Intrusion Detection With Zeek

As already discussed, Zeek, formerly known as Bro, is a powerful network security monitoring tool that allows us to delve deep into our network traffic and extract useful insights.

The flexibility and extensibility of Zeek make it a cornerstone of advanced network-based intrusion detection and investigation. With its rich set of logs and extensive scripting capabilities, we can customize it to suit our specific detection requirements and continuously improve our security posture.

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, let's SSH into the Target IP using the provided credentials. The vast majority of the commands covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

Let's move forward and explore some examples of detecting intrusions with Zeek.

Intrusion Detection With Zeek Example 1: Detecting Beaconing Malware

Beaconing is a process by which malware communicates with its command and control (C2) server to receive instructions or exfiltrate data. It's usually characterized by a consistent or patterned interval of outbound communications.

By analyzing connection logs (`conn.log`), we can look for patterns in outbound traffic. These patterns can include repetitive connections to the same destination IP or domain, constant data size in the sent data, or the connection timing. These are all indicative of potential beaconing behavior. Anomalies can be further explored using Zeek scripts specifically designed to spot beaconing patterns.

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ /usr/local/zeek/bin/zeek -C -r /home/htb-student/pcaps/psempire.pcap
```

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat conn.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2023-07-16-12-15-40
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   ser
#types  time    string  addr    port    addr    port    enum    string  interval        count   cou
1511269439.125289       CuQYC98rE69BBb7jb       192.168.56.14   50436   51.15.197.127   80      tcp
1511269436.547667       CTc2Qc2kleCjVaU0V1      fe80::ec23:e8b7:91cb:974d       61431   ff02::1:3
1511269436.548234       Cd4aTbH02m0iB9XS9       192.168.56.14   64755   224.0.0.252     5355    udp
1511269445.266039       CjKEcE3tUWBHhYM93d      192.168.56.14   50437   51.15.197.127   80      tcp
1511269446.190550       CNah6o4OZz5Sr5wGq1      192.168.56.14   50438   51.15.197.127   80      tcp
1511269451.891317       CA6iaN3UgCDI0Sy9x4      192.168.56.14   50439   51.15.197.127   80      tcp
1511269457.130160       ChcRft1mTccVo2yQfa      192.168.56.14   50440   51.15.197.127   80      tcp
1511269462.359918       Clja4s40wWlk8bkAW4      192.168.56.14   50441   51.15.197.127   80      tcp
1511269467.593242       CyE3Th1j6AunL5E3Pl      192.168.56.14   50442   51.15.197.127   80      tcp
1511269472.881671       CwuY7B34I442zmY0hf      192.168.56.14   50443   51.15.197.127   80      tcp
1511269478.120597       CVPMlj3atDGkCy1xyk      192.168.56.14   50444   51.15.197.127   80      tcp
1511269483.366011       Ckn8aZn8c67nuAE19       192.168.56.14   50445   51.15.197.127   80      tcp
1511269488.593094       CfeRTH1oej6g6gA5Li      192.168.56.14   50446   51.15.197.127   80      tcp
1511269493.824701       CWmiwT4QR8u71xp0h       192.168.56.14   50447   51.15.197.127   80      tcp
```


My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

```
1511269499.116879       C113hs4IWwgOGe0hxf      192.168.56.14   50448   51.15.197.127   80      tcp
1511269504.350011       CHI1AHQLm8ybrQ5ti       192.168.56.14   50449   51.15.197.127   80      tcp
1511269509.574454       CIpoyx4Sx3XEyiKbjh      192.168.56.14   50450   51.15.197.127   80      tcp
1511269514.842106       CDLbbm2nnHbr3RO9F9      192.168.56.14   50451   51.15.197.127   80      tcp
1511269520.114079       CipCM33FvSh7hWVHnc      192.168.56.14   50452   51.15.197.127   80      tcp
1511269525.359633       CwMhAI3giczB1gTeR2      192.168.56.14   50453   51.15.197.127   80      tcp
1511269530.579134       CowTCpq1Lon2Rp5T2       192.168.56.14   50454   51.15.197.127   80      tcp
1511269535.801940       CpYwvc23LmuhPsuuMc      192.168.56.14   50455   51.15.197.127   80      tcp
1511269541.044084       Cnvsqj2QcNcWSLBqH7      192.168.56.14   50456   51.15.197.127   80      tcp
1511269546.278570       CgbzqfgMFulKOP1xe       192.168.56.14   50457   51.15.197.127   80      tcp
1511269551.506084       CUlFD949mmSfKATJpc      192.168.56.14   50458   51.15.197.127   80      tcp
1511269556.712264       Cbc1No4FSSjiRQFoNc      192.168.56.14   50459   51.15.197.127   80      tcp
1511269561.963394       CYwON91Js8ssOY4503      192.168.56.14   50460   51.15.197.127   80      tcp
1511269567.178812       Cryspb4A5KOHbIWDY       192.168.56.14   50461   51.15.197.127   80      tcp
1511269572.442802       CRpXje3yCwJlayfhnj      192.168.56.14   50462   51.15.197.127   80      tcp
1511269577.652288       CkudtR34qPv7fMdMJ6      192.168.56.14   50463   51.15.197.127   80      tcp
1511269582.860772       Cmmlvl4K523e8SjCN6      192.168.56.14   50464   51.15.197.127   80      tcp
1511269588.129256       CPaFSTAJAIqVHwzPb       192.168.56.14   50465   51.15.197.127   80      tcp
1511269593.348262       CVz6Zn4A42L2kupGIg      192.168.56.14   50466   51.15.197.127   80      tcp
1511269598.574770       CHfjXhviIEXv6plH9       192.168.56.14   50467   51.15.197.127   80      tcp
1511269603.841610       CuLnP82MDaJG5EGhXf      192.168.56.14   50468   51.15.197.127   80      tcp
1511269609.055326       Cx6Ucw4sZSdBcmcIC4      192.168.56.14   50469   51.15.197.127   80      tcp
1511269614.297715       C1Fmoa1eqrmEFyfoZe      192.168.56.14   50470   51.15.197.127   80      tcp
1511269619.505350       C6d8iu18n9TSiDnsl2      192.168.56.14   50471   51.15.197.127   80      tcp
1511269624.718056       CmMGUH37oYmbgIBhlg      192.168.56.14   50472   51.15.197.127   80      tcp
1511269629.930502       CzI2GE1TrzEeBO1cTi      192.168.56.14   50473   51.15.197.127   80      tcp
1511269635.148168       CjyA8G3Z8uvE4tJVF9      192.168.56.14   50474   51.15.197.127   80      tcp
1511269640.373506       CYyb4A2VWcRgAYvWag      192.168.56.14   50475   51.15.197.127   80      tcp
1511269641.021152       CrYW4H0ghoFV71hA        192.168.56.14   50476   51.15.197.127   80      tcp
1511269646.585189       CbUYsK3SLFNyu6kw1       192.168.56.14   50477   51.15.197.127   80      tcp
1511269651.808258       C9p1Kbt661hlXmlXj       192.168.56.14   50478   51.15.197.127   80      tcp
1511269657.016924       CvxhCA2BroRtMx3fn8      192.168.56.14   50479   51.15.197.127   80      tcp
1511269662.249219       C9uc9Y3j6g4RlJCQE7      192.168.56.14   50480   51.15.197.127   80      tcp
#close  2023-07-16-12-15-40
```

If we look carefully enough we will notice connections being made to `51.15.197.127:80` approximately every 5 seconds, which is indicative of a malware beaconing.

The `psempire.pcap` file, which is located in the `/home/htb-student/pcaps` directory includes traffic related to PowerShell Empire. PowerShell Empire indeed beacons every 5 seconds in its default configuration.

Invest some time in scrutinizing the `psempire.pcap` file using `Wireshark`.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/psempire.pcap .
```

Intrusion Detection With Zeek Example 2: Detecting DNS Exfiltration

Zeek is also useful when we suspect data exfiltration. Data exfiltration can be difficult to detect as it often mimics normal network traffic. However, with Zeek, we can analyze our network traffic at a deeper level.

Zeek's files.log can be used to identify large amounts of data being sent to an unusual external destination, or over non-standard ports, which may suggest data exfiltration. The http.log and dns.log can also be utilized to identify potential covert exfiltration channels, such as DNS tunneling or HTTP POST requests to a suspicious domain.

Furthermore, Zeek's ability to reassemble files transferred over the network (regardless of the protocol used) can assist in identifying the nature of the data being exfiltrated.

PCAP credits to: Oleh Levytskyi and Bogdan Vennyk

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ /usr/local/zeek/bin/zeek -C -r /home/htb-student/pcaps/dnsexfil.pcapng
```

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat dns.log
```

```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dns
#open   2023-07-16-12-28-33
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   tra
        qtype_name      rcode   rcode_name      AA      TC      RD      RA      Z       answers TTL
#types  time    string  addr    port    addr    port    enum    count   interval        string  cou
1630061362.889769       CogoDL3T2prsNPkXhe      192.168.38.104  65463   192.168.38.102  53      udp
1630061369.739218       CTlobe1QTqUhc1CzS3      192.168.38.104  56692   192.168.38.102  53      udp
ne      1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0
1630061429.886391       CQPUxP37HbTlSOdLF6      192.168.38.104  49611   192.168.38.102  53      udp
ne      1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0
1630061469.956241       C0JPXx3z0WuxTE9Tbg      192.168.38.103  51888   192.168.38.102  53      udp
ERNET   1       A       3       NXDOMAIN        F       F       T       F       0       -       -
1630061490.031632       CIMbmp4Wgt287yiERh      192.168.38.104  52584   192.168.38.102  53      udp
ne      1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0
1630061490.175977       CLwvTc2MIadaIReXQd      192.168.38.104  61385   192.168.38.102  53      udp
e.letsgohunt.online     1       C_INTERNET      1       A       0       NOERROR F       F       T
1630061490.316414       CqbrTf39jEUB1hHd37      192.168.38.104  60333   192.168.38.102  53      udp
1.456c54f2.blue.letsgohunt.online       1       C_INTERNET      1       A       0       NOERROR F
1630061490.454478       CQAWsr3oTT6nmG7Hp4      192.168.38.104  53312   192.168.38.102  53      udp
1.456c54f2.blue.letsgohunt.online       1       C_INTERNET      1       A       0       NOERROR F
1630061490.598615       CF17ZJ2eHvUosEjVC       192.168.38.104  64078   192.168.38.102  53      udp
1.456c54f2.blue.letsgohunt.online       1       C_INTERNET      1       A       0       NOERROR F
1630061490.742694       CS0QSmWZe9bUEpNwf       192.168.38.104  54465   192.168.38.102  53      udp
1.456c54f2.blue.letsgohunt.online       1       C_INTERNET      1       A       0       NOERROR F
---SNIP---
```

Let's focus on the requested (sub)domains by leveraging `zeek-cut` as follows.

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat dns.log | /usr/local/zeek/bin/zeek-cut query | cut -d . -f1-7
safebrowsing.google.com
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
wpad.windomain.local
456c54f2.blue.letsgohunt.online
www.180.0c9a5671.456c54f2.blue.letsgohunt.online
www.1204192da26d109d4.1c9a5671.456c54f2.blue.letsgohunt.online
www.11a1855b98d2b71c3.2c9a5671.456c54f2.blue.letsgohunt.online
www.122aa166873fda051.3c9a5671.456c54f2.blue.letsgohunt.online
www.1d91f26756080c945.4c9a5671.456c54f2.blue.letsgohunt.online
www.1302c3663cc8a94f9.5c9a5671.456c54f2.blue.letsgohunt.online
www.1adef2977e4b3653f.6c9a5671.456c54f2.blue.letsgohunt.online
www.111edd479a7512c9c.7c9a5671.456c54f2.blue.letsgohunt.online
www.11483ec078e733131.8c9a5671.456c54f2.blue.letsgohunt.online
www.1f5e94740470d0157.9c9a5671.456c54f2.blue.letsgohunt.online
www.114cbea690a81874a.ac9a5671.456c54f2.blue.letsgohunt.online
www.10db7634eade0b736.bc9a5671.456c54f2.blue.letsgohunt.online
www.1d5aee37e1c25ba02.cc9a5671.456c54f2.blue.letsgohunt.online
www.1d4f517cdcf8807c2.dc9a5671.456c54f2.blue.letsgohunt.online
www.14d71477201813b75.ec9a5671.456c54f2.blue.letsgohunt.online
www.1e3723505f4ebd907.fc9a5671.456c54f2.blue.letsgohunt.online
www.1aa645b2d.10c9a5671.456c54f2.blue.letsgohunt.online
www.1cf2bfe54.11c9a5671.456c54f2.blue.letsgohunt.online
cdn.0600553f0.456c54f2.blue.letsgohunt.online
cdn.1600553f0.456c54f2.blue.letsgohunt.online
cdn.2600553f0.456c54f2.blue.letsgohunt.online
cdn.3600553f0.456c54f2.blue.letsgohunt.online
cdn.4600553f0.456c54f2.blue.letsgohunt.online
cdn.5600553f0.456c54f2.blue.letsgohunt.online
cdn.6600553f0.456c54f2.blue.letsgohunt.online
cdn.7600553f0.456c54f2.blue.letsgohunt.online
cdn.8600553f0.456c54f2.blue.letsgohunt.online
cdn.9600553f0.456c54f2.blue.letsgohunt.online
cdn.a600553f0.456c54f2.blue.letsgohunt.online
cdn.b600553f0.456c54f2.blue.letsgohunt.online
cdn.c600553f0.456c54f2.blue.letsgohunt.online
cdn.d600553f0.456c54f2.blue.letsgohunt.online
cdn.e600553f0.456c54f2.blue.letsgohunt.online
cdn.f600553f0.456c54f2.blue.letsgohunt.online
cdn.10600553f0.456c54f2.blue.letsgohunt.online
post.140.0346c53ab.456c54f2.blue.letsgohunt.online
post.10bb13b53.1346c53ab.456c54f2.blue.letsgohunt.online
post.104fb3984.2346c53ab.456c54f2.blue.letsgohunt.online
post.1bdfe1d1e.3346c53ab.456c54f2.blue.letsgohunt.online
post.19f3acfa6.4346c53ab.456c54f2.blue.letsgohunt.online
```

```
post.107f7e44c.6346c53ab.456c54f2.blue.letsgohunt.online
post.1ab508fac.7346c53ab.456c54f2.blue.letsgohunt.online
post.18ae33d21.8346c53ab.456c54f2.blue.letsgohunt.online
post.11edd6ce8.9346c53ab.456c54f2.blue.letsgohunt.online
post.1979ee0a5.a346c53ab.456c54f2.blue.letsgohunt.online
post.1cc9dd9e9.b346c53ab.456c54f2.blue.letsgohunt.online
post.17b865d4d.c346c53ab.456c54f2.blue.letsgohunt.online
post.1212da6de.d346c53ab.456c54f2.blue.letsgohunt.online
post.177a1fc1a.e346c53ab.456c54f2.blue.letsgohunt.online
post.19e7d023b.f346c53ab.456c54f2.blue.letsgohunt.online
post.1100b6576.10346c53ab.456c54f2.blue.letsgohunt.online
www.1f5e94740470d0157.9c9a5671.456c54f2.blue.letsgohunt.online
sgtqrgcask.windomain.local
zvfepxzuazrlds.windomain.local
kohaqbopxlq.windomain.local
www.1cf2bfe54.11c9a5671.456c54f2.blue.letsgohunt.online
sgtqrgcask.windomain.local
zvfepxzuazrlds.windomain.local
kohaqbopxlq.windomain.local
456c54f2.blue.letsgohunt.online
wpad.windomain.local
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
cdn.013821c34.456c54f2.blue.letsgohunt.online
cdn.113821c34.456c54f2.blue.letsgohunt.online
cdn.213821c34.456c54f2.blue.letsgohunt.online
cdn.313821c34.456c54f2.blue.letsgohunt.online
cdn.313821c34.456c54f2.blue.letsgohunt.online
cdn.413821c34.456c54f2.blue.letsgohunt.online
cdn.513821c34.456c54f2.blue.letsgohunt.online
cdn.613821c34.456c54f2.blue.letsgohunt.online
cdn.713821c34.456c54f2.blue.letsgohunt.online
cdn.813821c34.456c54f2.blue.letsgohunt.online
cdn.913821c34.456c54f2.blue.letsgohunt.online
cdn.a13821c34.456c54f2.blue.letsgohunt.online
cdn.b13821c34.456c54f2.blue.letsgohunt.online
cdn.c13821c34.456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
v10.vortex-win.data.microsoft.com
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
456c54f2.blue.letsgohunt.online
---SNIP---
post.1460.0467121d5.456c54f2.blue.letsgohunt.online
post.11a878166.1467121d5.456c54f2.blue.letsgohunt.online
post.12c1c89cf.2467121d5.456c54f2.blue.letsgohunt.online
post.1bdcdb1fb.3467121d5.456c54f2.blue.letsgohunt.online
post.1a6c6349c.4467121d5.456c54f2.blue.letsgohunt.online
post.14f3d0809.5467121d5.456c54f2.blue.letsgohunt.online
post.172d6c024.6467121d5.456c54f2.blue.letsgohunt.online
post.162ef0f19.7467121d5.456c54f2.blue.letsgohunt.online
post.15b5a7d2f.8467121d5.456c54f2.blue.letsgohunt.online
post.1286fe5b0.9467121d5.456c54f2.blue.letsgohunt.online
post.1fe01b96d.a467121d5.456c54f2.blue.letsgohunt.online
post.1ed530f2f.b467121d5.456c54f2.blue.letsgohunt.online
post.1c8d291d4.c467121d5.456c54f2.blue.letsgohunt.online
post.153699937.d467121d5.456c54f2.blue.letsgohunt.online
post.158c0e1f4.e467121d5.456c54f2.blue.letsgohunt.online
post.139cc5d29.f467121d5.456c54f2.blue.letsgohunt.online
post.1e189482f.10467121d5.456c54f2.blue.letsgohunt.online
post.189c8f742.11467121d5.456c54f2.blue.letsgohunt.online
post.1f6a4e146.12467121d5.456c54f2.blue.letsgohunt.online
post.16ec2a953.13467121d5.456c54f2.blue.letsgohunt.online
post.170c0d25b.14467121d5.456c54f2.blue.letsgohunt.online
post.113540390.15467121d5.456c54f2.blue.letsgohunt.online
post.1ca92006c.16467121d5.456c54f2.blue.letsgohunt.online
post.19092e499.17467121d5.456c54f2.blue.letsgohunt.online
post.1767e291d.18467121d5.456c54f2.blue.letsgohunt.online
post.15bb03130.19467121d5.456c54f2.blue.letsgohunt.online
post.180fe71ad.1a467121d5.456c54f2.blue.letsgohunt.online
post.196a0026d.1b467121d5.456c54f2.blue.letsgohunt.online
post.11a2ec7e4.1c467121d5.456c54f2.blue.letsgohunt.online
post.179b5c2cb.1d467121d5.456c54f2.blue.letsgohunt.online
post.1065838ef.1e467121d5.456c54f2.blue.letsgohunt.online
post.10113b20d.1f467121d5.456c54f2.blue.letsgohunt.online
post.1d78debc8.20467121d5.456c54f2.blue.letsgohunt.online
post.155a1b219.21467121d5.456c54f2.blue.letsgohunt.online
post.1b7ccee56.22467121d5.456c54f2.blue.letsgohunt.online
post.13cbcd295.23467121d5.456c54f2.blue.letsgohunt.online
```

```
post.1cf6a99a5.25467121d5.456c54f2.blue.letsgohunt.online
post.1cc391010.26467121d5.456c54f2.blue.letsgohunt.online
post.18f94bc21.27467121d5.456c54f2.blue.letsgohunt.online
post.1bfb7033c.28467121d5.456c54f2.blue.letsgohunt.online
post.18e36fa94.29467121d5.456c54f2.blue.letsgohunt.online
post.1d141f783.2a467121d5.456c54f2.blue.letsgohunt.online
post.16a96aac3.2b467121d5.456c54f2.blue.letsgohunt.online
post.1f30c5795.2c467121d5.456c54f2.blue.letsgohunt.online
post.196711e3e.2d467121d5.456c54f2.blue.letsgohunt.online
post.1297f6300.2e467121d5.456c54f2.blue.letsgohunt.online
post.16e18e7dd.2f467121d5.456c54f2.blue.letsgohunt.online
post.16a187dd4.30467121d5.456c54f2.blue.letsgohunt.online
post.1b164078f.31467121d5.456c54f2.blue.letsgohunt.online
post.15e30ba0e.32467121d5.456c54f2.blue.letsgohunt.online
post.1829f67d4.33467121d5.456c54f2.blue.letsgohunt.online
post.17675f25b.34467121d5.456c54f2.blue.letsgohunt.online
post.135fc439b.35467121d5.456c54f2.blue.letsgohunt.online
post.13c0803cb.36467121d5.456c54f2.blue.letsgohunt.online
post.1dbcb3f1b.37467121d5.456c54f2.blue.letsgohunt.online
---SNIP---
```

Upon close inspection, it becomes evident that the domain `letsgohunt.online` possesses a significant number of subdomains, similar to cloud providers. However, it's worth noting that interactions with dozens or even hundreds of subdomains are generally not considered typical behavior.

The `dnsexfil.pcapng` file, which is located in the `/home/htb-student/pcaps` directory includes traffic related to DNS exfiltration.

Invest some time in scrutinizing the `dnsexfil.pcapng` file using `Wireshark`.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/dnsexfil.pcapng .
```

Intrusion Detection With Zeek Example 3: Detecting TLS Exfiltration

PCAP credits to: Oleh Levytskyi and Bogdan Vennyk

Let's now go over an example of detecting data exfiltration over TLS.

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ /usr/local/zeek/bin/zeek -C -r /home/htb-student/pcaps/tlsexfil.pcap
```

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat conn.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2023-07-16-12-48-53
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   ser
state   local_orig      local_resp      missed_bytes    history orig_pkts       orig_ip_bytes   res
#types  time    string  addr    port    addr    port    enum    string  interval        count   cou
        count   count   set[string]
1628867750.258715       CdU24818il2WrB5gx9      fe80::4996:7026:833f:a154       546     ff02::1:2
1628867814.448052       CD4narIi677g3tdG7       10.0.10.100     54754   192.168.151.181 443     tcp
1628867874.573558       CCXldM1iyIuyhNiBe2      10.0.10.100     53905   192.168.151.181 443     tcp
1628867877.614701       Cg9e9K1AuI0k4cLZd9      10.0.10.100     53906   192.168.151.181 443     tcp
1628867883.643943       CA91RA1mwdLcwUJbEi      10.0.10.100     53931   192.168.151.181 443     tcp
1628867880.629877       CpYf8hQlyAnrcCcm3       10.0.10.100     53907   192.168.151.181 443     tcp
1628867883.655898       CGYvJ3saMB5dphXmd       10.0.10.100     53932   192.168.151.181 443     tcp
1628867889.688558       CM7Uex4iNNNdDuXQI9      10.0.10.100     53935   192.168.151.181 443     tcp
1628867890.907805       CA797aXtJqeOtKwq2       10.0.10.100     53936   192.168.151.181 443     tcp
1628867886.675238       CMSija4yWhe79PvBRa      10.0.10.100     53933   192.168.151.181 443     tcp
1628867893.923082       C08H2y2GdUfnpjolb8      10.0.10.100     53937   192.168.151.181 443     tcp
1628867896.938711       CkM3724NFKT3yly1ba      10.0.10.100     53938   192.168.151.181 443     tcp
1628867902.969959       CPT4hK31bvSaURqWH3      10.0.10.100     53940   192.168.151.181 443     tcp
```

```
1628867899.954481       Ccz3Dq202Zm8LFrzWl      10.0.10.100     53939   192.168.151.181 443     tcp
1628867909.001101       C19Vw03nPSvVEqus6a      10.0.10.100     53943   192.168.151.181 443     tcp
1628867912.016361       CNhVAiOpkgAh1R8sc       10.0.10.100     53944   192.168.151.181 443     tcp
1628867813.135021       C6tGC34oP3F21KORAa      10.0.10.100     54753   192.168.151.181 80      tcp
1628867915.031768       CFt2xn0eYzCSJ8Tm3       10.0.10.100     53945   192.168.151.181 443     tcp
1628867905.985349       CVQgKN1WiXXgZIEy16      10.0.10.100     53941   192.168.151.181 443     tcp
1628867921.063426       CPAfjN16aDWelGoQa5      10.0.10.100     53947   192.168.151.181 443     tcp
1628867924.078851       C0p8fW3d4pYpG44Jph      10.0.10.100     53948   192.168.151.181 443     tcp
1628867924.087301       CEw1Dx2GLoPquSbp4a      10.0.10.100     53949   192.168.151.181 443     tcp
1628867918.047485       CgnReehqaJvQprHy        10.0.10.100     53946   192.168.151.181 443     tcp
1628867927.110654       CkC7Zh1hj0i8MwNLJ4      10.0.10.100     53951   192.168.151.181 443     tcp
1628867931.281818       CaKMQO2fekZSAErjP       10.0.10.100     53952   192.168.151.181 443     tcp
1628867931.288461       CjcDcAwMHgOaoxGu6       10.0.10.100     53953   192.168.151.181 443     tcp
1628867934.297398       CiEfhC2odzlHli49Q2      10.0.10.100     53954   192.168.151.181 443     tcp
1628867937.313352       CfW6Lb4WRMgJUS7Rn8      10.0.10.100     53955   192.168.151.181 443     tcp
1628867940.328753       CerXJm10bIAxgVVqz5      10.0.10.100     53956   192.168.151.181 443     tcp
1628867940.336125       CsAfy6jGo3uLtDAA5       10.0.10.100     53957   192.168.151.181 443     tcp
1628867946.360157       CFtJB71l1uIyBiy4bl      10.0.10.100     53959   192.168.151.181 443     tcp
1628867949.375797       CXmWZc344kNYukfAZa      10.0.10.100     53961   192.168.151.181 443     tcp
1628867943.344713       C0tEUWB7VYkFzPRVk       10.0.10.100     53958   192.168.151.181 443     tcp
1628867955.407292       C4BsWIqN2EivsCq78       10.0.10.100     60677   192.168.151.181 443     tcp
1628867952.391209       CQ16vl3UTaFE6CAuP1      10.0.10.100     53962   192.168.151.181 443     tcp
1628867958.429096       CCgRqF34Zw0NJKdtc7      10.0.10.100     61579   192.168.151.181 443     tcp
1628867959.112081       CrCSPSO195LUPz6t2       10.0.10.100     61682   10.0.10.1       6000    tcp
1628867959.112205       CCuH0D1XNvS6KOMR4j      10.0.10.100     61683   10.0.10.1       5999    tcp
1628867959.112399       CpYbPQ1Ea1arKY1GQk      10.0.10.100     61684   10.0.10.1       5998    tcp
1628867959.112573       CpHaau3yHk4ZtqPtS2      10.0.10.100     61685   10.0.10.1       5997    tcp
1628867959.112748       CISSiF3c92oAe9BJPd      10.0.10.100     61686   10.0.10.1       5996    tcp
---SNIP---
```

The output is a bit tricky to analyze. Let's narrow things down by using `zeek-cut` one more time.

One-liner source: activecountermeasures

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat conn.log | /usr/local/zeek/bin/zeek-cut id.orig_h id.resp_h orig_bytes
10.0.10.100     192.168.151.181 270775912
10.0.10.100     10.0.10.1       0
```

Let's analyze the command above.

- `cat conn.log`: This command is used to read the content of the conn.log file. The `conn.log` file, generated by Zeek, provides a record of all connections that have taken place in our network.
- `/usr/local/zeek/bin/zeek-cut id.orig_h id.resp_h orig_bytes`: In this case, we're extracting the `id.orig_h` (originating host), `id.resp_h` (responding host), and `orig_bytes` (number of bytes sent by the originating host) fields.
- `sort`: This command is used to sort the output from the previous command. By default, sort will arrange the lines in ascending order based on the contents of the first field (in this case `id.orig_h`).
- `grep -v -e '^$'`: This command filters out any empty lines. The `-v` option inverts the selection, the `-e option allows for a regular expression, and '^$'` matches empty lines.
- `grep -v '-'`: This command filters out lines containing a dash `-`. In the context of Zeek logs, a dash often represents a missing value or an undefined field.
- `datamash -g 1,2 sum 3`: `datamash` is a command-line tool that performs basic numeric, textual, and statistical operations. The `-g 1,2` option groups the output by the first two fields (the IP addresses of the originating and responding hosts), and `sum 3` computes the sum of the third field (the number of bytes sent) for each group.
- `sort -k 3 -rn`: This command sorts the output of the previous command in descending order (`-r`) based on the numerical value (`-n`) of the third field (`-k 3`), which is the sum of `orig_bytes` for each pair of IP addresses.
- `head -10`: This command is used to limit the output to the top 10 lines, thus showing the top 10 pairs of IP addresses by total bytes sent from the originating host to the responding host.

We notice that ~270 MB (actually a bit less) of data have been sent to `192.168.151.181`.

The `tlsexfil.pcap` file, which is located in the `/home/htb-student/pcaps` directory includes traffic related to data exfiltration over TLS.

Invest some time in scrutinizing the `tlsexfil.pcap` file using `Wireshark`.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/tlsexfil.pcap .
```

Intrusion Detection With Zeek Example 4: Detecting PsExec

`PsExec`, a part of the Sysinternals Suite, is frequently used for remote administration within Active Directory environments. Given its powerful capabilities, it's no surprise that adversaries often prefer `PsExec` when they carry out remote code execution attacks.

To illustrate a typical attack sequence, let's consider this: an attacker transfers the binary file `PSEXESVC.exe` to a target machine using the `ADMIN$` share, a special shared folder used in Windows networks, via the SMB (Server Message Block) protocol. Following this, the attacker remotely launches this file as a temporary service by utilizing the `IPC$` share, another special shared resource that enables Inter-Process Communication.

We can identify SMB transfers and the typical use of `PsExec` using Zeek's `smb_files.log`, `dce_rpc.log`, and `smb_mapping.log` as follows.

PCAP source: 401TRG

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ /usr/local/zeek/bin/zeek -C -r /home/htb-student/pcaps/psexec_add_user.pcap
```

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat smb_files.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   smb_files
#open   2023-07-16-17-39-49
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       fuid    act
#types  time    string  addr    port    addr    port    string  enum    string  string  count   str
1507567479.268789       CksrR04Pziy7EPYOT6      192.168.10.31   49282   192.168.10.10   445     -
1507567500.496785       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     -
1507567500.496785       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     -
#close  2023-07-16-17-39-49
```

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat dce_rpc.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dce_rpc
#open   2023-07-16-17-39-49
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       rtt     nam
#types  time    string  addr    port    addr    port    interval        string  string  string
1507567479.286323       CBZaDq4j7VDeXjASO4      192.168.10.31   49283   192.168.10.10   135     0.0
1507567500.281997       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.282353       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.302505       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.302907       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.303301       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
```

```
1507567500.418004       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.418589       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.418987       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.490481       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.490791       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.491208       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.491979       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.492567       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.494209       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.494619       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.495069       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
1507567500.495494       CgPykN2qCki9kzhoh6      192.168.10.31   49285   192.168.10.10   445     0.0
#close  2023-07-16-17-39-49
```

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ cat smb_mapping.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   smb_mapping
#open   2023-07-16-17-39-49
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       path    ser
#types  time    string  addr    port    addr    port    string  string  string  string
1507567479.268407       CksrR04Pziy7EPYOT6      192.168.10.31   49282   192.168.10.10   445     \\\
1507567500.280462       CgPykN2qCki9kzhoh6       192.168.10.31   49285   192.168.10.10   445     \\\
1507567500.496371       CgPykN2qCki9kzhoh6       192.168.10.31   49285   192.168.10.10   445     \\\
#close  2023-07-16-17-39-49
```

The temporary service creation is apparent in the last two logs above.

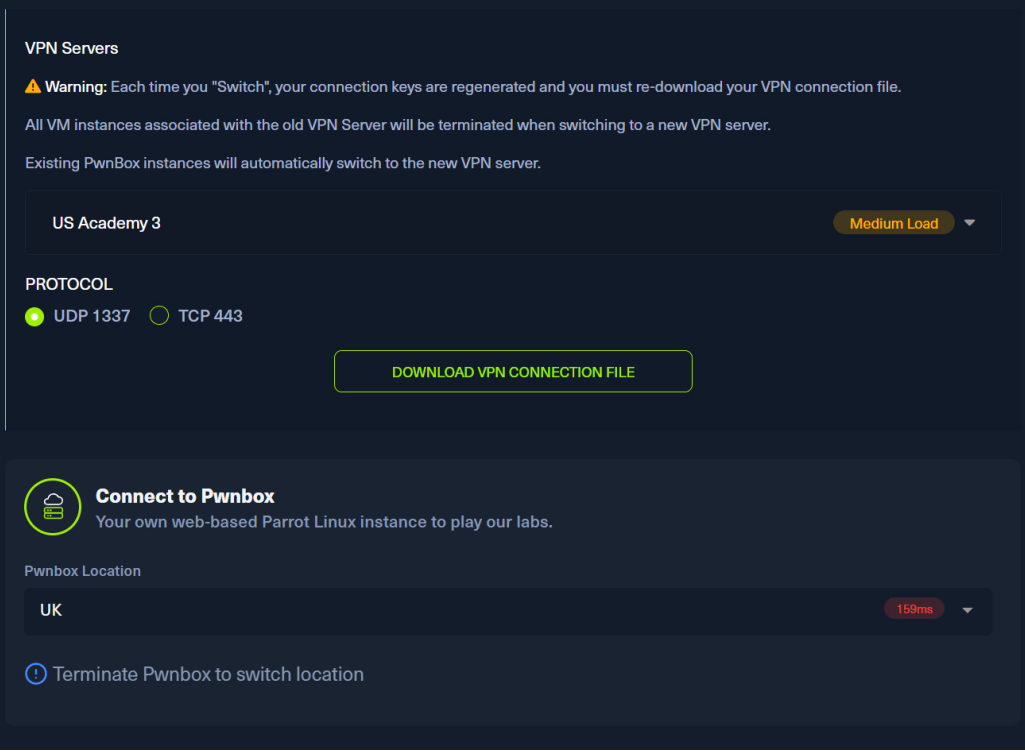
The `psexec_add_user.pcap` file, which is located in the `/home/htb-student/pcaps` directory includes traffic related to typical PsExec usage.

Invest some time in scrutinizing the `psexec_add_user.pcap` file using `Wireshark`.

We can download the PCAP file into the current directory of either Pwnbox or our own VM as follows.

Intrusion Detection With Zeek

```
MisaelMacias@htb[/htb]$ scp htb-student@[TARGET IP]:/home/htb-student/pcaps/psexec_add_user.pcap .
```



Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

SSH to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 2 There is a file named printnightmare.pcap in the /home/htb-student/pcaps directory, which contains network traffic related to the PrintNightmare (https://labs.jumpsec.com/printnightmare-network-analysis/) vulnerability. Enter the zeek log that can help us identify the suspicious spooler functions as your answer. Answer format: _.log

dce_rpc.log

Submit

SSH to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 2 There is a file named revilkaseya.pcap in the /home/htb-student/pcaps directory, which contains network traffic related to the REvil ransomware Kaseya supply chain attack. Enter the total number of bytes that the victim has transmitted to the IP address 178.23.155.240 as your answer.

2311

Submit

Previous Next

Mark Complete & Next