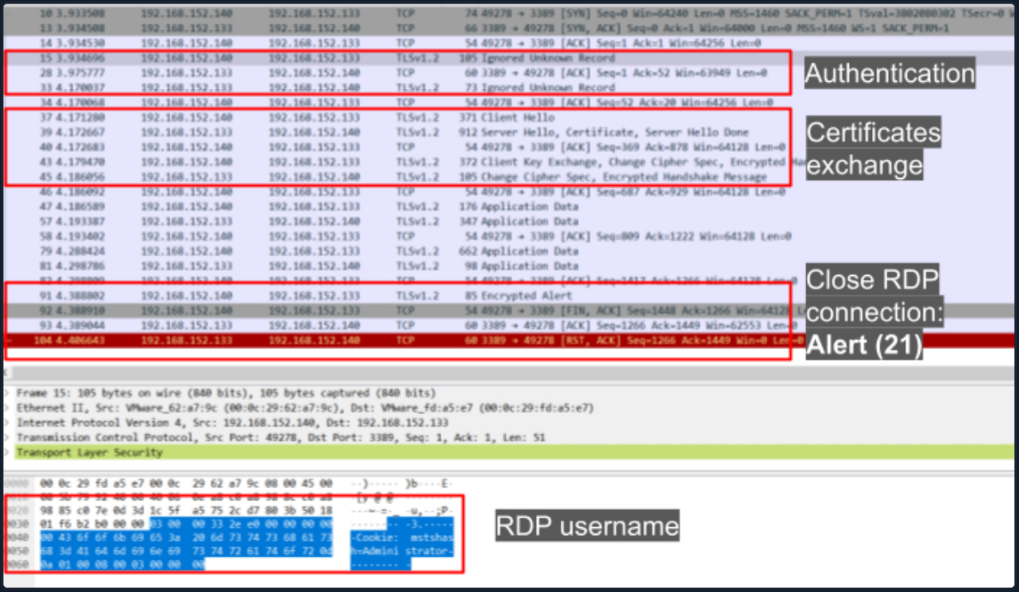
Detecting RDP Brute Force Attacks

We often encounter `Remote Desktop Protocol (RDP) brute force attacks` as a favorite vector for attackers to gain initial foothold in a network. The concept of an RDP brute force attack is relatively straightforward: attackers attempt to login into a Remote Desktop session by systematically guessing and trying different passwords until they find the correct one. This method exploits the fact that many users often have weak or default passwords that are easy to guess.

How RDP Traffic Looks Like



```
10 3.933508   192.168.152.140   192.168.152.133   TCP       74 49278 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3802000302 TSecr=0 W
13 3.934508   192.168.152.133   192.168.152.140   TCP       66 3389 → 49278 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1
14 3.934530   192.168.152.140   192.168.152.133   TCP       54 49278 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0
15 3.934696   192.168.152.140   192.168.152.133   TLSv1.2  105 Ignored Unknown Record
28 3.975777   192.168.152.133   192.168.152.140   TCP       60 3389 → 49278 [ACK] Seq=1 Ack=52 Win=63949 Len=0
33 4.170037   192.168.152.133   192.168.152.140   TLSv1.2   73 Ignored Unknown Record
34 4.170068   192.168.152.140   192.168.152.133   TCP       54 49278 → 3389 [ACK] Seq=52 Ack=20 Win=64256 Len=0
37 4.171280   192.168.152.140   192.168.152.133   TLSv1.2  371 Client Hello
39 4.172667   192.168.152.133   192.168.152.140   TLSv1.2  912 Server Hello, Certificate, Server Hello Done
40 4.172683   192.168.152.140   192.168.152.133   TCP       54 49278 → 3389 [ACK] Seq=369 Ack=878 Win=64128 Len=0
43 4.179470   192.168.152.140   192.168.152.133   TLSv1.2  372 Client Key Exchange, Change Cipher Spec, Encrypted Ha
45 4.186056   192.168.152.133   192.168.152.140   TLSv1.2  105 Change Cipher Spec, Encrypted Handshake Message
46 4.186092   192.168.152.140   192.168.152.133   TCP       54 49278 → 3389 [ACK] Seq=687 Ack=929 Win=64128 Len=0
47 4.186589   192.168.152.140   192.168.152.133   TLSv1.2  176 Application Data
57 4.193387   192.168.152.133   192.168.152.140   TLSv1.2  347 Application Data
58 4.193402   192.168.152.140   192.168.152.133   TCP       54 49278 → 3389 [ACK] Seq=809 Ack=1222 Win=64128 Len=0
79 4.288424   192.168.152.140   192.168.152.133   TLSv1.2  662 Application Data
81 4.298786   192.168.152.133   192.168.152.140   TLSv1.2   98 Application Data
82 4.288800   192.168.152.140   192.168.152.133   TCP       54 49278 → 3389 [ACK] Seq=1417 Ack=1266 Win=64128 Len=0
91 4.388802   192.168.152.140   192.168.152.133   TLSv1.2   85 Encrypted Alert
92 4.388910   192.168.152.140   192.168.152.133   TCP       54 49278 → 3389 [FIN, ACK] Seq=1448 Ack=1266 Win=64128 Le
93 4.389044   192.168.152.133   192.168.152.140   TCP       60 3389 → 49278 [ACK] Seq=1266 Ack=1449 Win=62553 Len=0
104 4.406643  192.168.152.133   192.168.152.140   TCP       60 3389 → 49278 [RST, ACK] Seq=1266 Ack=1449 Win=0 Len=0

> Frame 15: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
> Ethernet II, Src: VMware_62:a7:9c (00:0c:29:62:a7:9c), Dst: VMware_fd:a5:e7 (00:0c:29:fd:a5:e7)
> Internet Protocol Version 4, Src: 192.168.152.140, Dst: 192.168.152.133
> Transmission Control Protocol, Src Port: 49278, Dst Port: 3389, Seq: 1, Ack: 1, Len: 51
> Transport Layer Security

0000  00 0c 29 fd a5 e7 00 0c  29 62 a7 9c 08 00 45 00   ..)..... )b....E.
0020  98 85 c0 7e 0d 3d 1c 5f  a5 75 2c d7 80 3b 50 18   ...~.=._ .u,..;P.
0030  01 f6 b2 b0 00 00 03 00  00 33 2e e0 00 00 00 00   ........ .3......
0040  00 43 6f 6f 6b 69 65 3a  20 6d 73 74 73 68 61 73   .Cookie:  mstshas
0050  68 3d 41 64 6d 69 6e 69  73 74 72 61 74 6f 72 0d   h=Admini strator.
0060  0a 01 00 08 00 03 00 00  00                        ........ .
```

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at https://[Target IP]:8000 and launch the Search & Reporting Splunk application. The vast majority of searches 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.

Additionally, we can access the spawned target via RDP as outlined below. All files, logs, and PCAP files related to the covered attacks can be found in the /home/htb-student and /home/htb-student/module_files directories.

Detecting RDP Brute Force Attacks

```
MisaelMacias@htb[/htb]$ xfreerdp /u:htb-student /p:'HTB_@cademy_stdnt!' /v:[Target IP] /dynamic-res
```

Related Evidence

- **Related Directory**: `/home/htb-student/module_files/rdp_bruteforce`
- **Related Splunk Index**: `rdp_bruteforce`
- **Related Splunk Sourcetype**: `bro:rdp:json`

Detecting RDP Brute Force Attacks With Splunk & Zeek Logs

Now let's explore how we can identify RDP brute force attacks, using Splunk and Zeek logs.

Resources

? Go to Questions

Table of Contents

Leveraging Windows Event Logs

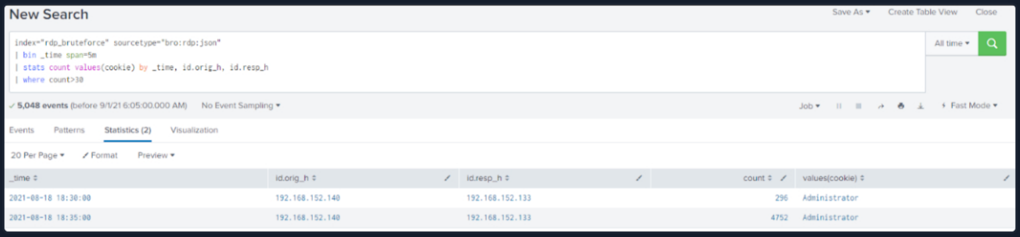
Leveraging Splunk's Application Capabilities

Leveraging Zeek Logs

Skills Assessment

Detecting RDP Brute Force Attacks

```
index="rdp_bruteforce" sourcetype="bro:rdp:json"
| bin _time span=5m
| stats count values(cookie) by _time, id.orig_h, id.resp_h
| where count>30
```



New Search

```
index="rdp_bruteforce" sourcetype="bro:rdp:json"
| bin _time span=5m
| stats count values(cookie) by _time, id.orig_h, id.resp_h
| where count>30
```

✓ 5,048 events (before 9/1/21 6:05:00.000 AM) No Event Sampling ▾

_time	id.orig_h	id.resp_h	count	values(cookie)
2021-08-18 18:30:00	192.168.152.140	192.168.152.133	296	Administrator
2021-08-18 18:35:00	192.168.152.140	192.168.152.133	4752	Administrator

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 Medium Load ▾

PROTOCOL

● UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 139ms ▾

ⓘ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start

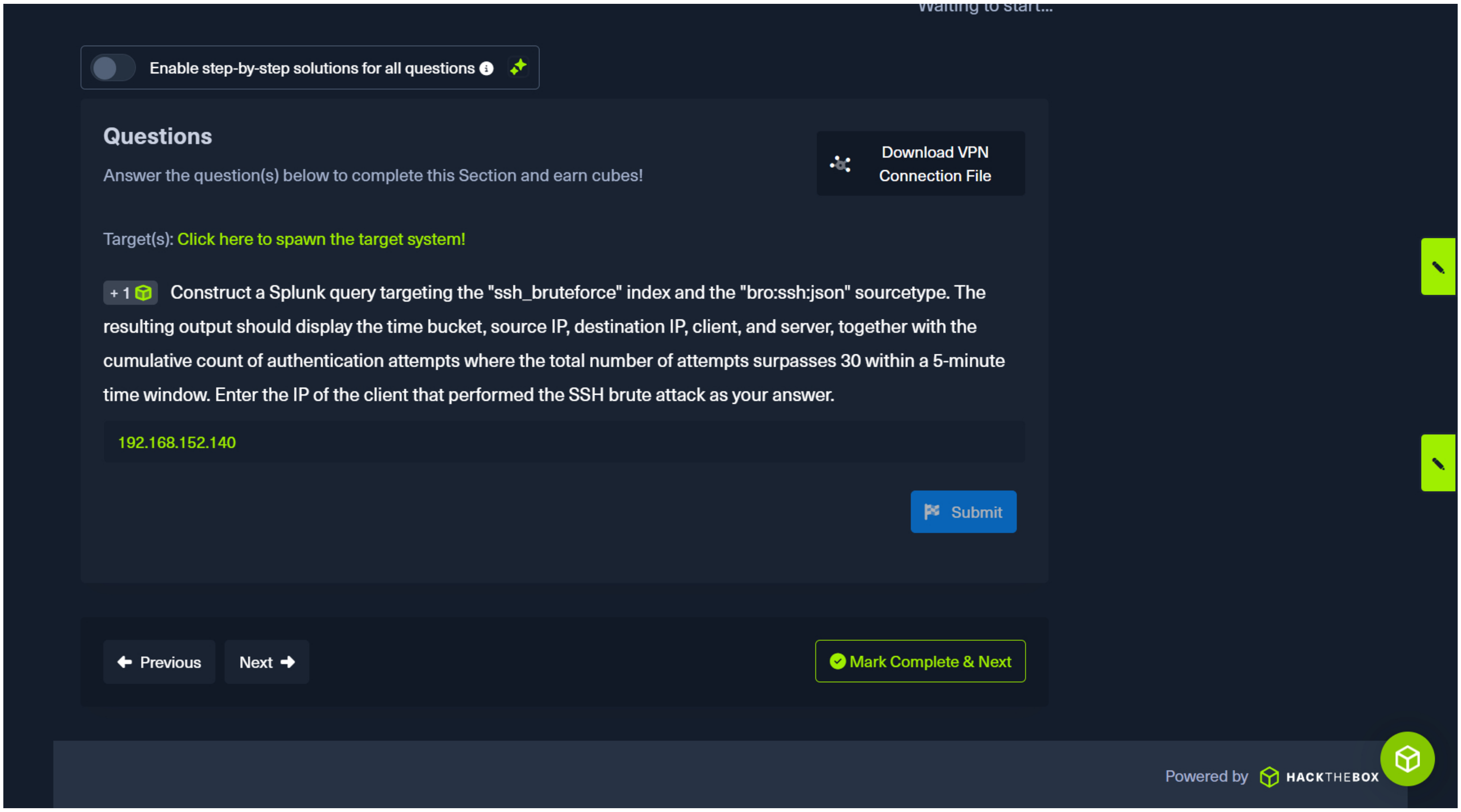
Skills Assessment ☑

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left



Questions

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

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

Construct a Splunk query targeting the "ssh_bruteforce" index and the "bro:ssh:json" sourcetype. The resulting output should display the time bucket, source IP, destination IP, client, and server, together with the cumulative count of authentication attempts where the total number of attempts surpasses 30 within a 5-minute time window. Enter the IP of the client that performed the SSH brute attack as your answer.

192.168.152.140