Detecting Kerberos Brute Force Attacks

When adversaries perform `Kerberos-based user enumeration`, they send an AS-REQ (Authentication Service Request) message to the Key Distribution Center (KDC), which is responsible for handling Kerberos authentication. This message includes the username they're trying to validate. They pay close attention to the response they receive, as it reveals valuable information about the existence of the specified user account.

A valid username will prompt the server to `return a TGT` or raise an error like `KRB5KDC_ERR_PREAUTH_REQUIRED`, indicating that preauthentication is required. On the other hand, an invalid username will be met with a Kerberos error code `KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN` in the AS-REP (Authentication Service Response) message. By examining the responses to their AS-REQ messages, adversaries can quickly determine which usernames are valid on the target system.

How Kerberos Brute Force Attacks Look Like On The Wire

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
3206	14.697848	192.168.38.104	192.168.38.102	KRB5	287	AS-REQ
3207	14.698175	192.168.38.102	192.168.38.104	KRB5	160	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
3216	14.755297	192.168.38.104	192.168.38.102	KRB5	289	AS-REQ
3217	14.755607	192.168.38.102	192.168.38.104	KRB5	160	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
3226	14.811835	192.168.38.104	192.168.38.102	KRB5	291	AS-REQ
3227	14.812134	192.168.38.102	192.168.38.104	KRB5	160	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
3236	14.869272	192.168.38.104	192.168.38.102	KRB5	289	AS-REQ
3237	14.869599	192.168.38.102	192.168.38.104	KRB5	160	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
3246	14.926350	192.168.38.104	192.168.38.102	KRB5	292	AS-REQ
3247	14.926667	192.168.38.102	192.168.38.104	KRB5	160	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
3256	14.983953	192.168.38.104	192.168.38.102	KRB5	291	AS-REQ
3257	14.984290	192.168.38.102	192.168.38.104	KRB5	160	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
3266	15.042399	192.168.38.104	192.168.38.102	KRB5	288	AS-REQ
3267	15.042723	192.168.38.102	192.168.38.104	KRB5	160	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
3276	15.098845	192.168.38.104	192.168.38.102	KRB5	296	AS-REQ

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 Kerberos 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/kerberos_bruteforce`
- `Related Splunk Index: kerberos_bruteforce`
- `Related Splunk Sourcetype: bro:kerberos:json`

Detecting Kerberos Brute Force Attacks With Splunk & Zeek Logs

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

Detecting Kerberos Brute Force Attacks

```
index="kerberos_bruteforce" sourcetype="bro:kerberos:json"
error_msg!=KDC_ERR_PREAUTH_REQUIRED
success="false" request_type=AS
| bin _time span=5m
| stats count dc(client) as "Unique users" values(error_msg) as "Error messages" by _time, id.orig_
| where count>30
```

New Search

Save As ▾ Create Table View Close

```
1 index="kerberos_bruteforce" sourcetype="bro:kerberos:json"
2 error_msg!=KDC_ERR_PREAUTH_REQUIRED
3 success="false" request_type=AS
4 | bin _time span=5m
5 | stats count dc(client) as "Unique users" values(error_msg) as "Error messages" by _time, id.orig_h, id.resp_h
6 | where count>30
```

All time ▾

✓ **593 events** (before 8/19/23 1:34:04.000 PM) No Event Sampling ▾ Job ▾ Fast Mode ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

_time	id.orig_h	id.resp_h	count	Unique users	Error messages
2021-08-21 12:35:00	192.168.38.104	192.168.38.102	593	593	KDC_ERR_C_PRINCIPAL_UNKNOWN

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 — 140ms ▾

ⓘ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Skills Assessment

My Workstation

OFFLINE

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!

+ 0 Use the "kerberos_bruteforce" index and the "bro:kerberos:json" sourcetype. Was the "accrescent/windomain.local" account part of the Kerberos user enumeration attack? Answer format: Yes, No

Yes

Submit

Previous Next

Mark Complete & Next