



# Certified SOC Analyst Writeups

Type	Writeup
Reviewed	<input checked="" type="checkbox"/>

## CVE Number

Introduction to Cybersecurity » CVE Number ✓

Category:	General Information	Level:	basic	Points:	25
-----------	---------------------	--------	-------	---------	----

Description

What is the CVE ID that is related to EternalBlue  
Flag Format: XXX-XXXX-XXXX

Answer

Write your answer here.

Google search of "EternalBlue" reveals EternalBlue is a Microsoft exploit which was used by the NSA in intelligence gathering operations. The exploit, officially named MS17-010 by Microsoft — gave the US National Security Agency (NSA) backend access to devices running Windows operating systems like Windows XP and Windows 7.

Article from which info is found [https://nordvpn.com/blog/what-is-eternalblue/#:~:text=What is EternalBlue%3F,Windows XP and Windows 7.](https://nordvpn.com/blog/what-is-eternalblue/#:~:text=What%20is%20EternalBlue%3F,Windows%20XP%20and%20Windows%207.)

Wikipedia has the CVE number <https://en.wikipedia.org/wiki/EternalBlue>

Also a simple google search of "CVE number of EternalBlue" → **CVE-2017-0144**

## Smart Role

## Introduction to SOC » Smart Role

Category: General Information

Level: basic

Points: 25

### Description

skills of collecting information out of cyberspace that has been previously analysed and shared between organisations about different attack scenarios and vectors. What is the role name of the above definition

### Answer

Write your answer here.

flag{threat intelligence}

# Backdoor

## Introduction to Network Security » Backdoor

Category: Digital Forensics

Level: medium

Points: 100

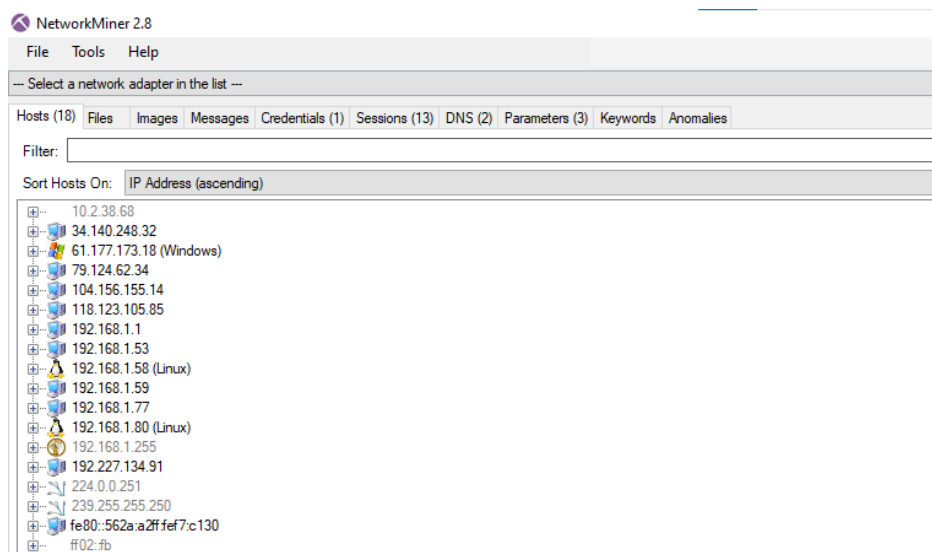
### Description

Our server compromised due to known vulnerability introduced from many years, Kindly check and identify this flow

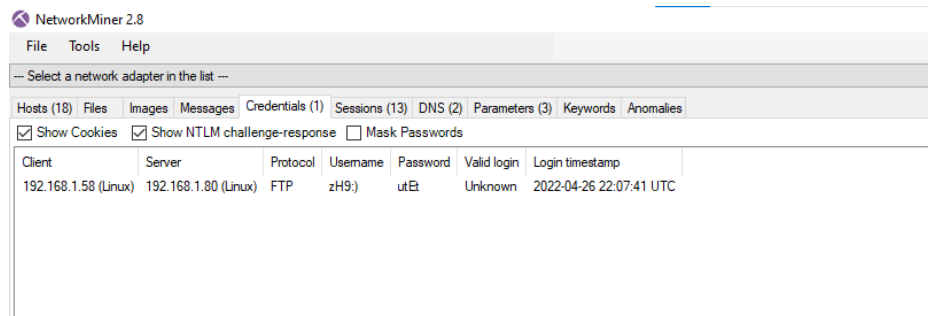
X: Attack source → EX. "Internal/External"  
Y: The Source IP → x.x.x.x  
Z: CVE Num of the attack → xxx  
W: Destination Mac Address  
Flag format: flag{X:Y:Z:w}  
Link: https://to-be-uploaded

Link: <https://hubchallenges.s3.eu-west-1.amazonaws.com/foren/backdoor.pcap>

Open pcap file in NetworkMiner to look for any abnormal behavior on the hosts.



From the screenshot above, there are seems to be login credentials sent which indicates potential login compromise.



The record shows the vulnerability is from an FTP protocol, and we have the source IP address; 192.168.1.58

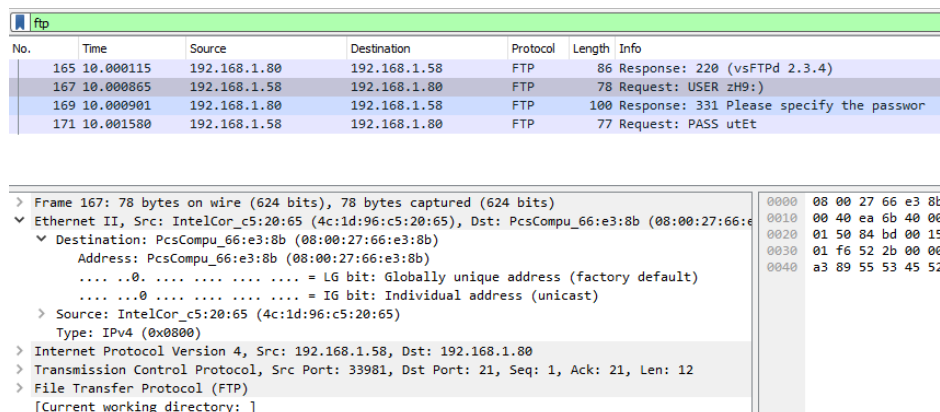
Also the attack is internal because it is within the same subnet mask as the sever IP address

The next step is to figure out what the cve of the vulnerability is. A google search "*ftp backdoor vulnerability cve*" show the vulnerability is CVE-2011-2523: vsftpd 2.3.4

Link below provides information on the vulnerability;

<https://subscription.packtpub.com/book/security/9781786463166/1/ch01lv1sec18/vulnerability-analysis-of-vsftpd-2-3-4-backdoor#:~:text=The concept of the attack,port 6200 of the system.>

The last requirement is to find the mac address of the destination server, for that, wireshark can be used, opening the pcap file and filtering packets the FTP shows the destination mac address 08:00:27:66:e3:8b



flag{Internal:192.168.1.58:CVE-2011-2523:08:00:27:66:e3:8b}

# Creepy DNS

## Network Security Tools » Creepy DNS

Category: Network Security Level: easy Points: 50

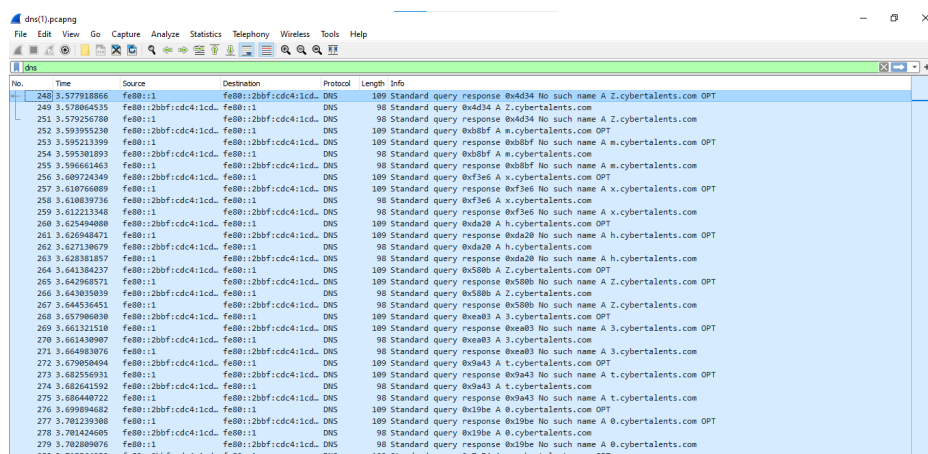
### Description

Our NMS detect a suspected traffic, your task is to investigate the captured traffic and find the anomaly reason

Link: <https://hubchallenges.s3.eu-west-1.amazonaws.com/foren/dns.pcapng>

Open the file in Wireshark

Filter the packets to only DNS and a stream of queries with different domain names is seen



No.	Time	Source	Destination	Protocol	Length	Info
248	3.577918866	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0x4d34 No such name A Z.cybertalents.com OPT
249	3.578064535	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0x4d34 A Z.cybertalents.com
251	3.579256780	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0x4d34 No such name A Z.cybertalents.com
252	3.593955230	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0xb8bf A m.cybertalents.com OPT
253	3.595213399	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0xb8bf No such name A m.cybertalents.com OPT
254	3.595381893	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0xb8bf A m.cybertalents.com
255	3.596661463	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0xb8bf No such name A m.cybertalents.com
256	3.609724349	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0xf36e A x.cybertalents.com OPT
257	3.610766809	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0xf36e No such name A x.cybertalents.com OPT
258	3.610839736	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0xf36e A x.cybertalents.com
259	3.612213348	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0xf36e No such name A x.cybertalents.com
260	3.625494808	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0xda28 A h.cybertalents.com OPT
261	3.626048471	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0xda28 No such name A h.cybertalents.com OPT
262	3.627138679	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0xda28 A h.cybertalents.com
263	3.628381857	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0xda28 No such name A h.cybertalents.com
264	3.641304237	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0x580b A Z.cybertalents.com OPT
265	3.642968571	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0x580b No such name A Z.cybertalents.com OPT
266	3.643835839	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0x580b A Z.cybertalents.com
267	3.644536451	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0x580b No such name A Z.cybertalents.com
268	3.657906838	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0xea03 A 3.cybertalents.com OPT
269	3.661321510	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0xea03 No such name A 3.cybertalents.com OPT
270	3.661430907	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0xea03 A 3.cybertalents.com
271	3.664983076	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0xea03 No such name A 3.cybertalents.com
272	3.679094044	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0x9a43 A t.cybertalents.com OPT
273	3.682556931	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0x9a43 No such name A t.cybertalents.com OPT
274	3.682641592	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0x9a43 A t.cybertalents.com
275	3.690480722	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0x9a43 No such name A t.cybertalents.com
276	3.690984682	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0x19be A 0.cybertalents.com OPT
277	3.701239308	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	109	Standard query response 0x19be No such name A 0.cybertalents.com OPT
278	3.701424605	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	98	Standard query 0x19be A 0.cybertalents.com
279	3.702093976	fe80::1	fe80::2b0f:cdc4:1cd...	DNS	98	Standard query response 0x19be No such name A 0.cybertalents.com
280	3.715564950	fe80::2b0f:cdc4:1cd...	fe80::1	DNS	109	Standard query 0x7e54 A r.cybertalents.com OPT

Looking at only the top level domains eg Z.cybertalents.com, m.cybertalents.com, a string of characters is found;

ZmxhZ3t0c2hBcmthSXNfQXdlczBtZV9OZXh3MHJraW5nX3RvMGx9

This is a base64 encoded string so decoding it from the internet

<https://www.base64decode.org/> give the flag;

flag{tshArk\_Is\_Awes0me\_Netw0rking\_to0!}

# FourOFour

Splunk » FourOFour 

Category: Web Security

Level: easy

Points: 50

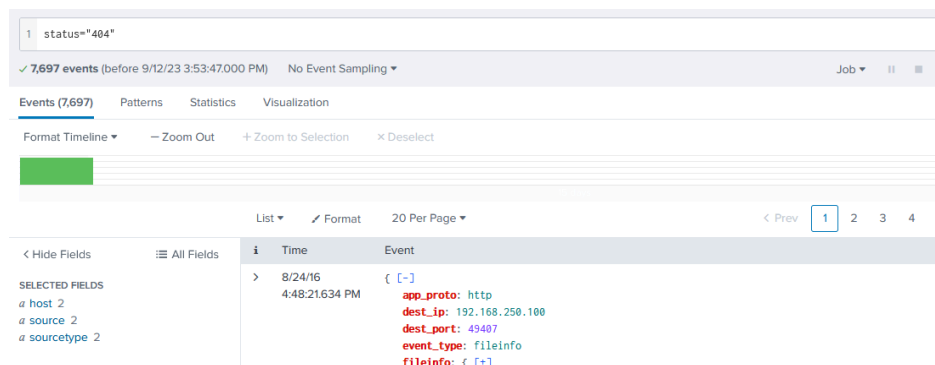
## Description

Challenge IP: 54.153.83.214

[Close Challenge](#)

Massive web bruteforce attack observed on our IIS server. Your lead has informed you to initiate some investigation to identify the following :  
X: The highest number of non-existent URLs request sent by the attacker → Number  
Y: The Source IP → x.x.x.x  
Z: The attacker source country → xxx  
Flag format: flag{X:Y:Z}

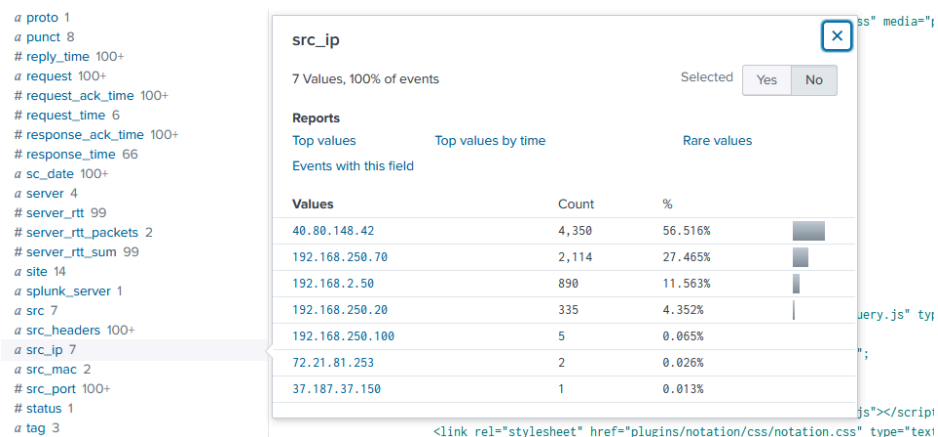
First thing is to search for content not found http code since the attacker tried to find non-existent URLs



The screenshot shows a Splunk search interface with the query `status="404"`. It displays 7,697 events. The event list shows a search result for `8/24/16 4:48:21.634 PM` with the following details:

- `app_proto: http`
- `dest_ip: 192.168.250.100`
- `dest_port: 49407`
- `event_type: fileinfo`
- `fileinfo: { [-]`

On the Fields side (left side) clicking on the `src_ip` field shows 40.80.148.42



The screenshot shows the Splunk Fields sidebar on the left with the `src_ip` field selected. On the right, a report for `src_ip` is displayed, showing 7 values, 100% of events. The report includes a table of top values by time:

Values	Count	%
40.80.148.42	4,350	56.516%
192.168.250.70	2,114	27.465%
192.168.2.50	890	11.563%
192.168.250.20	335	4.352%
192.168.250.100	5	0.065%
72.21.81.253	2	0.026%
37.187.37.150	1	0.013%



status="404" src\_ip="40.80.148.42" server="Microsoft-IIS/8.5"

content encoding: gzip

http.url

>100 Values, 68.611% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values	Count	%
/joomla/index.php	246	4.658%
/	214	4.052%
/login	22	0.416%
//index.php/api/xmlrpc	18	0.341%
//xmlrpc.php	18	0.341%
/login?redirects=10	18	0.341%
//xmlrpc	16	0.303%
//soap.php	15	0.284%
//soapserver/	15	0.284%
//xmlrpc-server.php	15	0.284%

## 55H Access

Splunk » 55H Access ✓

Category: Digital Forensics

Level: easy

Points: 50

Description

Challenge IP: 54.193.180.167

Close Challenge

We observed a huge traffic towards our SSH Server

X: How many source IPs attempting to connect → Number

Y: The Source IP with the most connections → x.x.x.x

Z: The Source IP with the most connections country → xxxxxxxx

W: The Firewall action taken from the security control → xxxxxxxx

Flag format: flag{X:Y:Z:W}

**Note:** our company uses Fortinet FortiGate firewall.

Search for events using the SSH server

**New Search** Save As ▾

1 service=ssh

✓ 151 events (before 9/12/23 3:18:10.000 PM) No Event Sampling ▾ Job ▾ || ↶ ↷

Events (151) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ ✓ Format 20 Per Page ▾ < Prev 1 2 3 4

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

i	Time	Event
>	8/24/16 6:22:43.000 PM	Aug 24 12:22:43 192.168.250.1 date=2016-08-24 time=12:22:43 devname=gotham-fortigate devid=FGT6801 ype=traffic subtype=forward level=notice vd=root srcip=202.170.88.40 srcport=35252 srcintf="wan1" 2 dstintf="wan1" sessionid=4236707 proto=6 action=deny policyid=0 dstcountry="United States" sro op service="SSH" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=30 cracti host = 192.168.250.1   source = udp:514   sourcetype = fgt_traffic

Results show 19 source IPs with 91.224.160.108 having the highest number of events

# session\_id 100+  
# sessionid 100+  
a splunk\_server 1  
a src 19  
a src\_interface 1  
a src\_ip 19  
# src\_port 73  
# src\_translated\_port 73  
a srccountry 10  
a srcintf 1  
a srcip 19  
# srcport 73  
a subtype 1  
a tag 2  
a tag:eventtype 2  
a time 40  
# timeendpos 1  
# timestartpos 1  
a trandisp 1  
a transport 1  
a type 1  
a user 1  
a vd 1  
a vendor 1  
a vendor\_action 1

+ Extract New Fields

i	Time	Event
	6:15:32.000 PM	ype=traffic subtype=forward level=notice vd=root srcip=201.16.1 22 dstintf="wan1" sessionid=4235385 proto=6 action=deny policyi

**srcip**

19 Values, 100% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
91.224.160.108	42	27.814%
91.224.160.131	21	13.907%
192.254.66.174	14	9.272%
42.115.168.134	13	8.609%
103.207.36.248	9	5.96%
195.154.43.165	7	4.636%
208.67.1.118	7	4.636%
218.87.109.253	7	4.636%
42.118.221.168	7	4.636%
64.137.214.131	7	4.636%

host = 192.168.250.1 | source = udp:514 | sourcetype = fgt\_traffic

The next thing to look for is the country from which this IP address comes from. This can be done by modifying the search query as shown below

1 service=ssh srcip="91.224.160.108"

✓ 42 events (before 9/12/23 3:23:06.000 PM) No Event Sampling ▾ Job ▾ || ↶ ↷ Smart Mode ▾

Events (42) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 day per column

List ▾ ✓ Format 20 Per Page ▾ < Prev 1 2 3 Next >

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

i	Time	Event
>	8/24/16 5:30:53.000 PM	Aug 24 11:38:53 192.168.250.1 date=2016-08-24 time=11:38:53 devname=gotham-fortigate devid=FGT6804614044725 logid=0000000013 t ype=traffic subtype=forward level=notice vd=root srcip=91.224.160.108 srcport=55749 srcintf="wan1" dstip=71.39.18.127 dstport= 22 dstintf="wan1" sessionid=4238397 proto=6 action=deny policyid=0 dstcountry="United States" srccountry="Netherlands" trandis p=noop service="SSH" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=30 craction=131072 crlevel=high host = 192.168.250.1   source = udp:514   sourcetype = fgt_traffic

From the event details the source country is Netherlands



A hint that the firewall is fortigate means the query can now be modified like this

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `1 service=ssh srcip="91.224.160.108" sourcetype=fgt_traffic action`. Below the search bar, it indicates **42 events** (before 9/12/23 3:32:52.000 PM) with **No Event Sampling**. The interface has tabs for **Events (42)**, **Patterns**, **Statistics**, and **Visualization**. Below these tabs are controls for **Format Timeline**, **Zoom Out**, **Zoom to Selection**, and **Deselect**. On the left, there are sections for **SELECTED FIELDS** (host 1, source 1, sourcetype 1) and **INTERESTING FIELDS** (action 1, app 1, agent 1). A modal window titled **action** is open, showing **1 Value, 100% of events**. It has a **Selected** dropdown set to **Yes**. Under the **Reports** section, there are links for **Top values**, **Top values by time**, and **Rare values**. A table titled **Values** shows the following data:

Values	Count	%
blocked	42	100%

And the action the firewall took is Block

So the flag is FLAG{19:91.224.160.108:netherlands:blocked}

This flag did not work, the IP geolocation seemed to be the problem so to check the origin country of this link <https://ipgeolocation.io/> can be used

The screenshot shows the IP geolocation results for the IP address 91.224.160.108. The input field at the top contains "91.224.160.108". The results are displayed in a JSON-like format:

```
"ip": "91.224.160.108",
"country_name": "Finland",
"state_prov": "South Finland",
"city": "Kerava",
"latitude": "60.40348",
"longitude": "25.13935",
"time_zone": "Europe/Helsinki",
"isp": "Aleksi Ursin trading as Nocode",
"currency": "Euro",
"country_flag": "🇫🇮"
```

This shows the origin of the IP is Finland instead of Netherlands. Now the flag is FLAG{19:91.224.160.108:finland:blocked}

# USB Case

## SIEM Use Cases » USB Case ✓

Category: Digital Forensics

Level: easy

Points: 50

### Description

Challenge IP: 54.176.25.74

Close Challenge

Your Team Lead ask you to develop splunk use case for detecting USB plugged on any device in your environment he sh  
ared with you also this link [https://lantern.splunk.com/Security/Use\\_Cases](https://lantern.splunk.com/Security/Use_Cases)  
Develop the use case and answer the below questions based on botsv1 dataset  
X: Date and time when the USB plugged on device (YYYY-MM-DD:HH:MM:SS)  
Y: The Machine name  
Z: Name of the USB device  
Flag format: flag{X:Y:Z:A}

Using the link provided and filtering the results with "usb" the following results appear

usb

Searching in All results

About 33 results

#### Removable devices connected to a machine

[https://lantern.splunk.com/Splunk\\_Platform/UC/Security/Incident\\_Management/Investigating\\_a\\_ransomware\\_attack/Removable\\_devices\\_connected\\_to\\_a\\_machine](https://lantern.splunk.com/Splunk_Platform/UC/Security/Incident_Management/Investigating_a_ransomware_attack/Removable_devices_connected_to_a_machine)

You need to identify removable devices that were connected to computer or other network device.

#### File added to the system through external media

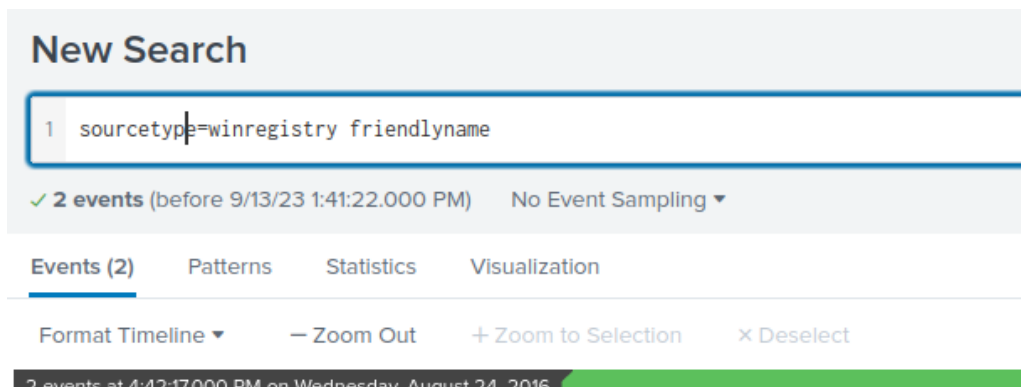
[https://lantern.splunk.com/Splunk\\_Platform/UC/Security/Incident\\_Management/Investigating\\_a\\_ransomware\\_attack/File\\_added\\_to\\_the\\_system\\_through\\_external\\_media](https://lantern.splunk.com/Splunk_Platform/UC/Security/Incident_Management/Investigating_a_ransomware_attack/File_added_to_the_system_through_external_media)

You need to identify files that were downloaded from removable media, such as a USB stick.

From the instruction "Removable devices connected to a machine", the following search query is made

```
sourcetype=winregistry friendlyname
```

Search for a registry entry value specific to USB devices. If friendlyname doesn't yield results, try other entries, as described in [Microsoft documentation](#).



Based on the events /results the machine name as well as date and time are available

i	Time	Event
>	8/24/16	08/24/2016 10:42:17.287
	4:42:17.000 PM	... 2 lines omitted ... process_image="c:\Windows\System32\svchost.exe" registry_type="SetValue" key_path="HKLM\system\controlset001\enum\wpdusenumroot\umb\2837c186b80&storage#volume#??_usbstor#disk&ven_generic&prod_flash_d1sk&rev_8.07#7d961196&0#friendlyname" data_type="REG_SZ" Show all 8 lines host = we8105desk : source = WinRegistry : sourcetype = WinRegistry

The value in the "registry\_value\_data" field is the name of the USB device

```
# process_id 2
a process_image 2
a punct 2
a registry_key_name 2
a registry_path 2
a registry_type 1
a registry_value_data 1
a registry_value_name 1
a registry_value_type 1
a splunk_server 1
a src 1
a status 1
a tag 5
```

**registry\_value\_data**

1 Value, 100% of events

Selected

**Reports**

Top values      Top values by time      Rare values

Events with this field

Values	Count	%
MIRANDA_PRI	2	100%

After you have identified the device, you might want to look at the host or src\_ip fields in the search result to identify the machine the device was plugged into. You might also want to identify any files that were downloaded from the removable device.

FLAG{2016-08-24:10:42:17:we8105desk:MIRANDA\_PRI}

