets which surpass a predefined limit. This type of alert is associated with a tactic used by attackers involving sending a large amount of data to overwhelm a system or evade detection by breaking up malicious data into tiny pieces. Snort also revealed that the majority of the alerts were generated by the device with IP address of 192.168.132.129, targeting the device with an IP of 192.168.132.132.

```
07/08-14:09:45.771675 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.129->192.168.134.132
07/08-14:10:07.690853 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.129->192.168.134.132
07/08-14:10:20.198281 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.129->192.168.134.132
07/08-14:10:56.824496 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.129->192.168.134.132
07/08-14:13:22.663281 [**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO:255} 192.168.134.129->192.168.134.132
07/08-14:13:26.586722 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.132->192.168.134.129
07/08-14:13:26.588439 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.132->192.168.134.129
07/08-14:13:26.582824 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.132->192.168.134.129
07/08-14:13:26.530763 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.132->192.168.134.129
07/08-14:13:26.542385 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.132->192.168.134.129
07/08-14:13:26.547037 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.132->192.168.134.129
07/08-14:13:26.564846 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.134.132->192.168.134.129
```

2 Alert types Src. 129, Dest. 132.

Next, I analyzed the TCP stream between the 129 and 132 devices to understand the meaning behind the traffic between the devices. When analyzing the stream, I found further proof for the “exceeded threshold” attack. In the stream, I discovered a runtime error log detailing a heap error caused by a bug in the application.

The TCP stream log reveals an example of system overwhelming due to multiple critical errors related to memory allocation and resource initialization failures. Errors such as “unable to initialize heap” and “CRT not initialized” indicate that the system is running out of memory. These issues are symptoms of a system struggling with excessive demands.

```

-- .A.t.t.e.m.p.t. .t.o. .u.s.e. .M.S.I.L. .c.o.d.e. .f.r.o.m. .t.h.i.s. .a.s.s.e.m.b.l.y. .d.u.r.i.n.g.
.T.h.i.s. .i.n.d.i.c.a.t.e.s. .a. .b.u.g. .i.n. .y.o.u.r. .a.p.p.l.i.c.a.t.i.o.n... .I.t. .i.s. .m.o.s.t.
m. a. .n.a.t.i.v.e. .c.o.n.s.t.r.u.c.t.o.r. .o.r. .f.r.o.m. .D.l.l.M.a.i.n...
.

....R.6.0.3.2.

-- .n.o.t. .e.n.o.u.g.h. .s.p.a.c.e. .f.o.r. .l.o.c.a.l.e. .i.n.f.o.r.m.a.t.i.o.n.

....R.6.0.3.1.

-- .A.t.t.e.m.p.t. .t.o. .i.n.i.t.i.a.l.i.z.e. .t.h.e. .C.R.T. .m.o.r.e. .t.h.a.n. .o.n.c.e...
.T.h.i.s. .i.n.d.i.c.a.t.e.s. .a. .b.u.g. .i.n. .y.o.u.r. .a.p.p.l.i.c.a.t.i.o.n...
.

....R.6.0.3.0.

-- .C.R.T. .n.o.t. .i.n.i.t.i.a.l.i.z.e.d.

....R.6.0.2.8.

-- .u.n.a.b.l.e. .t.o. .i.n.i.t.i.a.l.i.z.e. .h.e.a.p.

.....R.6.0.2.7.

-- .n.o.t. .e.n.o.u.g.h. .s.p.a.c.e. .f.o.r. .l.o.w.i.o. .i.n.i.t.i.a.l.i.z.a.t.i.o.n.

.....R.6.0.2.6.

-- .n.o.t. .e.n.o.u.g.h. .s.p.a.c.e. .f.o.r. .s.t.d.i.o. .i.n.i.t.i.a.l.i.z.a.t.i.o.n.

.....R.6.0.2.5.

-- .p.u.r.e. .v.i.r.t.u.a.l. .f.u.n.c.t.i.o.n. .c.a.l.l.

.....R.6.0.2.4.

-- .n.o.t. .e.n.o.u.g.h. .s.p.a.c.e. .f.o.r. .o.n.e.x.i.t./.a.t.e.x.i.t. .t.a.b.l.e.

.....R.6.0.1.9.

-- .u.n.a.b.l.e. .t.o. .o.p.e.n. .c.o.n.s.o.l.e. .d.e.v.i.c.e.

.....R.6.0.1.8.

-- .u.n.e.x.p.e.c.t.e.d. .h.e.a.p. .e.r.r.o.r.

```

Heap error.

In the same TCP stream, I found further proof of system overwhelm through TCP limits being exceeded. Frames 642 and 644 reveal a "TCP Window Full" and "TCP ZeroWindow" warning. The 129 device is receiving a warning that the receiver's TCP window is now completely full. Additionally, the 132 device is sending a "ZeroWindow" warning to the 129 device, telling the sender to stop sending data because its buffer is completely full and cannot accept any more data. TCP ZeroWindow is a preventative measure against system overwhelm, such as that caused by buffer overflow attacks. Therefore, the immense

density of traffic from the 129 device, coupled with the Zero-Window buffer warnings, indicates an attack from the 129 device targeting the 132 device.

192.168.134.129	192.168.134.132	TCP	1514 [TCP Window Full]
192.168.134.132	192.168.134.129	TCP	60 1241 → 29922 [ACK]
192.168.134.132	192.168.134.129	TCP	60 [TCP ZeroWindow]

Window Full Packet Capture Warning.

```
▼ [TCP Analysis Flags]
  ▼ [Expert Info (Warning/Sequence): TCP window specified by the receiver is now completely full]
    [TCP window specified by the receiver is now completely full]
    [Severity level: Warning]
```

TCP window is now completely full.

The second alert generated by Snort was for a port scan. I found additional evidence of the port scan through Wireshark, where I discovered that the user conducted the scan between frames 1898 and 2211. The attacker (192.168.134.129) sent SYN packets to 291 ports ranging from port 21 to port 65535.

TCP RST Traffic Resulting From Port Scan

To skip the RST Traffic table, jump to page 13.

Packet #	Src Port	Dest. Port	Source	Destination
1898	69	53678	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1900	80	42832	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1902	49	54297	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1904	81	44382	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1906	105	43410	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1908	42	42350	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1910	25	52129	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1912	23	37992	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1914	22	48859	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1916	21	37485	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

1918	143	40977	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1920	161	50284	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1922	389	50414	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1924	407	42067	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1943	111	40743	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1945	110	47601	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1947	548	33055	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1951	623	41958	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1953	689	35074	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1955	515	43347	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1957	514	34516	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1959	513	45771	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1961	512	55428	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1966	443	33888	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1971	1000	44464	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1973	1099	41477	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1975	1000	44464	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1977	1433	43774	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

1979	921	58793	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1981	912	32959	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1983	912	32849	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1985	902	60928	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1987	783	38602	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1989	705	45548	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1991	1723	52226	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1993	1755	53556	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1995	1900	45551	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1997	2000	52405	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
1999	1720	41726	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2001	1582	49684	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2003	1581	41829	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2005	1533	48066	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2007	1521	47122	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2009	1434	40375	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2011	2947	47345	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2013	2967	50722	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

2015	3000	37683	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2017	3050	56979	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2019	2525	43556	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2021	2380	50891	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2023	2207	35976	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2025	2103	40926	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2027	2100	46673	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2029	2046	37341	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2031	4000	41733	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2033	4659	33636	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2035	4848	58980	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2037	5038	33074	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2039	3690	44254	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2041	3632	53783	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2043	3628	44751	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2045	3306	57665	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2047	3128	45169	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2049	3057	55634	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

2051	5405	57990	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2053	5432	59107	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2055	5554	42645	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2057	5555	46182	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2059	5250	36033	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2061	5168	51029	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2063	5093	45326	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2065	5061	52146	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2067	5060	44594	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2069	5051	41554	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2071	6070	52850	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2073	6080	42972	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2075	6101	60868	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2079	6050	60132	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2081	5985	48966	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2083	5900	47461	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2085	5800	40695	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2087	5631	39710	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

2089	5560	50645	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2091	7144	39440	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2093	7510	47874	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2095	7579	48136	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2097	7580	41114	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2099	6905	40500	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2101	6667	41562	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2103	6660	51607	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2105	6504	37782	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2107	6503	49148	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2109	6502	37568	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2111	8080	38117	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2113	8090	54953	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2115	8300	37442	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2117	8800	36143	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2119	8028	40247	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2121	8014	59177	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2123	8008	38663	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

2125	8000	59050	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2127	7787	45429	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2129	7777	44226	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2131	10001	47916	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2133	10050	52437	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2135	10202	47520	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2137	10203	52156	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2139	10000	51029	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2141	9999	53193	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2143	9495	59046	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2145	9090	58805	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2147	9080	40665	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2149	8812	35607	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2151	12401	49156	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2153	13500	53418	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2155	16102	39335	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2157	17185	50515	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2159	12203	40308	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

2161	12174	57284	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2163	11234	56462	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2165	11000	59257	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2167	10628	52129	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2169	10616	37771	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2171	26000	56643	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2173	30000	39403	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2175	34443	44485	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2177	38080	40729	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2179	22222	41009	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2181	20222	32837	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2183	20034	42669	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2185	20031	48670	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2187	19810	50945	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2189	18881	37100	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2191	50000	45978	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2193	50013	45607	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2195	57772	44999	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

2197	62514	41840	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2199	46823	34197	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2201	44334	38694	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2203	41524	43909	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2205	41523	49035	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2207	41025	39348	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2209	38292	57884	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31
2211	65535	42433	192.168.134.132 00:0c:29:7d:f3:78	192.168.134.129 00:0c:29:3f:20:31

The attacker conducted the port scan by sending SYN packets to a multitude of ports on the 132 device. The attacker would determine whether the port was open by analyzing the flag in the TCP response packet. If the response packet contains a SYN,ACK flag, then a connection can be established and the port is deemed open. On the other hand, If the responding packet contains a RST flag, the connection is refused and the port is deemed closed. The table above reveals 288 closed ports which returned a RST flag as a result of the port scan.

1971 230.295621	192.168.134.132	192.168.134.129	TCP	60 1000 → 44464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1972 230.295935	192.168.134.129	192.168.134.132	TCP	74 41479 → 1099 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1973 230.296021	192.168.134.132	192.168.134.129	TCP	68 1099 → 41479 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1974 230.296332	192.168.134.129	192.168.134.132	TCP	74 50795 → 1100 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1975 230.296374	192.168.134.132	192.168.134.129	TCP	60 1100 → 50795 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1976 230.296556	192.168.134.129	192.168.134.132	TCP	74 43773 → 1453 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1977 230.296694	192.168.134.132	192.168.134.129	TCP	68 1433 → 43773 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1978 230.297068	192.168.134.129	192.168.134.132	TCP	74 58793 → 321 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1979 230.297117	192.168.134.132	192.168.134.129	TCP	60 921 → 58793 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1980 230.297427	192.168.134.129	192.168.134.132	TCP	74 32859 → 912 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1981 230.297463	192.168.134.132	192.168.134.129	TCP	60 912 → 32859 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1982 230.297807	192.168.134.129	192.168.134.132	TCP	74 43857 → 918 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1983 230.297843	192.168.134.132	192.168.134.129	TCP	60 918 → 43857 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1984 230.298285	192.168.134.129	192.168.134.132	TCP	74 69028 → 982 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1985 230.298323	192.168.134.132	192.168.134.129	TCP	60 982 → 69028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1986 230.299311	192.168.134.129	192.168.134.132	TCP	74 38682 → 783 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1987 230.299349	192.168.134.132	192.168.134.129	TCP	60 783 → 38682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1988 230.299868	192.168.134.129	192.168.134.132	TCP	74 45548 → 705 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1989 230.299885	192.168.134.132	192.168.134.129	TCP	60 705 → 45548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1990 230.350032	192.168.134.129	192.168.134.132	TCP	74 52226 → 1273 [SYN] Seq=0 Win=14600 Len=0 MSS=146
1991 230.350066	192.168.134.132	192.168.134.129	TCP	60 1723 → 52226 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1992 230.350430	192.168.134.129	192.168.134.132	TCP	74 53556 → 1755 [SYN] Seq=0 Win=14600 Len=0 MSS=146

TCP RST Packets Resulting From Closed Ports.

Through my analysis of the response packets, I determined that the scan returned 3 open ports: Port 135, 139, and 445. Port 135 is used for RPC (Remote Procedure Call), which is used in Windows environments for remote client-server connections. The other two ports are SMB ports 445 and 139. SMB is used for file sharing between local network devices by enabling interprocess communication, which, in turn, allows applications and services to communicate with each other. Through SMB, core network services such as file, print, and device sharing are enabled.

```

Internet Protocol Version 4, Src: 192.168.134.132, Dst: 192.168.134.129
Transmission Control Protocol, Src Port: 445, Dst Port: 50952, Seq: 0, Ack: 1
    Source Port: 445
    Destination Port: 50952
    [Stream index: 31]
    [Stream Packet Number: 2]
    [Conversation completeness: Complete, NO_DATA (23)]
    [TCP Segment Len: 0]
    Sequence Number: 0      (relative sequence number)
    Sequence Number (raw): 144384765
    [Next Sequence Number: 1      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 3435461108
    1011 .... = Header Length: 44 bytes (11)
    Flags: 0x012 (SYN, ACK)
    Window: 64240

```

Open Port 445 as Shown by SYN, ACK Response.

Finding port 445 open is expected as in my initial overview of the pcap, I found several pockets of SMB traffic between the 129 and 132 devices. Upon further analysis of the SMB traffic, I found several references to printer traffic through artifacts such as the SPOOLS protocol, enum printer requests, and file operations such as NOT Create AndX and Write AndX commands, which indicate that the client is attempting to enumerate available printers, establish connections to the print spooler, and potentially submit or manage print jobs.

Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Information
61 7.932482	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400b, 155 bytes		
62 7.934304	192.168.134.129	192.168.134.132	DCERPC	291 Bind: call_id: 0, Fragment: Single, 12 context items: 5041009c-1		
63 7.934415	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400b, 158 bytes		
64 7.936209	192.168.134.129	192.168.134.132	SMB	129 Read Andx Request, FID: 0x400b, 349 bytes at offset 14		
65 7.936364	192.168.134.132	192.168.134.129	DCERPC	462 Bind_Ack: call_id: 0, Fragment: Single, max_xmit: 4280 max_recv:		
66 7.938570	192.168.134.129	192.168.134.132	SRVSVC	177 NetRemoteIO request:		
67 7.938955	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400b, 44 bytes		
68 7.940431	192.168.134.129	192.168.134.132	SMB	129 Read Andx Request, FID: 0x400b, 252 bytes at offset 720		
69 7.940499	192.168.134.132	192.168.134.129	SRVSVC	210 NetRemoteIO response:		
70 7.943263	192.168.134.129	192.168.134.132	SMB	162 NT Create Andx Request, FID: 0x400c, Path: \SPOOLSS		
71 7.943561	192.168.134.132	192.168.134.129	SMB	285 NT Create Andx Response, FID: 0x400c		
72 7.949252	192.168.134.129	192.168.134.132	SMB	159 Write Andx Request, FID: 0x400c, 26 bytes at offset 177		
73 7.949342	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400c, 26 bytes		
74 7.951135	192.168.134.129	192.168.134.132	DCERPC	839 Bind: call_id: 0, Fragment: Single, 16 context items: 094094f7-e		
75 7.951218	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400c, 706 bytes		
76 7.953812	192.168.134.129	192.168.134.132	SMB	129 Read Andx Request, FID: 0x400c, 667 bytes at offset 653		
77 7.953259	192.168.134.132	192.168.134.129	DCERPC	558 Bind_Ack: call_id: 0, Fragment: Single, max_xmit: 4280 max_recv:		
78 7.958282	192.168.134.158	192.168.134.2	DNS	76 Standard query 0xe4f4 A dns.msftncsi.com		
79 7.988361	192.168.134.2	192.168.134.158	DNS	92 Standard query response 0xe4f4 A dns.msftncsi.com A 131.107.255.		
80 7.988618	192.168.134.158	192.168.134.2	DNS	76 Standard query 0x9207 AAAA dns.msftncsi.com		
81 7.989342	192.168.134.2	192.168.134.158	DNS	104 Standard query response 0x9287 AAAA dns.msftncsi.com AAAA fd3e:4		
82 7.993462	192.168.134.129	192.168.134.132	TCP	66 41254 -> 445 [ACK] Seq=42483 Ack=3085 WIn=23296 Len=0 TSval=11434		
83 8.058927	192.168.134.129	192.168.134.132	SPOOLSS	181 EnumPrinters request, level 1		
84 8.051844	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400c, 48 bytes		
85 8.051370	192.168.134.129	192.168.134.132	TCP	66 41254 -> 445 [ACK] Seq=4363 Ack=3136 WIn=23296 Len=0 TSval=11434		
86 8.053268	192.168.134.129	192.168.134.132	SMB	129 Read Andx Request, FID: 0x400c, 214 bytes at offset 226		
87 8.053366	192.168.134.132	192.168.134.129	SPOOLSS	174 EnumPrinters response, level 1\Uninformated packet		
88 8.056588	192.168.134.129	192.168.134.132	SMB	162 NT Create Andx Request, FID: 0x400d, Path: \SPOOLSS		
89 8.056944	192.168.134.132	192.168.134.129	SMB	285 NT Create Andx Response, FID: 0x400d		
90 8.062743	192.168.134.129	192.168.134.132	SMB	593 Write Andx Request, FID: 0x400d, 480 bytes at offset 502		
91 8.062835	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400d, 460 bytes		
92 8.064761	192.168.134.129	192.168.134.132	DCERPC	361 Bind: call_id: 0, Fragment: Single, 15 context items: ace49308-e		
93 8.064843	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400d, 228 bytes		
94 8.066641	192.168.134.129	192.168.134.132	SMB	129 Read Andx Request, FID: 0x400d, 468 bytes at offset 88		
95 8.066693	192.168.134.132	192.168.134.129	DCERPC	534 Bind_Ack: call_id: 0, Fragment: Single, max_xmit: 4280 max_recv:		
96 8.069848	192.168.134.129	192.168.134.132	SPOOLSS	697 EnumPrinters request, level 1		
97 8.069131	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400d, 564 bytes		
98 8.071161	192.168.134.129	192.168.134.132	SMB	129 Read Andx Request, FID: 0x400d, 193 bytes at offset 784		
99 8.071249	192.168.134.132	192.168.134.129	SMB	323 Read Andx Response, FID: 0x400d, 193 bytes		
100 8.073188	192.168.134.129	192.168.134.132	SMB	129 Read Andx Request, FID: 0x400d, 65169 bytes at offset 612		
101 8.073392	192.168.134.132	192.168.134.129	SPOOLSS	497 EnumPrinters response, level 1		
102 8.077888	192.168.134.129	192.168.134.132	SMB	162 NT Create Andx Request, FID: 0x400e, Path: \BROWSER		
103 8.077458	192.168.134.132	192.168.134.129	SMB	285 NT Create Andx Response, FID: 0x400e		
104 8.083256	192.168.134.129	192.168.134.132	SMB	558 Write Andx Request, FID: 0x400e, 417 bytes at offset 197		
105 8.083395	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400e, 417 bytes		
106 8.085188	192.168.134.129	192.168.134.132	DCERPC	448 Bind: call_id: 0, Fragment: Single, 16 context items: 40f190fd-e		
107 8.085289	192.168.134.132	192.168.134.129	SMB	117 Write Andx Response, FID: 0x400e, 315 bytes		

SMB Spools Traffic.

I then checked the event logs for printer logs or warnings. In analyzing the event logs, I found several alarming entries that point to issues with a printer system and its interaction with SMB traffic. Event ID

20 indicates a problem with the printer driver, particularly related to the TP Output Gateway system, which involves various dynamic link libraries (DLLs) and configuration files. The logs reference multiple versions of files such as PSCRIPT5.DLL, PS5UI.DLL, TPPS.PPD, etc., which reveal that different components of the printing system may be misconfigured and acting abnormally. Additionally, entries related to TPPRN.DLL, TPPrnUI.DLL, and several localized versions of TPPrnUI files point to potential issues with the printer interface and user interface components. Because the SMB traffic is originating from the attacker, the security event logs show abnormal behavior in the printer libraries, and there are signs of malformed packets, it is necessary to analyze the libraries to ensure their legitimacy and confirm that the attacker isn't using malicious files as a backdoor to gain access to the device.

The screenshot shows the Windows Event Viewer interface. At the top, there is a table of events with columns for Level, Date, Source, Task Category, and Event ID. Below this is a detailed view for Event ID 20, titled "Event 20, Print". The "General" tab is selected, displaying the following information:

- Description:** The description for Event ID 20 from source Print cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.
- Display Information:** If the event originated on another computer, the display information had to be saved with the event.
- Event Data:** The following information was included with the event:
 - TP Output Gateway
 - Windows NT x86
 - Version-3
 - TPPRN.DLL, TPPrnUI.DLL, TPOG.bin, TPOG.chm, TPPrnUlchs.dll, TPPrnUlcht.dll, TPPrnUlcsy.dll, TPPrnUldeu.dll, TPPrnUldeu.dll, TPPrnUlesn.dll, TPPrnUlfra.dll, TPPrnUlhusn.dll, TPPrnUljpnn.dll, TPPrnUlkor.dll, TPPrnUlplk.dll, TPPrnUlptb.dll, TPPrnUlrus.dll, TPPrnUltha.dll, TPPrnUlita.dll, TPPrnUlsve.dll
- Message Resource:** The message resource is present but the message was not found in the message table.

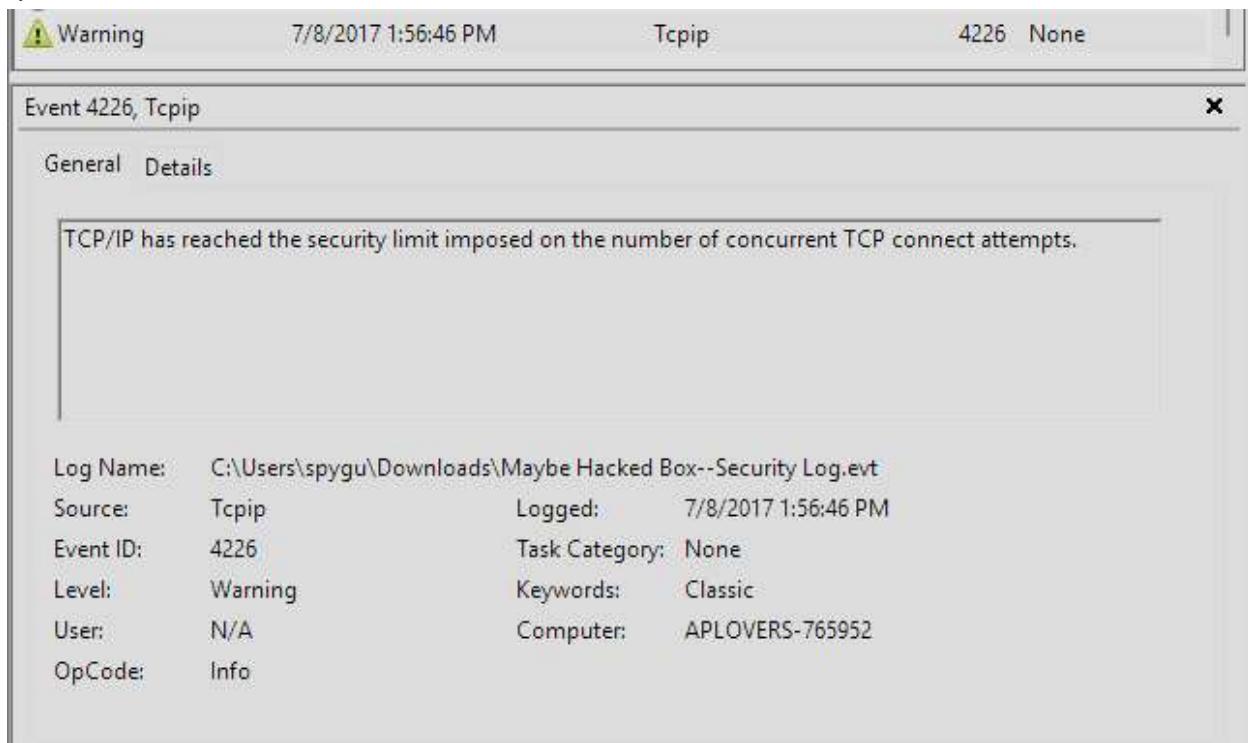
At the bottom of the event details pane, there is a table of log properties:

Log Name:	C:\Users\spygu\Downloads\Maybe Hacked Box--Security Log.evt		
Source:	Print	Logged:	8/6/2016 3:13:13 PM
Event ID:	20	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	SYSTEM	Computer:	APLOVERS-765952
OpCode:	Info		

Event ID 20: Printer DLL Warnings.

Event ID 4226 indicates a TCP/IP warning triggered when the system reaches the security limit for concurrent connection attempts. The log reads, “TCP/IP has reached the security limit imposed on the number of concurrent TCP connect attempts”. This warning is generated when a system makes too many concurrent outgoing TCP connection attempts in a short period. Windows imposes a limit on these attempts to protect against port scanning or worm propagation. As previously mentioned, the 129 device

did conduct a port scan on the 132 device. Therefore, this warning shows further proof of port scanning by the 129 device.



Event ID 4226: TCP Security Limit.

Other notable artifacts I found in my investigation include IPC\$ and DCERPC. In the SMB traffic, the user was attempting to connect to an IPC\$ share, which allows anonymous users to perform activities like enumerating domain accounts and network shares. This can be a common target for attackers seeking information about network resources. Additionally, DCERPC (Distributed Computing Environment Remote Procedure Call) was observed, which enables distributed software to operate as if it were running on the same system.

Therefore, the SMB traffic reflects an attempt to exploit or gather information about network shares and printer services, which ties into the previously mentioned reconnaissance conducted via a port scan of the ports on the 132 device.

```

SMB    143 Tree Connect AndX Request, Path: \\192.168.134.132\IPC$ 
SMB    116 Tree Connect AndX Response
SMB    161 NT Create AndX Request, Path: \SRVSVC
SMB    105 NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
SMB    162 NT Create AndX Request, FID: 0x400a, Path: \BROWSER
SMB    205 NT Create AndX Response, FID: 0x400a
DCERPC 733 Bind: call id: 0, Fragment: Single, 13 context items: 0e042bc0-cab3-517d-523f-7cbe
  
```

IPC\$ Share and DCERPC.

Analyzing the application logs, I found multiple warnings (Event ID 63) related to Windows Management Instrumentation (WMI) providers being registered to use the LocalSystem account, which has elevated privileges. Specifically, the provider HiPerfCooker_v1 and CmdTriggerConsumer were registered in the Root\WMI and Root\cimv2 namespaces, respectively. This is concerning because improper impersonation of user requests by these privileged providers can lead to security violations and potential exploitation.

Attackers could abuse these providers to execute commands or scripts with system-level privileges, which is a common technique for maintaining persistence or performing privilege escalation on a compromised system.

The screenshot shows the Windows Event Viewer interface. At the top, there is a table with three rows of event logs. Each row contains a yellow warning icon, the text "Warning", the date and time "8/6/2016 3:07:09 PM", the source "WinMgmt", the event ID "63", and the category "None". Below this table is a window titled "Event 63, WinMgmt". Inside this window, there are two tabs: "General" and "Details". The "General" tab displays a message: "A provider, HiPerfCooker_v1, has been registered in the Windows Management Instrumentation namespace Root\WMI to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests." The "Details" tab lists event properties:

Log Name:	C:\Users\spygu\Downloads\Maybe Hacked Box--Application Log.evt		
Source:	WinMgmt	Logged:	8/6/2016 3:07:09 PM
Event ID:	63	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	SYSTEM	Computer:	APLOVERS-765952
OpCode:	Info		

Event ID 63: Root\WMI.

Finally, through an NBNS refresh request, I pieced together the final parts of the investigation. Since all of the DNS queries in the packet capture were being sent to 192.168.134.2, I determined that the .2 device was the DNS server.

Therefore, I concluded that on frame 2217, the 132 device requested an NBNS refresh from the DNS server for the APLOVERS machine to check if the system is still registered and available on the network. As a result, the 132 device is not APLOVERS and is not the owner of the event logs. Instead, the 129 device is APLOVERS, as the event logs (Event ID 4226) show signs of port scanning, which was found to have been initiated by the 129 device in both Snort and Wireshark.

2217	231.999348	192.168.134.132	192.168.134.2	NBNS	110 Refresh NB APLOVERS-765952<20>
------	------------	-----------------	---------------	------	------------------------------------

NBNS Refresh.

Summary of What Happened:

I was provided with a packet capture from July 8th, 2017, recorded between 2:09 PM and 2:13 PM, capturing 2364 packets from a Windows device. The majority of the traffic—about 91%—was concentrated between the devices with IP addresses 192.168.134.129 and 192.168.134.132. This unusually dense communication warranted further investigation.

Upon analysis, it became clear that the 129 device generated most of the traffic, initiating 66% of the packets. Using Snort to analyze the pcap, I found two types of alerts: “Consecutive TCP small segments exceeding threshold” and “TCP Port Scan – Attempted Information Leak”. These alerts suggested that the 129 device was sending a high volume of small TCP packets to overwhelm the 132 device and performing a port scan to gather information. The exceeded threshold alert is consistent with system overwhelm tactics where excessive traffic can cause memory and buffer issues.

Further examination of the TCP stream between the 129 and 132 devices revealed runtime errors and heap errors in the logs. These errors, such as “unable to initialize heap” and “CRT not initialized”, indicate that the 132 device was overwhelmed by the traffic. Additionally, I observed “TCP Window Full” and “TCP ZeroWindow” warnings, showing that the 132 device’s buffer was full and could no longer accept data. This evidence confirms that the 129 device was actively overwhelming the 132 device through TCP traffic.

A detailed examination of the SMB traffic revealed further malicious activity. The 129 device was attempting to interact with printer services on the 132 device, as shown by SPOOLS protocol references, enum printer requests, and SMB commands like “NT Create AndX” and “Write AndX”. These interactions suggest an attempt to enumerate printers, submit print jobs, or exploit vulnerabilities in the print service.

In the event logs, I found Event ID 20 indicating issues with the TP Output Gateway system and its associated DLLs (e.g., PSCRIPT5.DLL, TPPRN.DLL, TPPrnUI.DLL). These DLL warnings, coupled with the SMB traffic anomalies, suggest that the attacker may have been exploiting the printer system to gain access or persistence.

Additionally, Event ID 4226 warned of the system reaching its limit for concurrent TCP connection attempts, further confirming the port scanning activity initiated by the 129 device. This scan targeted 291 ports on the 132 device, with 3 ports found open: 135 (RPC), 139 (SMB over NetBIOS), and 445 (SMB over TCP).

In the application logs, Event ID 63 showed that WMI providers were registered with the LocalSystem account, a privileged context. This indicates potential abuse of WMI for persistence or privilege escalation by the attacker.

Finally, an NBNS Refresh request from the 132 device to the DNS server (192.168.134.2) confirmed that 192.168.134.132 was not the APLOVERS machine. Instead, the 129 device is APLOVERS, as it was responsible for the port scan and generated the concurrent TCP connection warning.

Conclusion: The 129 device (APLOVERS) initiated an attack on the 132 device involving port scanning, TCP flood attacks, and attempts to exploit SMB and printer services. This attack led to system resource exhaustion and potentially compromised the target's print services and WMI infrastructure.

Next Steps:

Due to abnormal findings in the packet capture and event logs, the APLOVERS-765952 (192.168.134.129) system appears to be compromised and is attempting lateral movement through reconnaissance (port scans) and malformed SMB packets, which it is sending to the 132 system. The APLOVERS logs reveal suspicious dynamic libraries (Event ID 20), possible privilege escalation (Event ID 63), and port scanning (Event ID 4226). Further signs of compromise include alerts generated by Snort (TCP Port Scan), confirming that APLOVERS is conducting a port scan on the 132 system. Snort also detected full TCP buffers caused by the 129 system (TCP small segments exceeding threshold), visible in Wireshark frames 254, 272, 642, 644, 1318, 1352, 1398, and 1399.

As a result, the APLOVERS system should be scanned for malicious files and rootkits, especially within the printer dynamic link libraries, and reimaged to remove any malicious content. Additionally, the 132 system (192.168.132.132) should be reimaged as well, as APLOVERS exchanged several packets with it, including malformed SMB packets (frame 2310) and SPOOLS/printer traffic. The 132 system was also the victim of port scanning by APLOVERS, which discovered open ports 135, 139, and 445. This led to the exploitation of port 445 for SMB traffic. The attacker exchanged several packets between itself and the open ports on the victim, so the 132 system should also be scanned for malicious files and reimaged if any malicious content is found.

Citations

"Inter-Process Communication and Share Null Session." Microsoft Learn,
<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/inter-process-communication-share-null-session>.

"NetBIOS/NBNS." Wireshark Wiki, <https://wiki.wireshark.org/NetBIOS/NBNS>.

"Remote Procedure Call." Wikipedia, https://en.wikipedia.org/wiki/Remote_procedure_call.

"Remote Procedure Call (RPC)." IBM Documentation,
<https://www.ibm.com/docs/en/aix/7.3?topic=concepts-remote-procedure-call>.

"DCE/RPC." Wireshark Wiki, <https://wiki.wireshark.org/DCE/RPC>.

"DCE/RPC." Wikipedia, <https://en.wikipedia.org/wiki/DCE/RPC>.

"Server Message Block." Wikipedia, https://en.wikipedia.org/wiki/Server_Message_Block.

"Server Message Block Protocol." TechTarget,
<https://www.techtarget.com/searchnetworking/definition/Server-Message-Block-Protocol>.

"Microsoft SMB Protocol Authentication." Microsoft Learn,
<https://learn.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-authentication>.