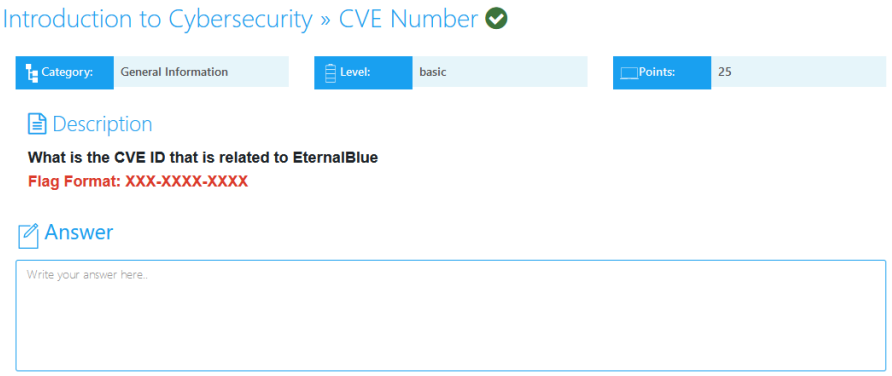
Certified SOC Analyst Writeups

Type	Writeup
Reviewed	☑

CVE Number



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.

Wikepedia 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

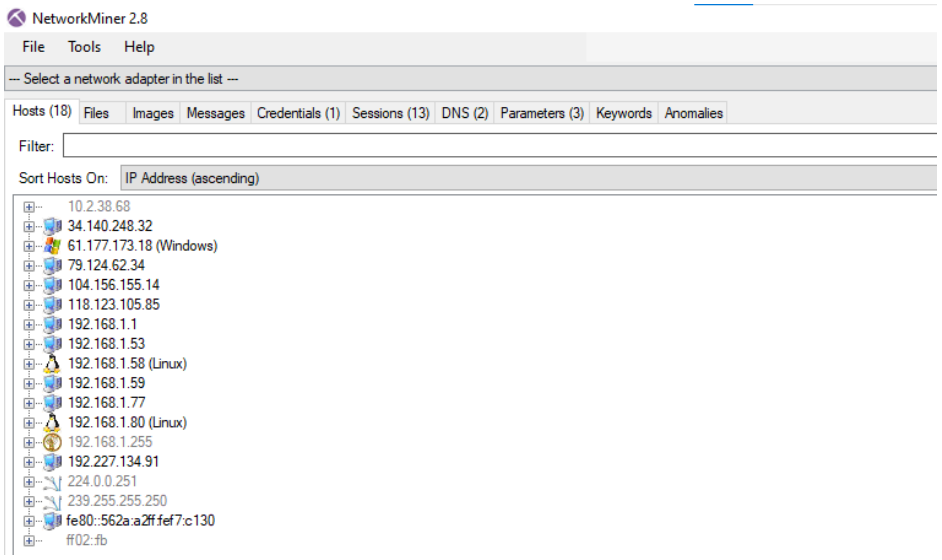
Category: Digital Forensics | Level: medium | Points: 100

Description

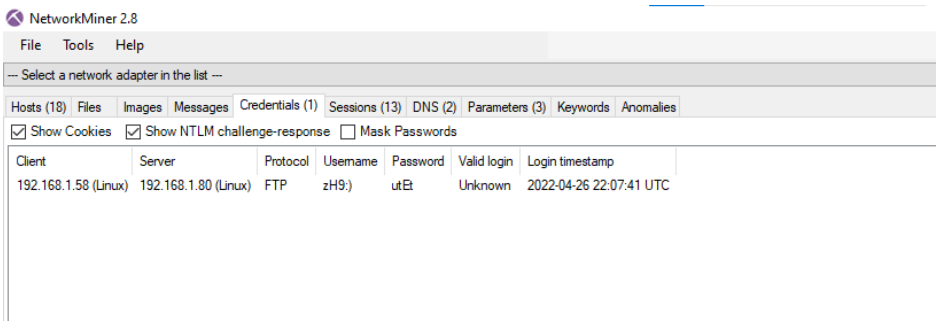
```
Our server compromised due to known vulnerability introduced from many years, Kindly check and identify this flow

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

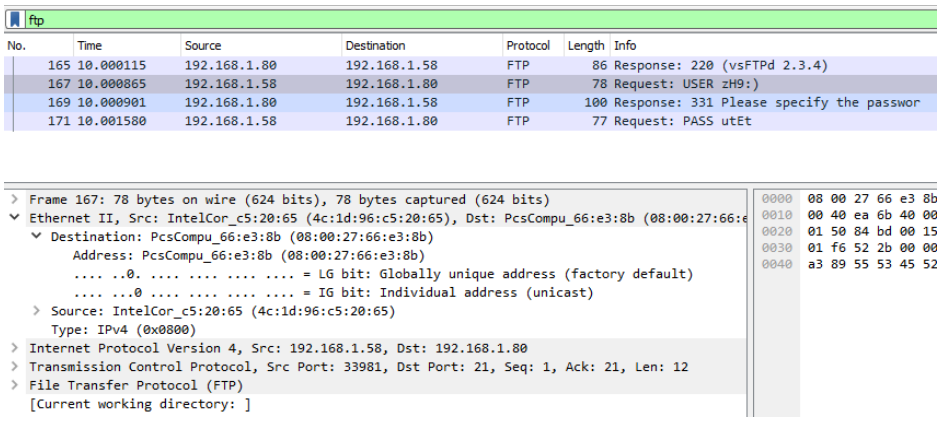
Also the attack is internal because it is within the same subnet mask as the sever IP address

The next step is to figure out what the cve of the vulnerablity 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/ch01lvl1sec18/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

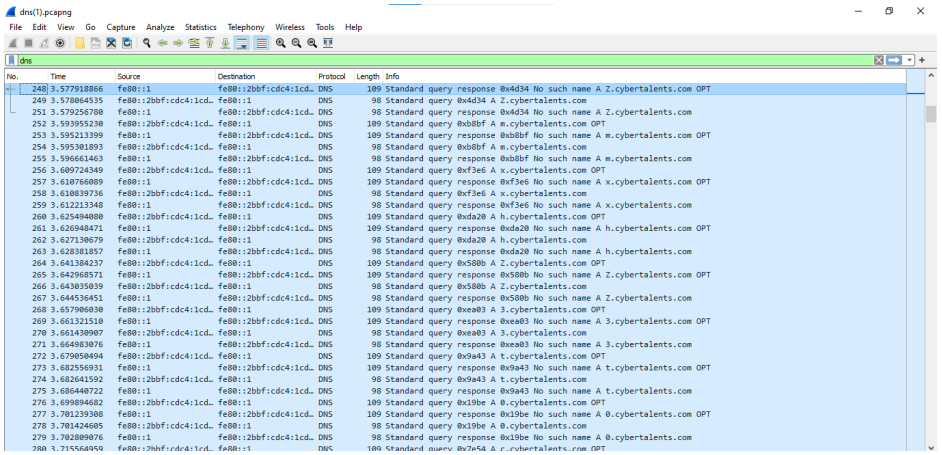
Description

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



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

ZmxhZ3t0c2hBcmtfSXNfQXdlczBtZV9OZXR3MHJraW5nX3RvMGx9

This is a base64 encoded string so decoding it from the internet https://www.base64decode.org/ give the flag;

flag{tshArk_Is_Awes0me_Netw0rking_to0l}

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

```
status="404"
```

7,697 events (before 9/12/23 3:53:47.000 PM) No Event Sampling

Events (7,697) Patterns Statistics Visualization

Time | Event

8/24/16 4:48:21.634 PM

```
{ [-]
  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

src_ip	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”

http.url

>100 Values, 68.611% of events

Selected Yes No

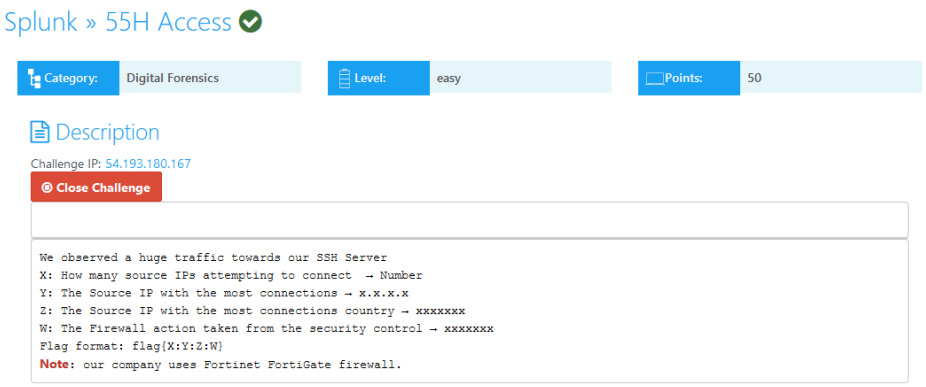
Reports

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

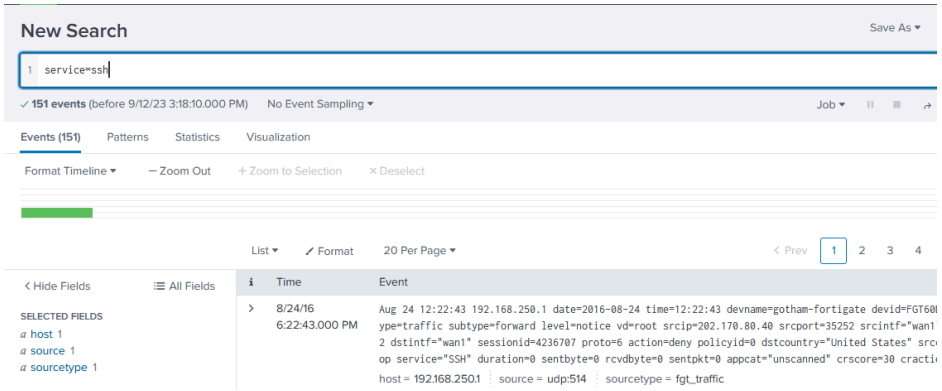
Description

Challenge IP: 54.193.180.167

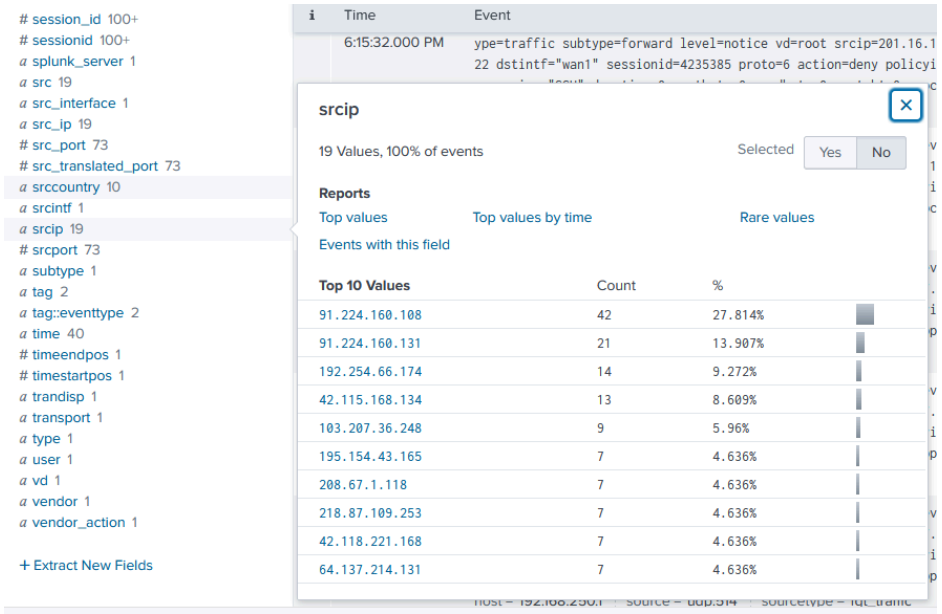
Close Challenge

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 → xxxxxxx
W: The Firewall action taken from the security control → xxxxxxx
Flag format: flag{X:Y:Z:W}
Note: our company uses Fortinet FortiGate firewall.

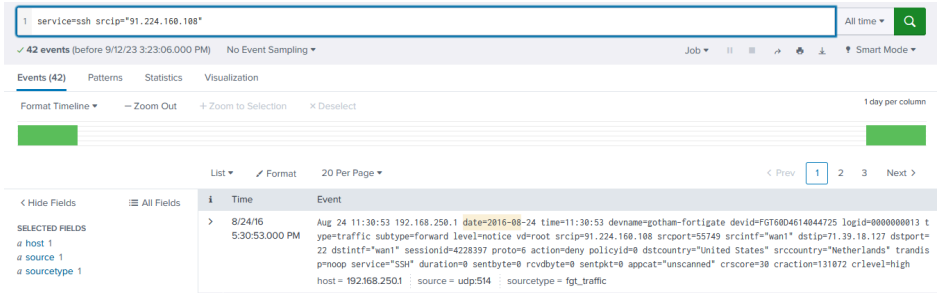
Search for events using the SSH server



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

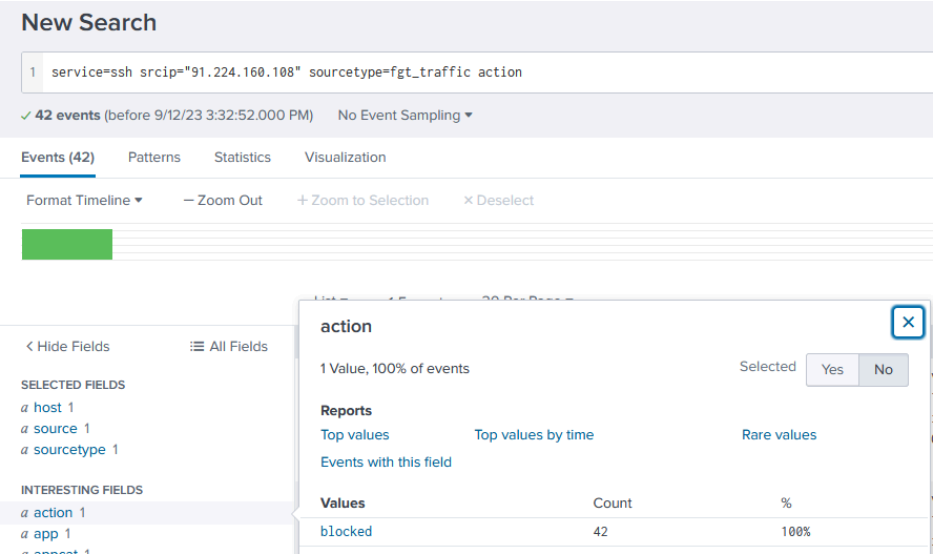


The next thing to look for is the country from which this IP address comes from. This can be done by modifying the search query as shown below



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



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

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
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/UCE/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

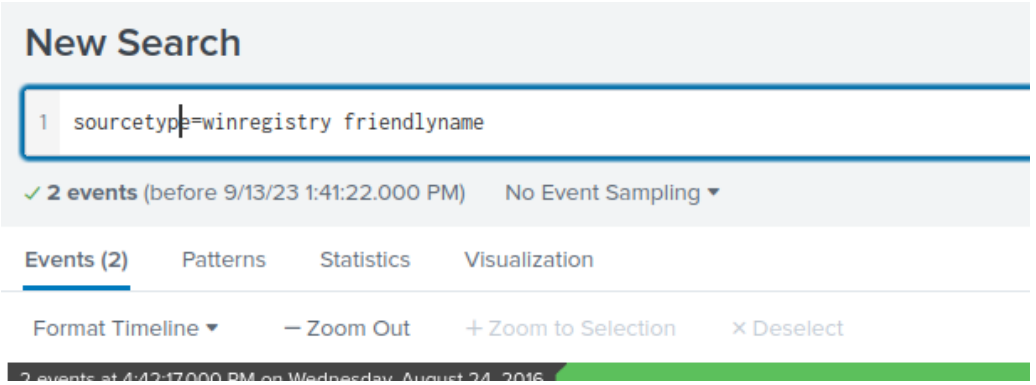
https://lantern.splunk.com/Splunk_Platform/UCE/Security/Incident_Management/Investigating_a_ransomware_attack/File_added_to_the_system_through_external_media

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

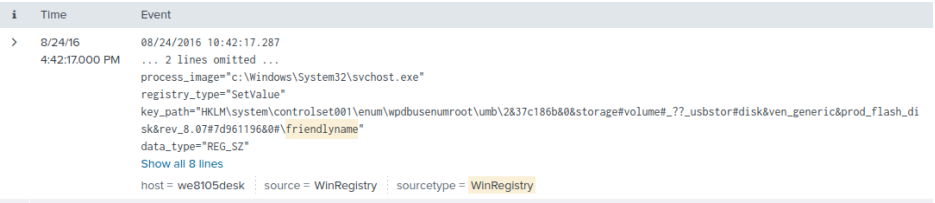
From the instruction “Removable devices connected to a machine”, the following search query is made

`sourcetype=winregistry friendlyname`

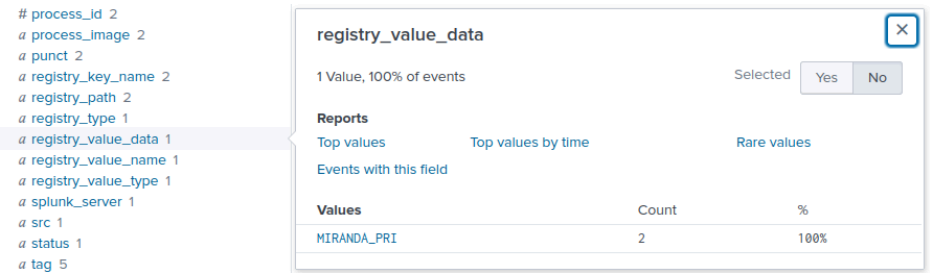
Search for a registry entry value specific to USB devices. If friendlyname doesn’t yield results, try other entries, as described in Microsoft documentation.



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



The value in the “registry_value_data field is the name of the USB device



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}