

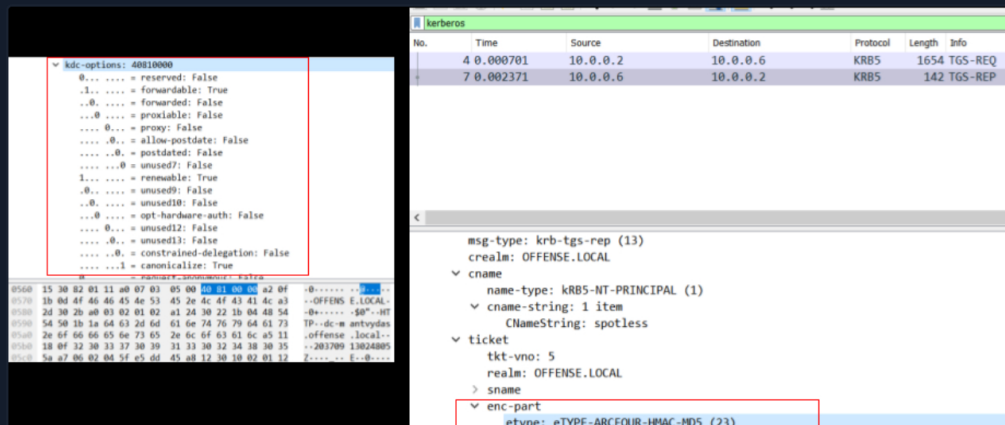
Detecting Kerberoasting

In 2016, a number of blog posts and articles emerged discussing the tactic of querying Service Principal Name (SPN) accounts and their corresponding tickets, an attack that came to be known as **Kerberoasting**. By possessing just one legitimate user account and its password, an attacker could retrieve the SPN tickets and attempt to break them offline.

After examining numerous resources on kerberoasting, it is evident that **RC4** is utilized for ticket encryption behind the scenes. We will exploit this underpinning as a detection point in this section.

Evidence Source: <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/t1208-kerberoasting>

How Kerberoasting Traffic Looks Like



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](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 Kerberoasting

```
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/sharphound`
- Related Splunk Index: `sharphound`
- Related Splunk Sourcetype: `bro:kerberos:json`

Detecting Kerberoasting With Splunk & Zeek Logs

Now let's explore how we can identify Kerberoasting, using Splunk and Zeek logs.

Resources

? Go to Questions

Table of Contents

Leveraging Windows Event Logs

- ✓ Detecting Common User/Domain Recon
- ✓ Detecting Password Spraying
- ✓ Detecting Responder-like Attacks
- ✓ Detecting Kerberoasting/AS-REProasting
- ✓ Detecting Pass-the-Hash
- ✓ Detecting Pass-the-Ticket
- ✓ Detecting Overpass-the-Hash
- ✓ Detecting Golden Tickets/Silver Tickets
- ✓ Detecting Unconstrained Delegation/Constrained Delegation Attacks
- ✓ Detecting DCSync/DCShadow

Leveraging Splunk's Application Capabilities

- ✓ Creating Custom Splunk Applications

Leveraging Zeek Logs

- ✓ Detecting RDP Brute Force Attacks
- ✓ Detecting Beaconing Malware
- ✓ Detecting Nmap Port Scanning
- ✓ Detecting Kerberos Brute Force Attacks
- ✓ Detecting Kerberoasting
- ✓ Detecting Golden Tickets
- ✓ Detecting Cobalt Strike's PSEXec
- ✓ Detecting Zerologon
- ✓ Detecting Exfiltration (HTTP)
- ✓ Detecting Exfiltration (DNS)
- ✓ Detecting Ransomware

Skills Assessment

Detecting Kerberoasting

```
index="sharphound" sourcetype="bro:kerberos:json"
request_type=TGS cipher="rc4-hmac"
forwardable="true" renewable="true"
| table _time, id.orig_h, id.resp_h, request_type, cipher, forwardable, renewable, client, service
```

New Search

```
1 index="sharphound" sourcetype="bro:kerberos:json"
2 request_type=TGS cipher="rc4-hmac"
3 forwardable="true" renewable="true"
4 | table _time, id.orig_h, id.resp_h, request_type, cipher, forwardable, renewable, client, service
```

14 events before 8/29/24 9:03:52.000 AM. No Event Sampling

Events (14)		Patterns		Statistics (14)		Visualization										
20 Per Page		Format		Preview												
_time		id.orig_h		id.resp_h		request_type		cipher		forwardable		renewable		client		service
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:12		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:11		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL
2021-08-25 14:34:11		10.0.10.100		10.0.10.20		TGS		rc4-hmac		true		true		Administrator/LAB_INTERNAL.LOCAL		cifs/DC.LAB_INTERNAL.LOCAL

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

137ms

ⓘ 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!](#)

+ 1

What port does the attacker use for communication during the Kerberoasting attack?

88

Submit

← Previous

Next →

✔ Mark Complete & Next

Powered by HACKTHEBOX

