Kerberoast Attack Techniques

In this blog we will focus on Kerberoast attack techniques (Old Technique and New Technique).

NOV 1, 2017 EST READ TIME: 5 MIN

COBALT

In this blog we will focus on Kerberoast attack techniques (Old Technique and New Technique). I will try to cover the basics about Kerberos protocol and then we will see the attacking techniques from a penetration testing perspective.

What is Kerberos?

Kerberos is designed to provide authentication of user identity in a networked computing environment consisting of workstations and servers.

Kerberos Defined

Kerberos is an exploitation attack that extracts service account credentials with a combination of weak encryption and poor service account passwords.

Kerberos in a Nutshell

The Kerberos authentication system is built on top of tickets served by KDC. The core idea behind Kerberos is that the users don't share account passwords to each service they want to use. Instead, they share a ticket which they get from KDC.

Steps in Kerberos Authentication

- Password converted to **NTLM hash**, a timestamp is encrypted with the hash and sent to the

- The **Domain Controller** (KDC) checks user information & creates **Ticket-Granting Ticket** (TGT).
- The TGT is encrypted, signed, & delivered to the user (AS-Reply). Only the Kerberos service (**KRBTGT**) in the domain can open and read TGT data.

- The User presents the TGT to the DC when requesting a **Ticket Granting Service** (TGS) ticket (TGS-Request). The data in the TGT is effectively copied to create the TGS ticket.
- The TGS is encrypted using the target service accounts' NTLM password hash and sent to the user (TGS-Reply).
- The user connects to the server hosting the service on the appropriate port & presents the TGS. The service opens the TGS ticket using its NTLM password hash.

Kerberos Attacks:

There are several different types of Kerberos attacks ranging from recon (SPN Scanning), to offline service account password cracking (Kerberoast), to persistence (Silver & Golden Tickets).

Here are the most popular AD Kerberos attacks:

1. ***SPN Scanning*** *– finding services by requesting service principal names of a specific SPN class/type.*
2. ***Silver Ticket*** *– forged Kerberos TGS service ticket*
3. ***Golden Ticket*** *– forged Kerberos TGT authentication ticket*
4. ***MS14–068 Forged PAC Exploit*** *– exploitation of the Kerberos vulnerability on Domain Controllers.*

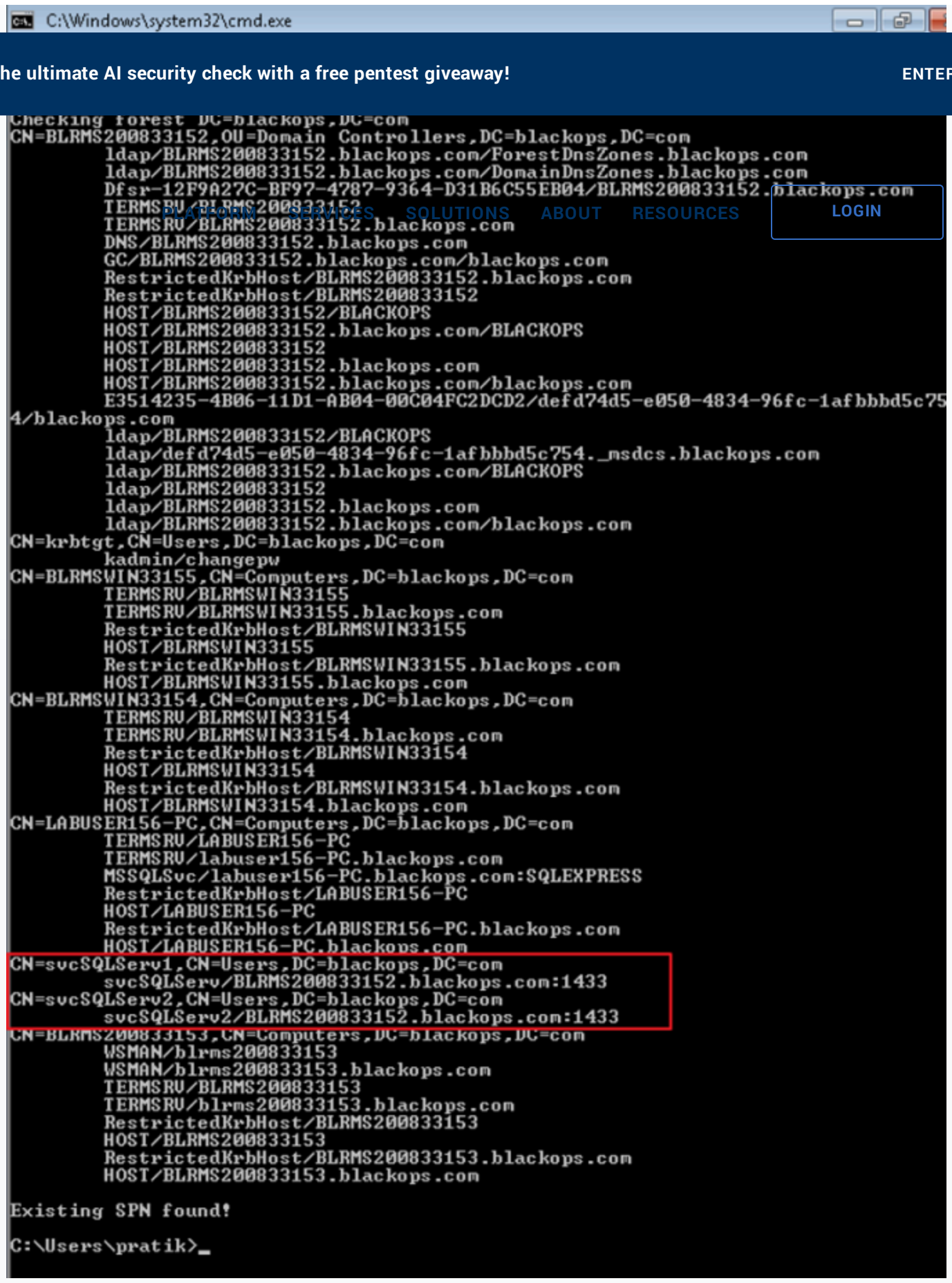
Now, let's see how we can leverage the Kerberos implementation to our advantage.

Old Technique

We will see and understand the old technique first (i.e. SPN Scanning and then cracking the tickets).

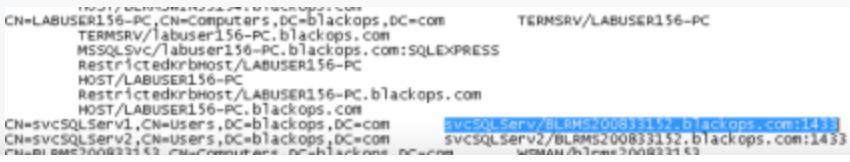
In general, we follow the process below:

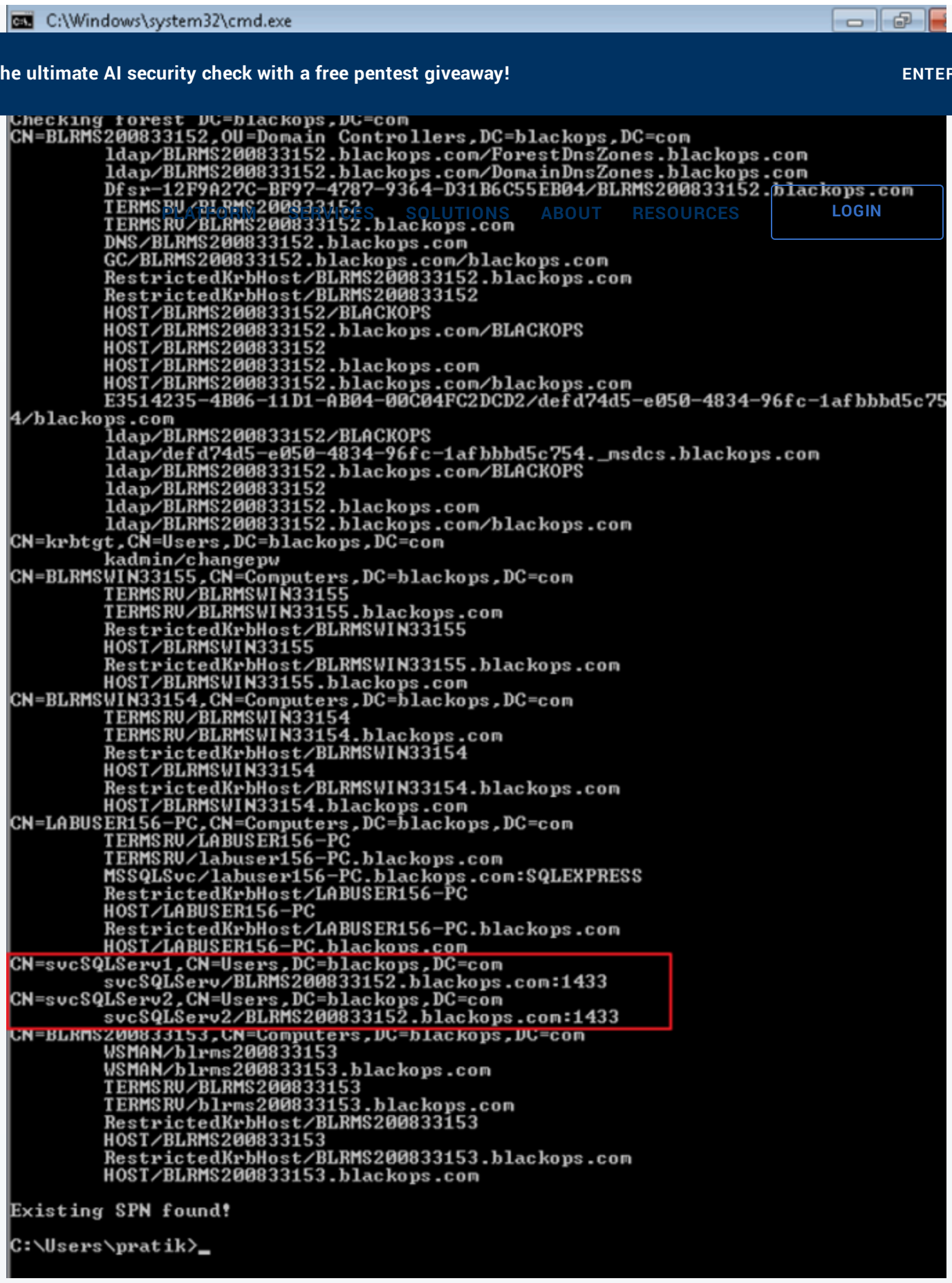
- Enumerate the domain accounts with SPNs set- either with GetUserSPNS.ps1 script from PowerView's or Impacket's "GetUserSPN.py".
- Request TGSs for these specific SPNs with the built-in Windows tool setspn.exe.
- Extract these tickets from memory by invoking the kerberos::list /export Mimikatz command, with the optional base64 export format set first. The tickets were then downloaded, or the



"setspn.exe" output

Now, if you notice we have "CN= Computers" and "CN=Users" for listed service accounts. We will be focusing on "CN=Users" as these are user generated and so we can try to crack :).





Powershell Command (Non Admin User)

Now, we have tickets in memory. We will use Mimikatz to export the tickets from memory. This is one of the down side of this method as you are running Mimikatz this might trigger Alert or this can be detected by AV's.

Note: You can also load Mimikatz into memory using PowerShell "IEX (New-Object Net.WebClient).DownloadString" feature)

We have successfully extracted the tickets from memory. Can we crack these tickets?? There are

1 > Using Kerberosast: Tgsrepcrack.py

We have provided the wordlist to crack the kirbi file

Command: *C:\Users\pratik\Desktop\kerberoast>python tgsrepcrack.py dict.txt "Ticket.kirbi"*

Cracked Ticket

:) Cracked

2> Convert .kirbi file to John the Ripper format

Now, we will use John the Ripper to crack the tickets. We know that tickets are in kirbi format so first we will convert the ticket to John the Ripper format. We can use Kerberoast (kirbi2john.py) for the same.

John the Ripper format

Command: *./john –format=krb5tgs crack_file – wordlist=dict.txt*

Cracked using John the Ripper

Cracked :)

New Technique

HarmJ0y has written a good blog on kerberoasting without Mimikatz. This technique is pretty

Invoke-Kerberoast

Crack the tickets using John the Ripper

Cracked using John the Ripper

Back to Blog

Blog

A Pentester's Guide to Code Injection

READ MORE

Blog

4 Simple Steps to Protect Your Organization from Ransomware Attacks

READ MORE

Blog

Dangers of Ransomware File-Sharing Software

READ MORE

Cobalt

PLATFORM SERVICES SOLUTIONS ABOUT RESOURCES BLOG GET STARTED

SEE MORE

Never miss a story

Stay updated about Cobalt news as it happens

YOUR EMAIL*

I agree that the data I provide can be used to send me updates in the form of a newsletter. More details in our privacy policy.

SUBMIT

Cobalt

SCHEDULE A DEMO CONTACT

PLATFORM
- Cobalt Platform
- Offensive Security PtaaS
- Pricing

SERVICES
- Application Security
- Application Pentest
- Network Security
- Cloud Security
- Brand Protection
- Device Security

COMPANY
- About
- Leadership
- Core Community
- Careers
- Partners

HELPFUL LINKS
- Product Documentation
- Resource Library
- Blog
- Events & Webinars
- Vulnerability Wiki
- Trust Center