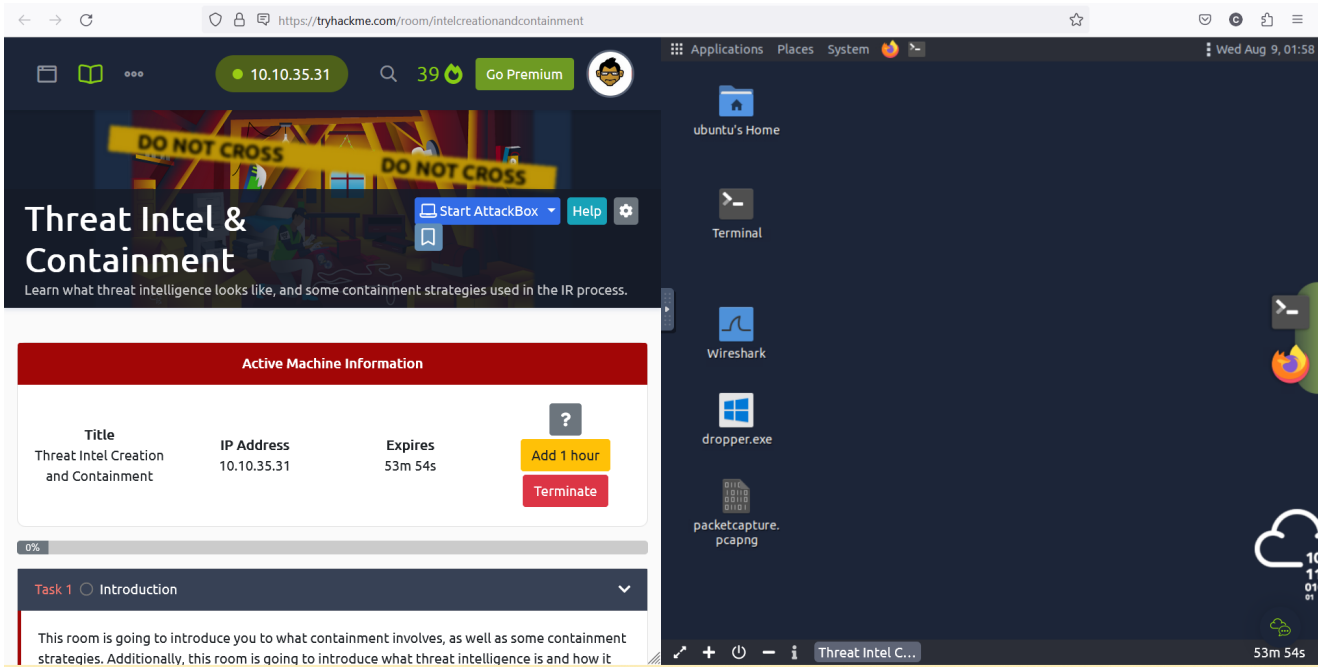
Threat Intel & Containment

09082023Wed

[TryHackMe | Threat Intel & Containment]

```
Learn what threat intelligence looks like, and some containment strategies used
in the IR process.
```



https://tryhackme.com/room/mitre

https://tryhackme.com/room/introtosiem

https://www.elastic.co/beats/packetbeat

https://tryhackme.com/room/wazuhct

https://osint.digitalside.it/

https://otx.alienvault.com/

https://threatfeeds.io/

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

https://www.ncsc.gov.uk/collection/incident-management

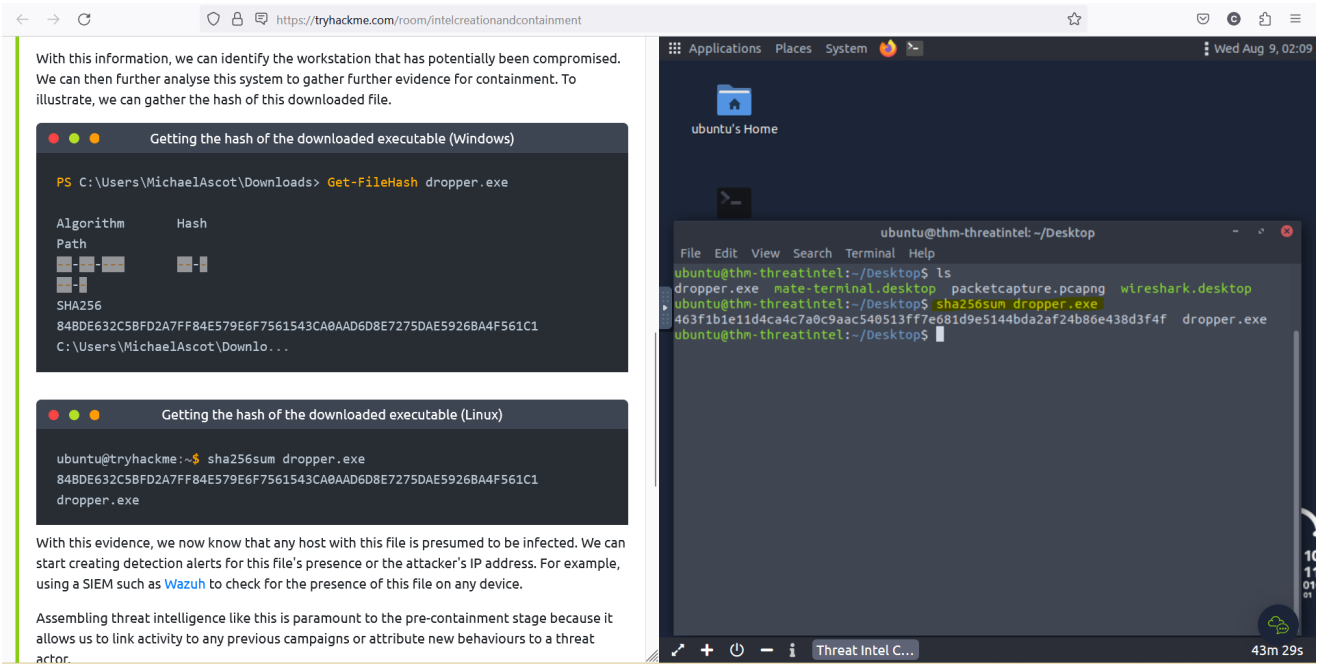
https://www.sans.org/media/score/504-incident-response-cycle.pdf

url.full: Descending	Count
http://3.250.38.141/	3
http://3.250.38.141/dropper.exe	1
http://3.250.38.141/favicon.ico	1
http://edge-http.microsoft.com/captiveportal/generate_204	1
http://www.talonix.com/	1

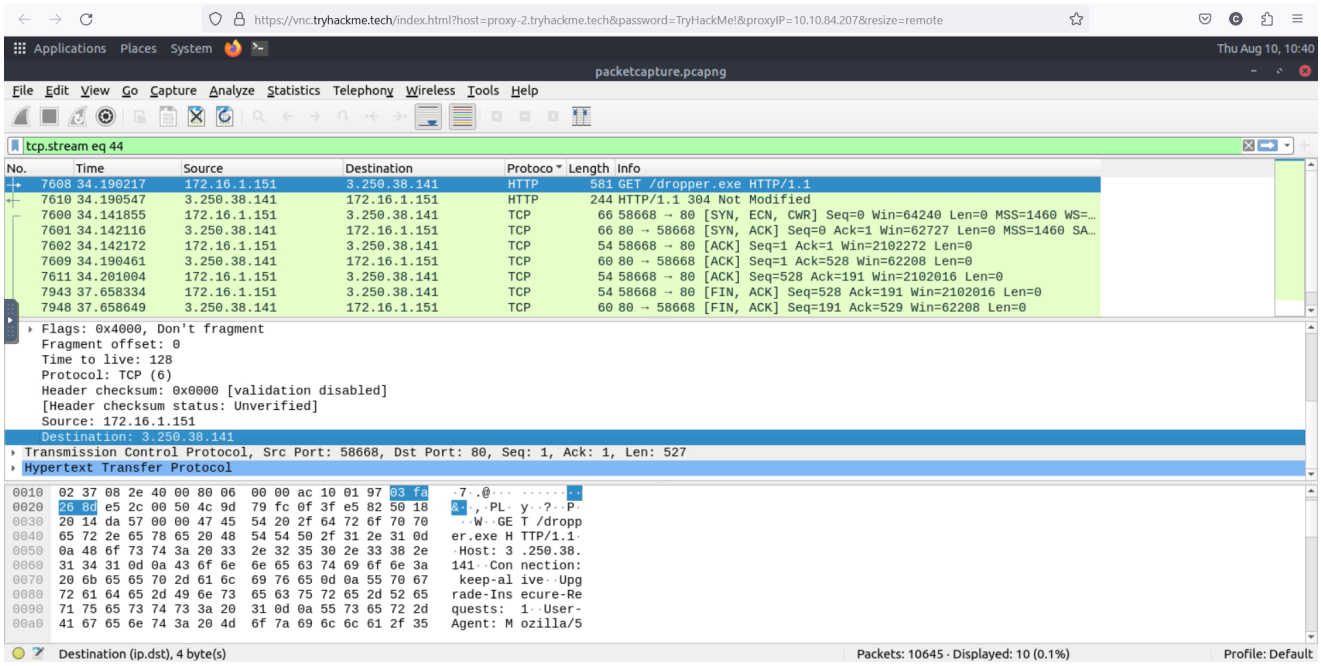
```
Get-FileHash dropper.exe
```

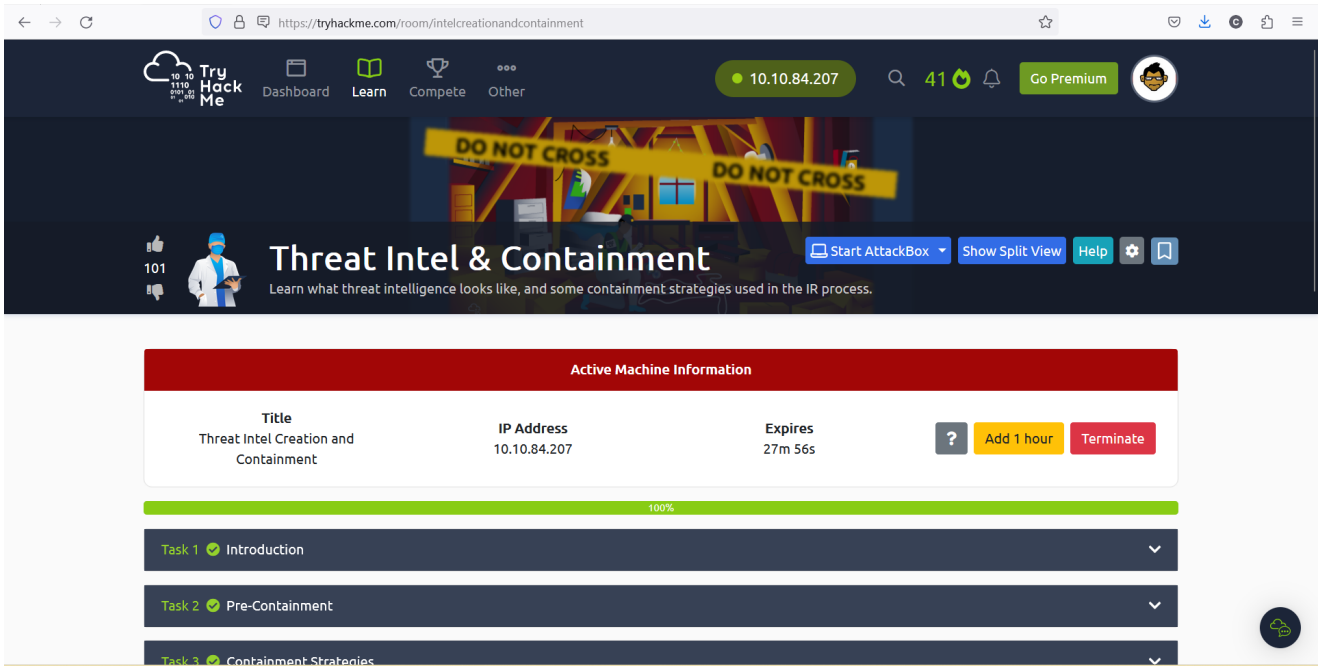
```
sha256sum dropper.exe
```

```
463f1b1e11d4ca4c7a0c9aac540513ff7e681d9e5144bda2af24b86e438d3f4f  dropper.exe
```



10082023Thu


https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=TryHackMe!&proxyIP=10.10.84.207&resize=remote
Applications Places System
Thu Aug 10, 10:40
packetcapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 44
No. Time Source Destination Protoco Length Info
7608 34.190217 172.16.1.151 3.250.38.141 HTTP 581 GET /dropper.exe HTTP/1.1
7610 34.190547 3.250.38.141 172.16.1.151 HTTP 244 HTTP/1.1 304 Not Modified
7600 34.141855 172.16.1.151 3.250.38.141 TCP 66 58668 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=…
7601 34.142116 3.250.38.141 172.16.1.151 TCP 66 80 → 58668 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SA…
7602 34.142172 172.16.1.151 3.250.38.141 TCP 54 58668 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
7609 34.190461 3.250.38.141 172.16.1.151 TCP 60 80 → 58668 [ACK] Seq=1 Ack=528 Win=62208 Len=0
7611 34.201004 172.16.1.151 3.250.38.141 TCP 54 58668 → 80 [ACK] Seq=528 Ack=191 Win=2102016 Len=0
7943 37.658334 172.16.1.151 3.250.38.141 TCP 54 58668 → 80 [FIN, ACK] Seq=528 Ack=191 Win=2102016 Len=0
7948 37.658649 3.250.38.141 172.16.1.151 TCP 60 80 → 58668 [FIN, ACK] Seq=191 Ack=529 Win=62208 Len=0
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.1.151
Destination: 3.250.38.141
Transmission Control Protocol, Src Port: 58668, Dst Port: 80, Seq: 1, Ack: 1, Len: 527
Hypertext Transfer Protocol
0010 02 37 08 2e 40 00 80 06 00 00 ac 10 01 97 03 fa
0020 26 8d e5 2c 00 50 4c 9d 79 fc 0f 3f e5 82 50 18
0030 20 14 da 57 00 00 47 45 54 20 2f 64 72 6f 70 70
0040 65 72 2e 65 78 65 20 48 54 54 50 2f 31 2e 31 0d
0050 0a 48 6f 73 74 3a 20 33 2e 32 35 30 2e 33 38 2e
0060 31 34 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a
0070 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67
0080 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65
0090 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d
00a0 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35
Destination (ip.dst), 4 byte(s)
Packets: 10645 · Displayed: 10 (0.1%)
Profile: Default


https://tryhackme.com/room/intelcreationandcontainment
Try Hack Me
Dashboard
Learn
Compete
Other
10.10.84.207
41
Go Premium
DO NOT CROSS
DO NOT CROSS
101
Threat Intel & Containment
Learn what threat intelligence looks like, and some containment strategies used in the IR process.
Start AttackBox
Show Split View
Help
Active Machine Information
Title
Threat Intel Creation and Containment
IP Address
10.10.84.207
Expires
27m 56s
?
Add 1 hour
Terminate
100%
Task 1 Introduction
Task 2 Pre-Containment
Task 3 Containment Strategies