nviso

“This is fine”

Red Team edition

Firat Acar

July 2023

whoami

Firat Acar

Senior Red Teamer

firat.acar@nviso.eu

https://ares.nviso.eu

Red Team vs Pentest

What is the difference?

Red Team vs Pentest

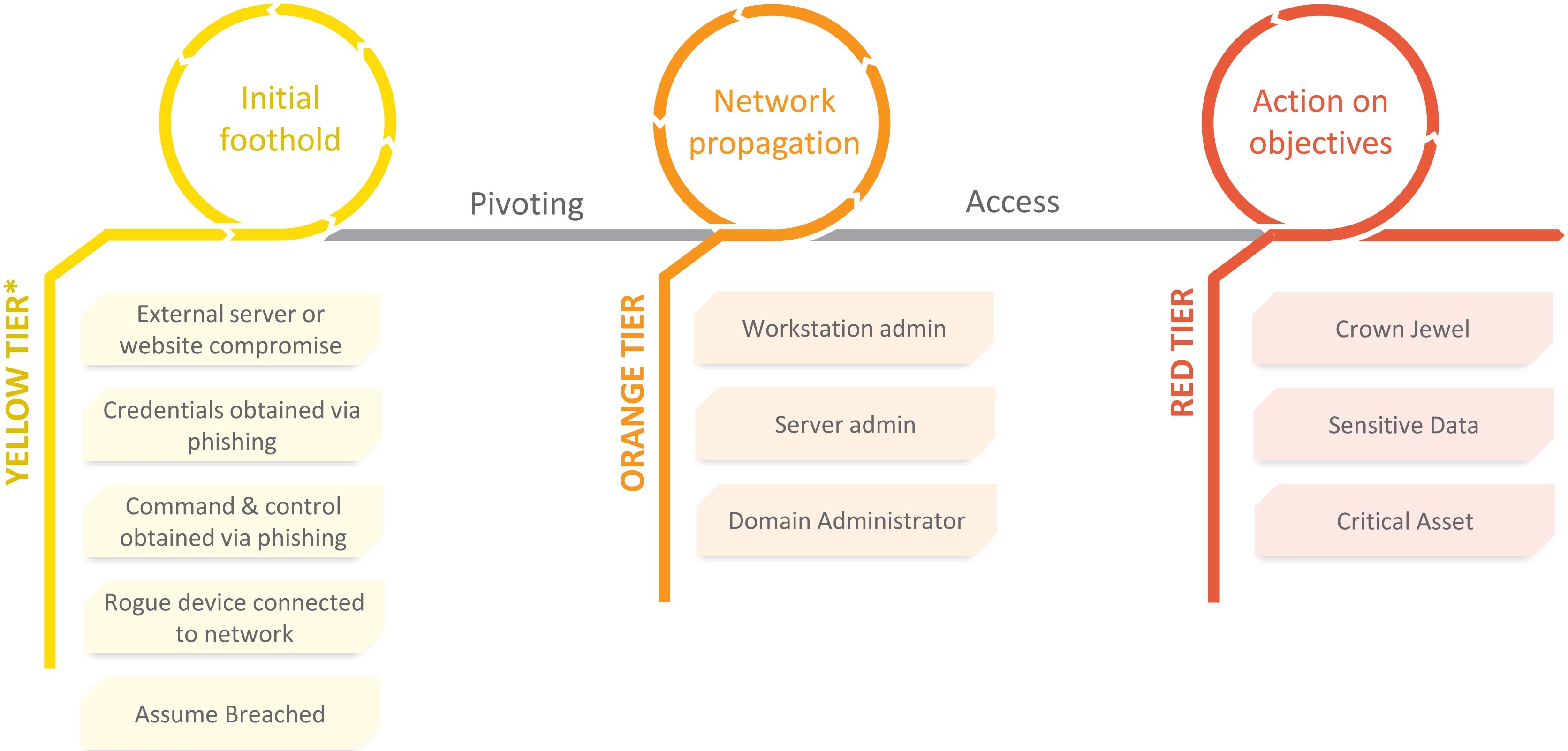
Security testing of different technologies / applications, e.g. Web, Mobile, WIFI, Cloud, Internal / External Network

Attack simulation against a company with objectives, stealth, wide scope (including people), phishing, physical breach

Red Team – Similar exercises

	Objective-based Penetration Test	Red Team & TIBER	Purple Team Exercise
EXECUTION	**External** & **internal** focused on **technology**	Simulation of a **realistic attack** based on adversary TTPs along a **kill chain**	Execution of **selected TTPs**, possibly based on attack scenarios and/or along a kill chain
GOAL	**Assess resilience** in terms of **technology**	Assess **people, processes, technology** in terms of **prevention, detection & response**	**Improve detection**
STEALTH	None	Yes	None, cooperation with blue team
OUTCOME	Identify & fix low-hanging fruit Get a **baseline** in technical security	Determine the **impact of a realistic attack** and identify **improvement areas**	**Improved logging** and **detection** of selected use cases & TTPs

Red Team – Unified Kill Chain



Initial foothold

Pivoting

Network propagation

Access

Action on objectives

YELLOW TIER*

- External server or website compromise
- Credentials obtained via phishing
- Command & control obtained via phishing
- Rogue device connected to network
- Assume Breached

ORANGE TIER

- Workstation admin
- Server admin
- Domain Administrator

RED TIER

- Crown Jewel
- Sensitive Data
- Critical Asset

Red Team – Who is Who?

- Executes an attack scenario
- Has to find their way in, either via physical or cyber intrusion
- Tries to reach one or more objectives
- They attempt to operate stealthily

- Fully aware of the operation
- Involved in all planning
- Connection between Red and Blue Team
- Frequent and direct communication with Red Team
- Vital role for risk mitigation
- Act as if they are unaware of the ongoing red team assessment when blue team raises an incident (eventually informing them)

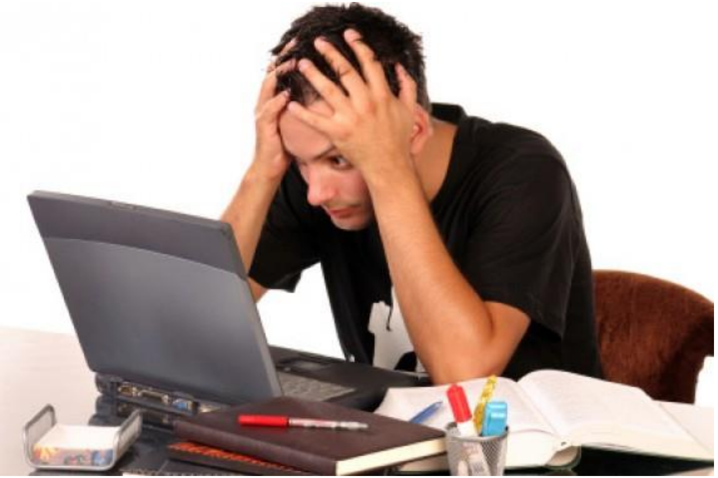
- Usually not (fully) aware of the attack
- Supposed to treat incidents as real and investigate
- Make the Red Teamer‘s life difficult

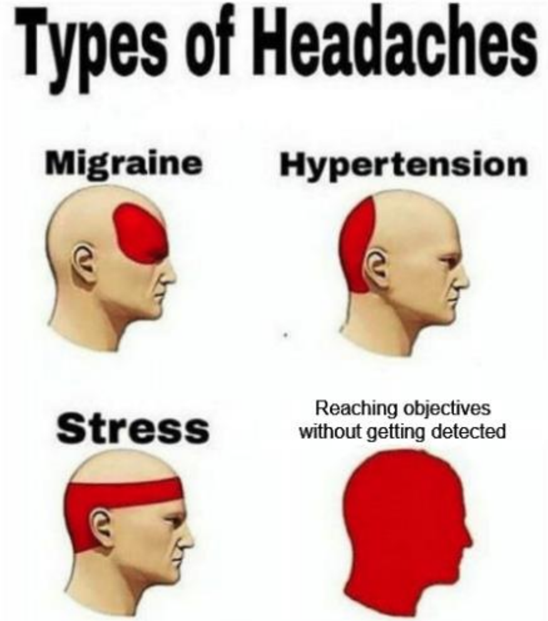
Stories

Tool Trial

Stories – Tool Trial

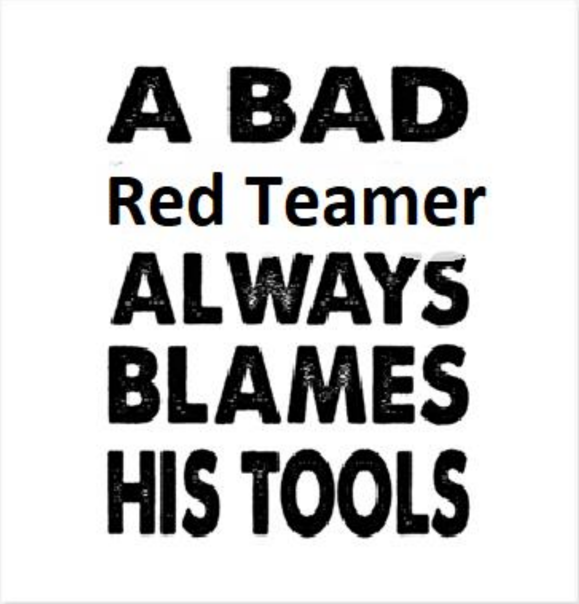
High stakes, stressful red team, already detected once





Stories – Tool Trial

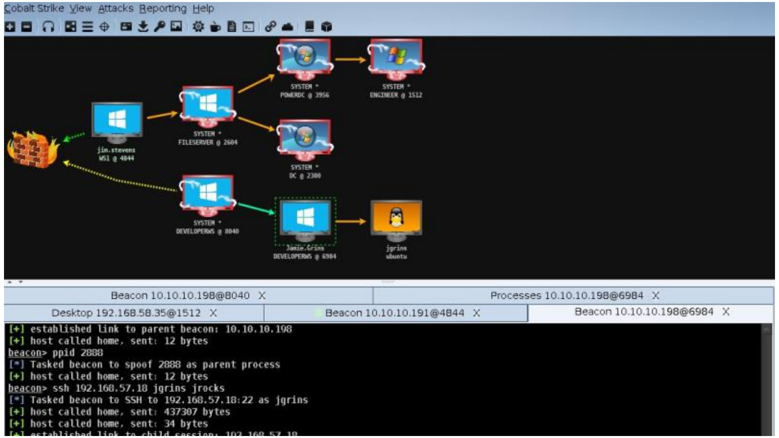
A good toolset is VERY important to red teamers!



A BAD
Red Teamer
ALWAYS
BLAMES
HIS TOOLS

Stories – Tool Trial

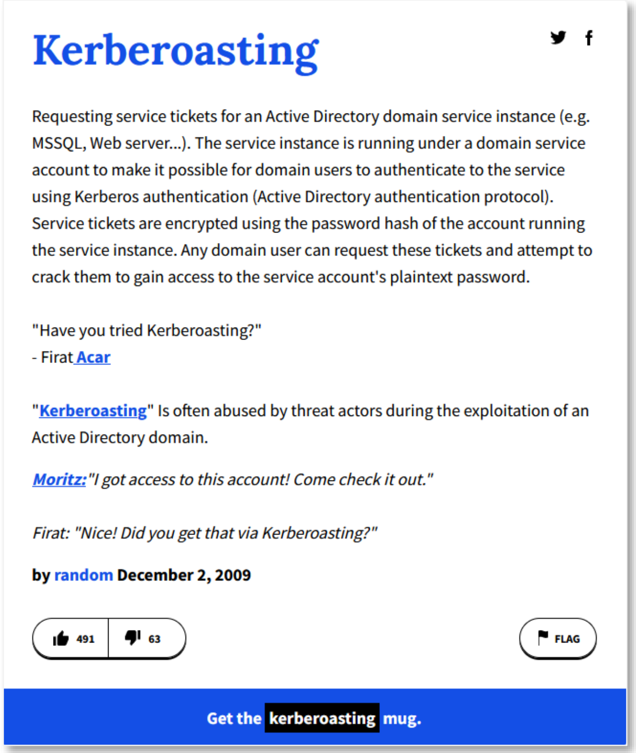
Cobalt Strike is a command-and-control framework commonly used by threat actors.



```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18
```

Beacon Object Files (BOFs) are the current hype and very useful during red teaming.

Stories – Tool Trial



Kerberoasting

Requesting service tickets for an Active Directory domain service instance (e.g. MSSQL, Web server...). The service instance is running under a domain service account to make it possible for domain users to authenticate to the service using Kerberos authentication (Active Directory authentication protocol). Service tickets are encrypted using the password hash of the account running the service instance. Any domain user can request these tickets and attempt to crack them to gain access to the service account's plaintext password.

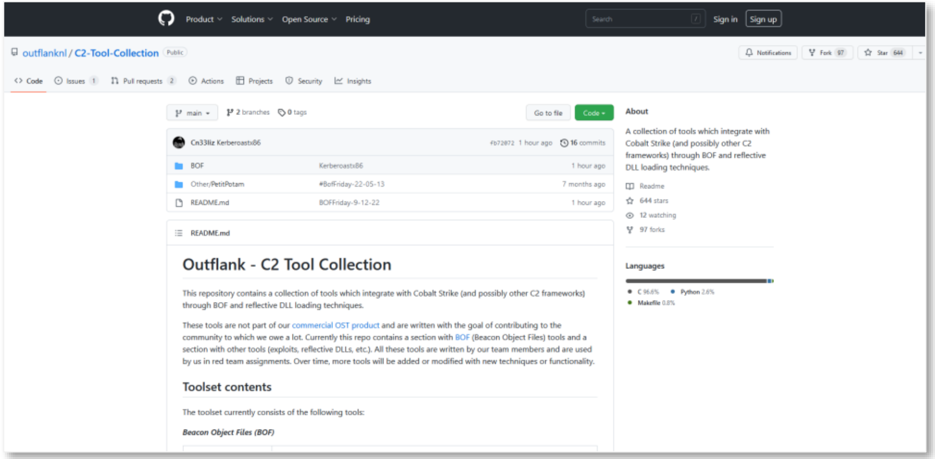
"Have you tried Kerberoasting?"
- Firat Acar

"Kerberoasting" Is often abused by threat actors during the exploitation of an Active Directory domain.

Moritz: "I got access to this account! Come check it out."

Firat: "Nice! Did you get that via Kerberoasting?"

by random December 2, 2009



Cn33liz Kerberoastx86	fb72872 1 hour ago	16 commits
BOF	Kerberoastx86	1 hour ago
Other/PetitPotam	#BofFriday-22-05-13	7 months ago
README.md	BOFFriday-9-12-22	1 hour ago

README.md

Outflank - C2 Tool Collection

This repository contains a collection of tools which integrate with Cobalt Strike (and possibly other C2 frameworks) through BOF and reflective DLL loading techniques.

These tools are not part of our commercial OST product and are written with the goal of contributing to the community to which we owe a lot. Currently this repo contains a section with BOF (Beacon Object Files) tools and a section with other tools (exploits, reflective DLLs, etc.). All these tools are written by our team members and are used by us in red team assignments. Over time, more tools will be added or modified with new techniques or functionality.

Toolset contents

The toolset currently consists of the following tools:

Beacon Object Files (BOF)

About

A collection of tools which integrate with Cobalt Strike (and possibly other C2 frameworks) through BOF and reflective DLL loading techniques.

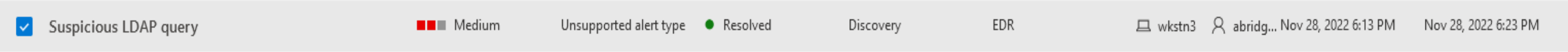
https://github.com/outflanknl/C2-Tool-Collection/tree/main/BOF/Kerberoast

Stories – Tool Trial

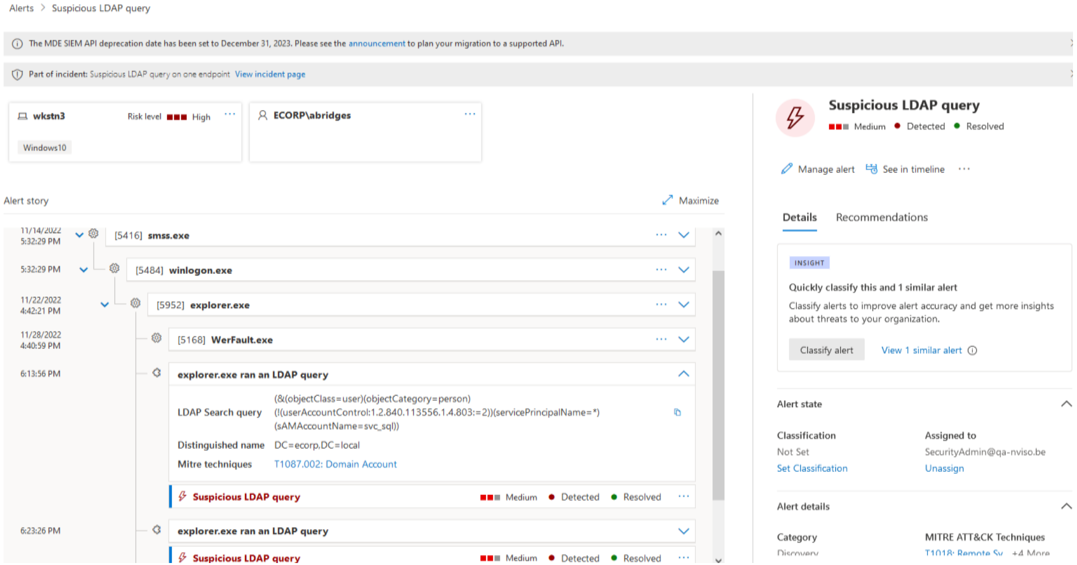
Suspicious LDAP queries commonly used to find Kerberoastable targets:

```
(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2))(service
PrincipalName=*)(sAMAccountName=*))
```

```
(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2))(service
PrincipalName=*)(sAMAccountName=svc_sql))
```



☑ Suspicious LDAP query | ■■■ Medium | Unsupported alert type | ● Resolved | Discovery | EDR | wkstn3 | abridg... | Nov 28, 2022 6:13 PM | Nov 28, 2022 6:23 PM



Alerts > Suspicious LDAP query

ⓘ The MDE SIEM API deprecation date has been set to December 31, 2023. Please see the announcement to plan your migration to a supported API.

Part of incident: Suspicious LDAP query on one endpoint View incident page

wkstn3 Risk level ■■■ High
Windows10

ECORP\abridges

Alert story

11/14/2022 5:32:29 PM	[5416] smss.exe
5:32:29 PM	[5484] winlogon.exe
11/22/2022 4:42:21 PM	[5952] explorer.exe
11/28/2022 4:40:59 PM	[5168] WerFault.exe
6:13:56 PM	explorer.exe ran an LDAP query

LDAP Search query: (&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2))(servicePrincipalName=*)(sAMAccountName=svc_sql))

Distinguished name: DC=ecorp,DC=local

Mitre techniques: T1087.002: Domain Account

Suspicious LDAP query ■■■ Medium ● Detected ● Resolved

6:23:26 PM explorer.exe ran an LDAP query

Suspicious LDAP query ■■■ Medium ● Detected ● Resolved

Suspicious LDAP query

■■■ Medium ● Detected ● Resolved

INSIGHT

Quickly classify this and 1 similar alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Alert state

Classification: Not Set
Set Classification

Assigned to: SecurityAdmin@qa-nviso.be
Unassign

Alert details

Category: Discovery

MITRE ATT&CK Techniques: T1018: Remote Sy... +4 More

Stories – Tool Trial

Me not testing my tools during a red team:

Stories

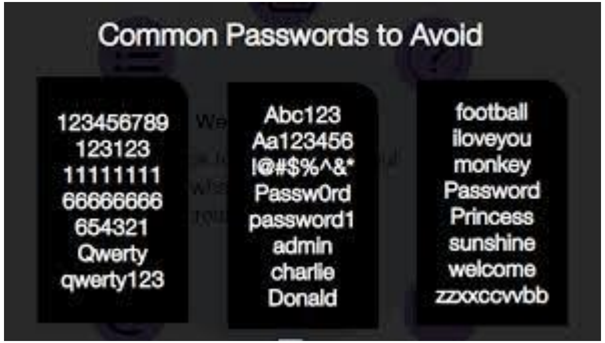
Credentials: How not to store them

Stories – Credentials: How not to store them

The age old debate of storing passwords, password managers vs sticky notes vs password reuse...

KeePass

Enpass



Common Passwords to Avoid

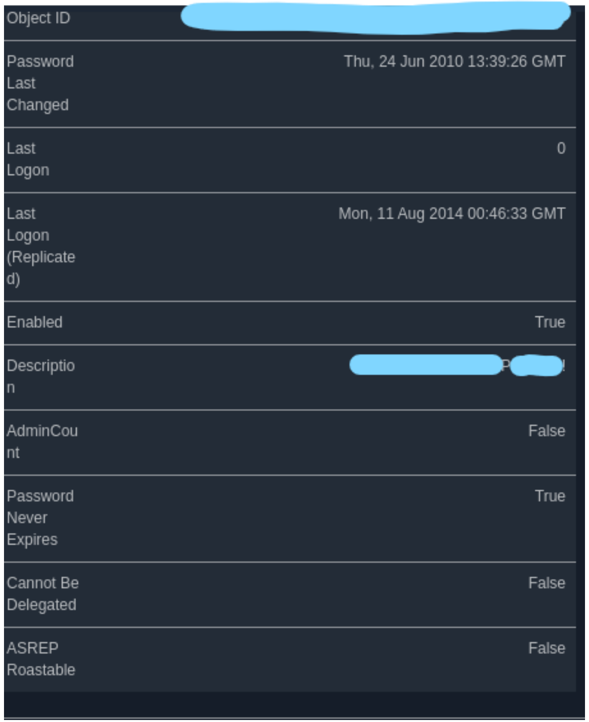
123456789
123123
11111111
66666666
654321
Qwerty
qwerty123

Abc123
Aa123456
!@#$%^&*
Passw0rd
password1
admin
charlie
Donald

football
iloveyou
monkey
Password
Princess
sunshine
welcome
zzxxccvvbb

Stories – Credentials: How not to store them

During the reporting phase of an assessment, I noticed something strange...

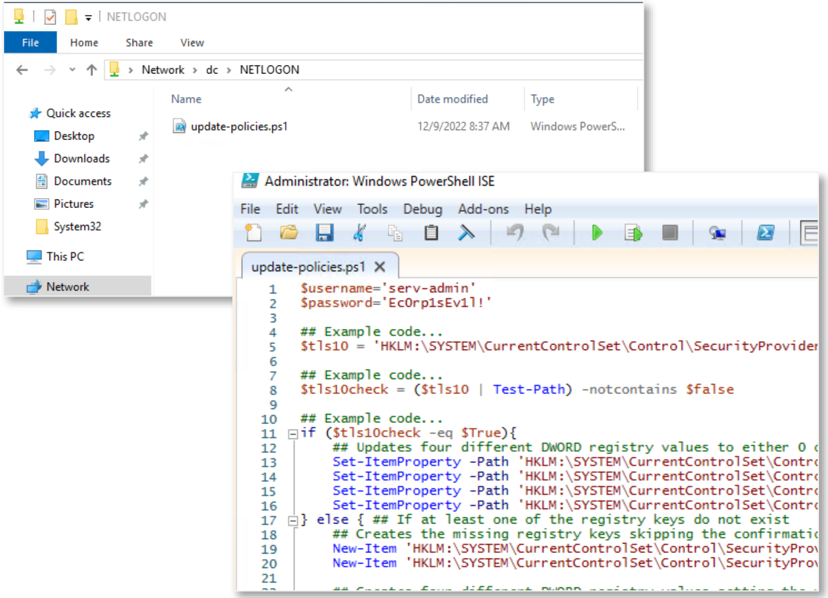


Object ID	[redacted]
Password Last Changed	Thu, 24 Jun 2010 13:39:26 GMT
Last Logon	0
Last Logon (Replicated)	Mon, 11 Aug 2014 00:46:33 GMT
Enabled	True
Description	[redacted]
AdminCount	False
Password Never Expires	True
Cannot Be Delegated	False
ASREP Roastable	False

Stories – Credentials: How not to store them

Sometimes it can be too good to be true...
and then it turns out that it was.

Not only honeypot users, also files!



Network › dc › NETLOGON

Name	Date modified	Type
update-policies.ps1	12/9/2022 8:37 AM	Windows PowerS...

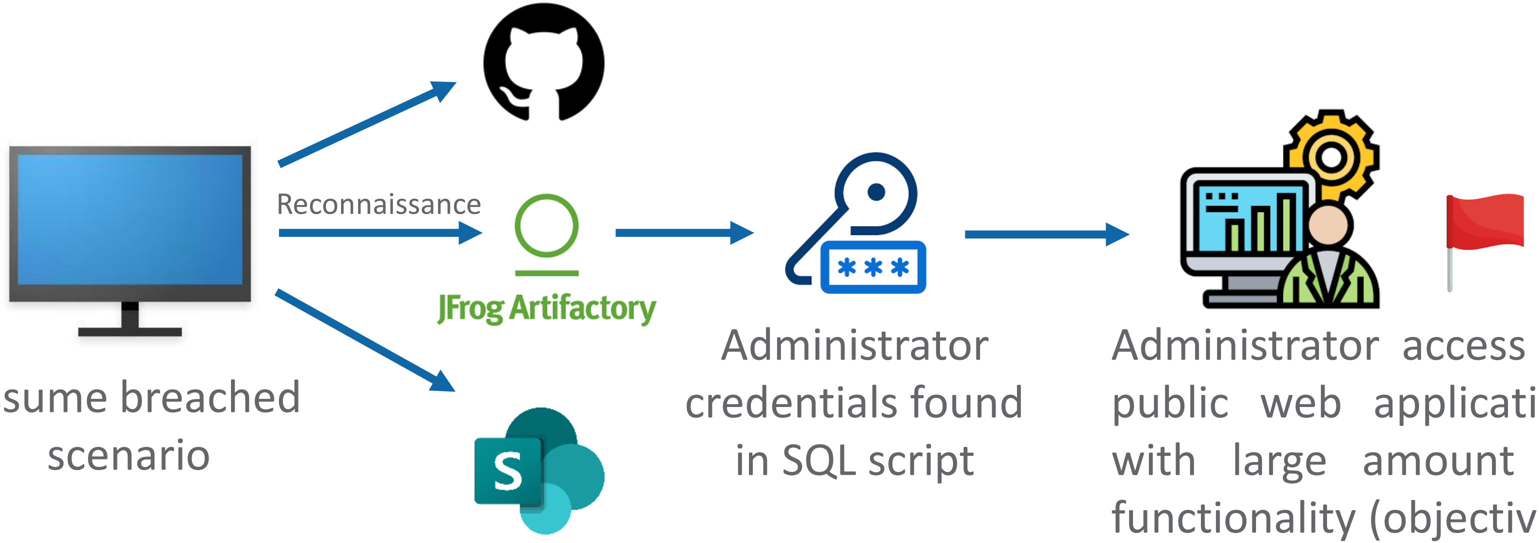
```
$username='serv-admin'
$password='Ec0rp1sEv1l!'

## Example code...
$tls10 = 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProvider

## Example code...
$tls10check = ($tls10 | Test-Path) -notcontains $false

## Example code...
if ($tls10check -eq $True){
    ## Updates four different DWORD registry values to either 0 o
    Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Contro
    Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Contro
    Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Contro
    Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Contro
} else { ## If at least one of the registry keys do not exist
    ## Creates the missing registry keys skipping the confirmatio
    New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProv
    New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProv

    ## Creates four different DWORD registry values setting the
```

Stories

Traversing the Forest: SQL Server Jumping

Stories – Traversing the Forest: SQL Server Jumping

Backstory...



Reconnaissance

JFrog Artifactory

Assume breached scenario

Administrator credentials found in SQL script

Administrator access to public web application with large amount of functionality (objective)

Stories – Traversing the Forest: SQL Server Jumping

Continue with new objectives, see where we can get via the web application.

Local file inclusion found, didn't lead to RCE

Found SQL Server administration page...

Stories – Traversing the Forest: SQL Server Jumping

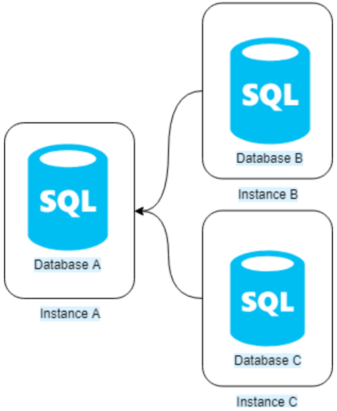
Access to SQL Server can provide a wide range of opportunities during red teaming, not only in terms of data breaches (privesc, local server access, lateral movement...)

Restriction: queries have to be in **select X from Y** format and no sysadmin privileges on local server

Stories – Traversing the Forest: SQL Server Jumping

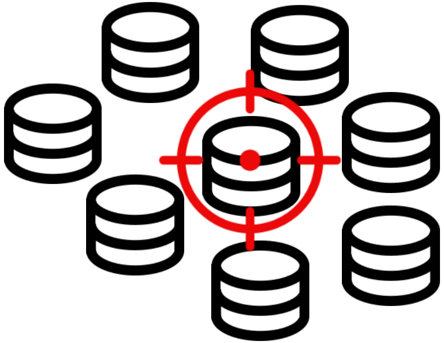
With no sysadmin role access to local server, we headed for linked servers

SELECT * FROM sys.servers;



70+ linked servers

Out of all linked servers, only **one** link was configured with sysadmin privileges



Stories – Traversing the Forest: SQL Server Jumping

Time to abuse linked SQL Servers via the web UI…

```
select * from openquery(“SQL76", 'sp_configure ''show advanced
options'', 1; RECONFIGURE;')

select * from openquery(“SQL76", 'sp_configure ''xp_cmdshell'', 1;
RECONFIGURE;')
```

Not that easy, restrictions still apply!
Need to find another way

Stories – Traversing the Forest: SQL Server Jumping

More recon on the web application provided a SQL batch query page, which provides a way to execute big queries without restrictions

After activating xp_cmdshell on the linked server, we could finally execute system commands via the web UI

```
Select * from openquery("SQL76",'exec
xp_cmdshell ''dir "c:\program files"'' with
result sets ( (a varchar(1000) ) )')
```

Stories – Traversing the Forest: SQL Server Jumping

Time to spawn a Cobalt Strike beacon, should be easy

except that we faced restrictions again

No internet access

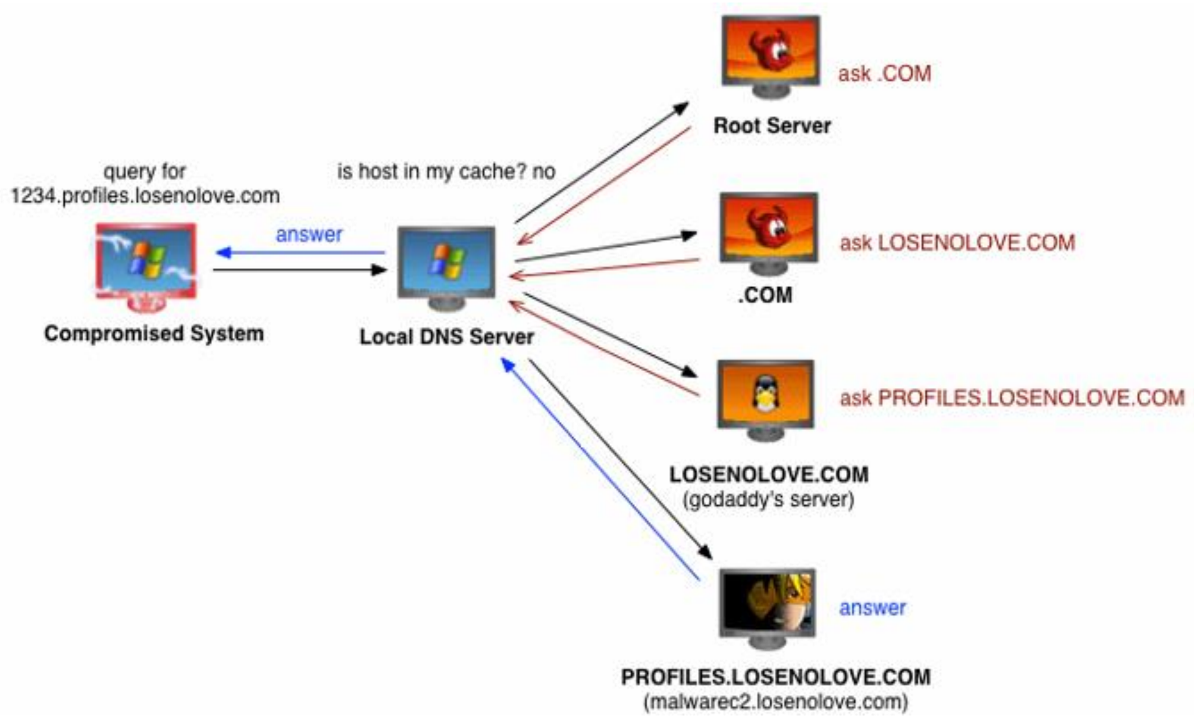
This time however, we were not entirely in the disadvantage!

No Antivirus

No EDR

Stories – Traversing the Forest: SQL Server Jumping

Despite the lack of internet, we could still communicate outbound via DNS



Pros: we get a beacon, which can communicate over DNS TXT records, DNS AAAA records, or DNS A records

Cons: quite slow, quite anomalous depending on traffic inspection

Stories – Traversing the Forest: SQL Server Jumping

One problem solved, but how do we actually get the beacon executable on the server

Techniques from back in the days: drop executables to disk using base64 encoding

Step by step:

1. Zip one or more executables
2. Base64 encode zip file via Powershell
3. Drop base64 encoded zip on linked server disk via following command:

```
echo|set /p="<base64>" >>
C:\Windows\Temp\bin_dmp.txt
```

4. Decode from base64 and unzip files on linked server disk
5. Execute binaries
6. Profit

Stories – Traversing the Forest: SQL Server Jumping

We finally got a DNS beacon running as SYSTEM in a new AD forest, eventually leading to owning the whole forest. (detected in the end)

Stories

Bring your own badge

Stories – Bring your own badge

Physical breach for multi-scenario red team

Mission: Reach highest floor of building and see if you can find interesting objects (workstations, (un)plugged network cables, documents, laptops...)

Stories – Bring your own badge

Threat intelligence briefing and equipment: what we know and what we have

Fake badge

Security guard absent after noon break

Tailgating is not possible

Stories – Bring your own badge

Two steps needed to accomplish the mission

Buy food, make hands look full

Act like you belong

Stories – Bring your own badge

It was time to go in...

Thank you!