Akamai

Off The Record: Weaponizing DHCP DNS Dynamic Updates

Ori David

black hat®

Agenda

- Unfamiliar attack surface in Active Directory
- Series of attacks allowing **DNS records overwrite without authentication**
- Mitigations

whoami

Ori David

Security Researcher at Akamai

Background in red teaming & threat hunting

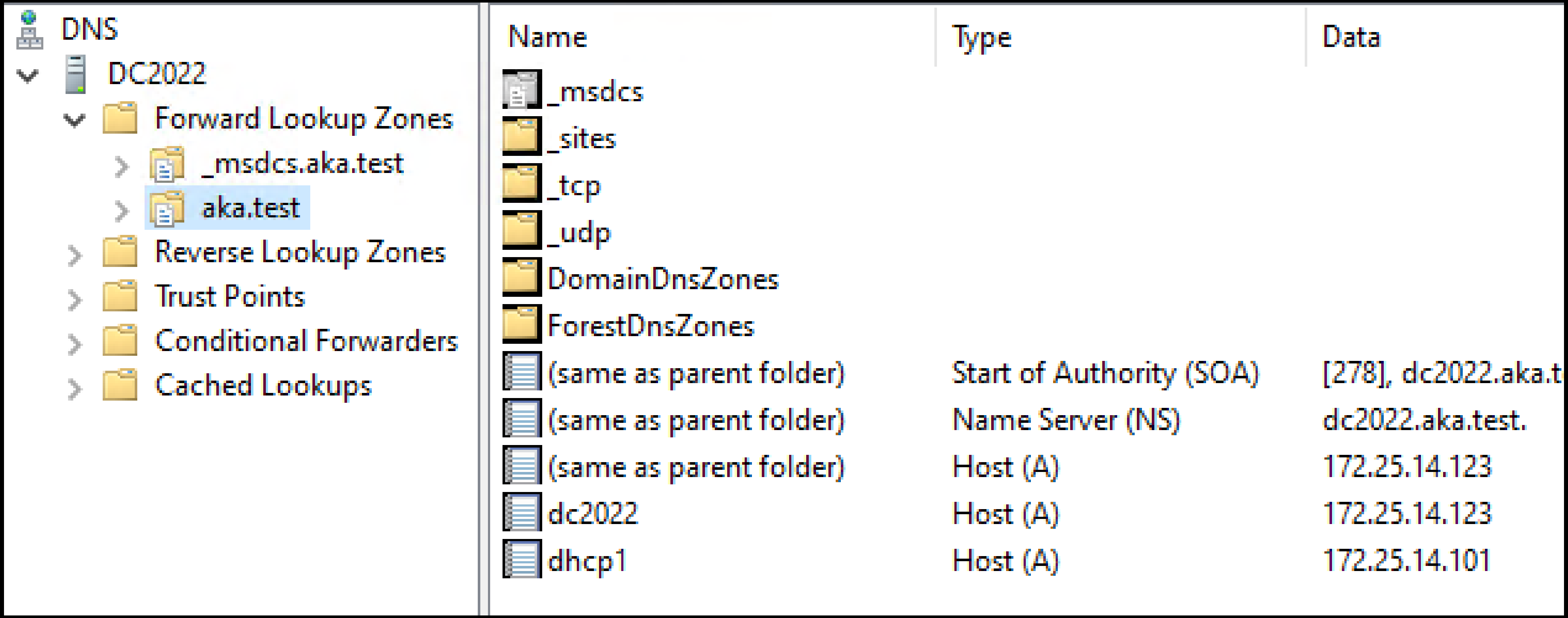
@oridavid123

It’s always DNS

- DNS exposes a lot of attack opportunities
  - DNS Spoofing
  - DNS Tunneling
  - DNS Amplification
  - …
- Decided to look at DNS in Active Directory domains

ADI DNS

Every domain requires an Active Directory Integrated DNS zone

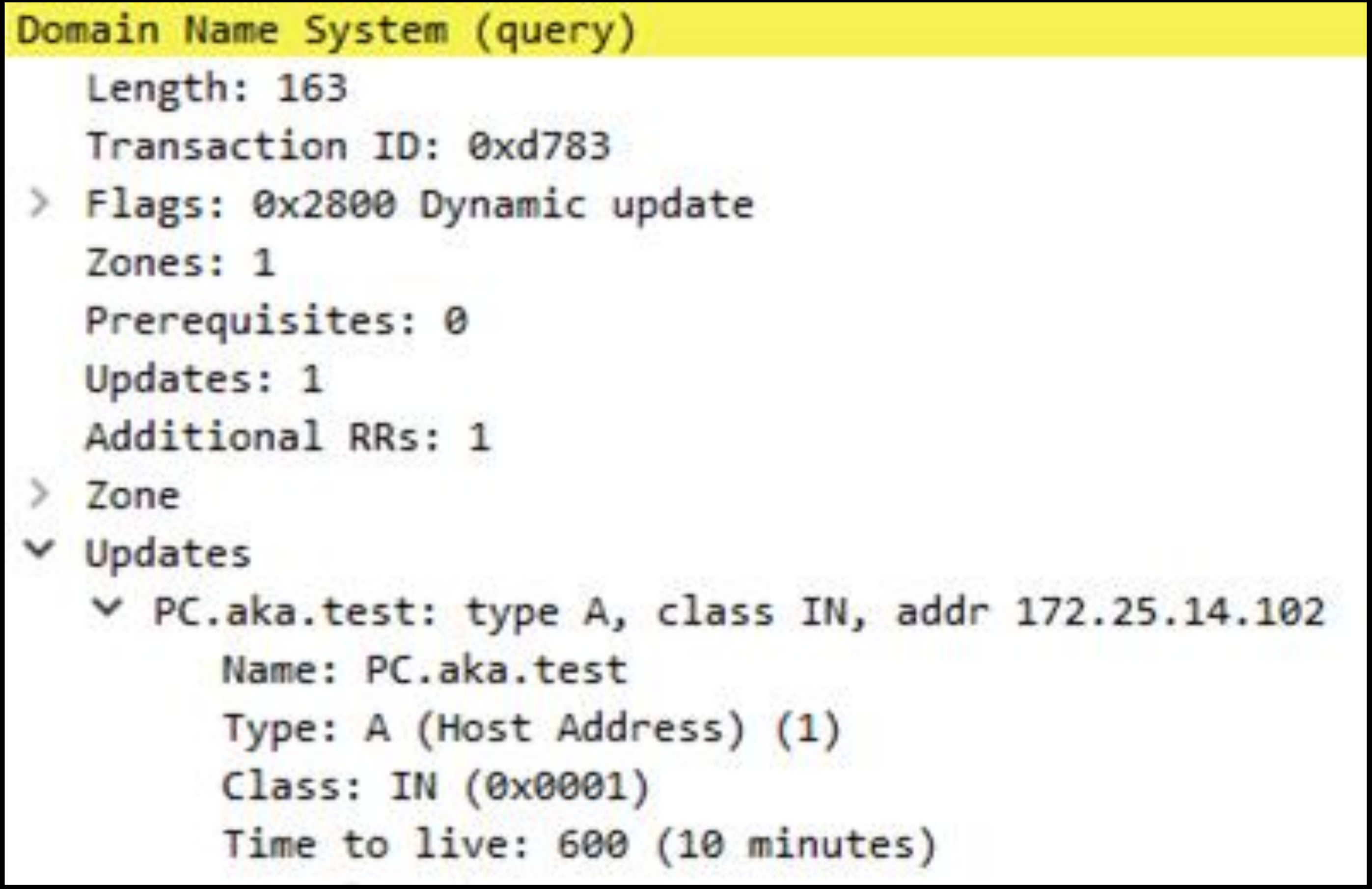


- DNS
  - DC2022
    - Forward Lookup Zones
      - _msdcs.aka.test
      - aka.test
    - Reverse Lookup Zones
    - Trust Points
    - Conditional Forwarders
    - Cached Lookups

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[278], dc2022.aka.t
(same as parent folder)	Name Server (NS)	dc2022.aka.test.
(same as parent folder)	Host (A)	172.25.14.123
dc2022	Host (A)	172.25.14.123
dhcp1	Host (A)	172.25.14.101

DNS Dynamic Updates

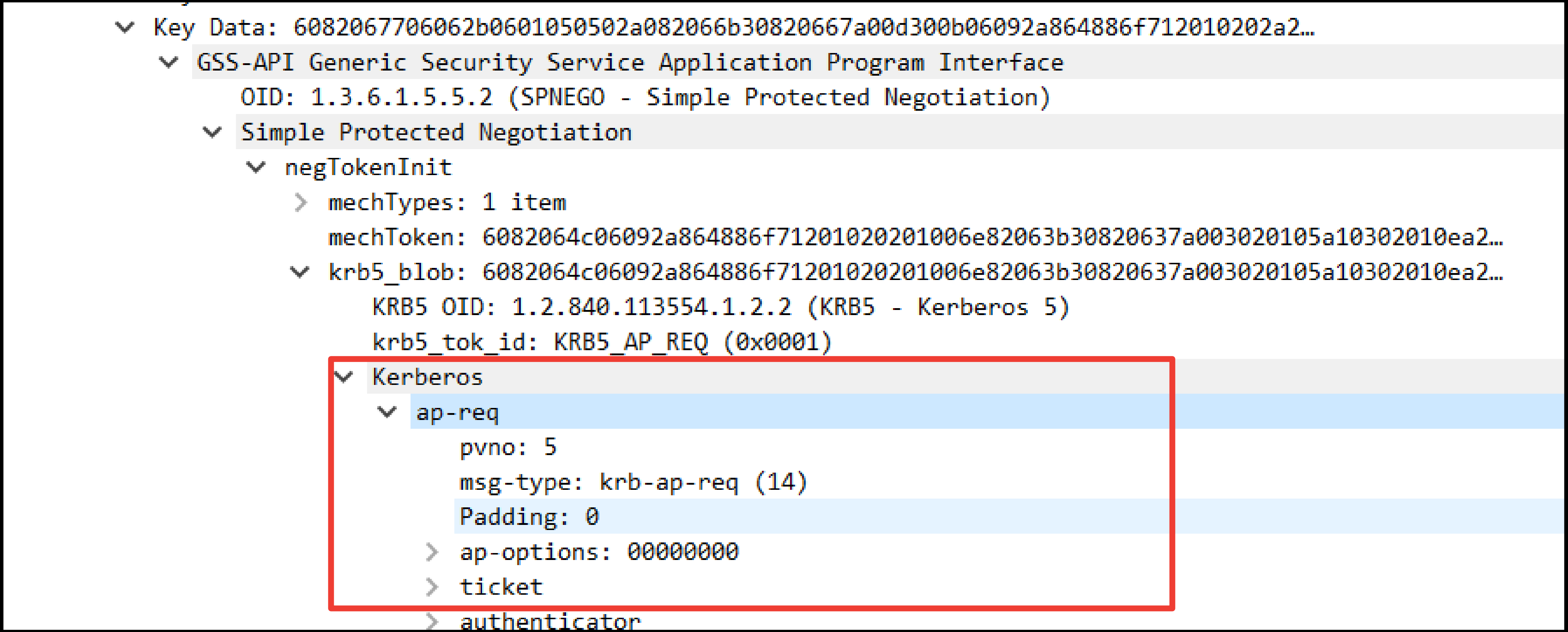
Every Windows host manages its own DNS record



```
Domain Name System (query)
    Length: 163
    Transaction ID: 0xd783
  > Flags: 0x2800 Dynamic update
    Zones: 1
    Prerequisites: 0
    Updates: 1
    Additional RRs: 1
  > Zone
  ˅ Updates
      ˅ PC.aka.test: type A, class IN, addr 172.25.14.102
            Name: PC.aka.test
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 600 (10 minutes)
```

Secure Dynamic Updates

By default, DNS updates are Kerberos authenticated



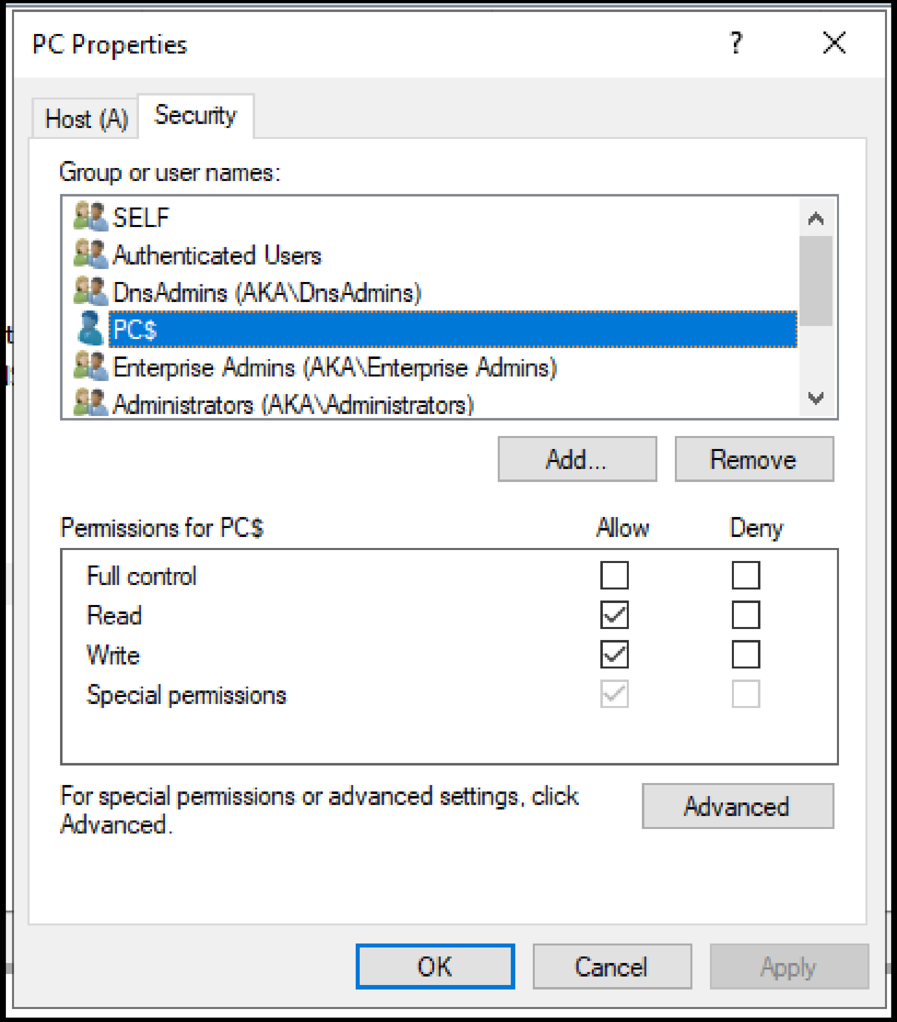
```
  Key Data: 6082067706062b0601050502a082066b30820667a00d300b06092a864886f712010202a2…
    GSS-API Generic Security Service Application Program Interface
      OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
      Simple Protected Negotiation
        negTokenInit
          mechTypes: 1 item
          mechToken: 6082064c06092a864886f71201020201006e82063b30820637a003020105a10302010ea2…
          krb5_blob: 6082064c06092a864886f71201020201006e82063b30820637a003020105a10302010ea2…
            KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
            krb5_tok_id: KRB5_AP_REQ (0x0001)
            Kerberos
              ap-req
                pvno: 5
                msg-type: krb-ap-req (14)
                Padding: 0
                ap-options: 00000000
                ticket
                authenticator
```

Secure Dynamic Updates

Updates are authorized based on ACLs

- Once created - every machine controls its own record

- Authenticated users can create records for non-existing names



PC Properties

Group or user names:

- SELF
- Authenticated Users
- DnsAdmins (AKA\DnsAdmins)
- PC$
- Enterprise Admins (AKA\Enterprise Admins)
- Administrators (AKA\Administrators)

Permissions for PC$	Allow	Deny
Full control	□	□
Read	☑	□
Write	☑	□
Special permissions	☑	□

For special permissions or advanced settings, click Advanced.

DHCP & DNS

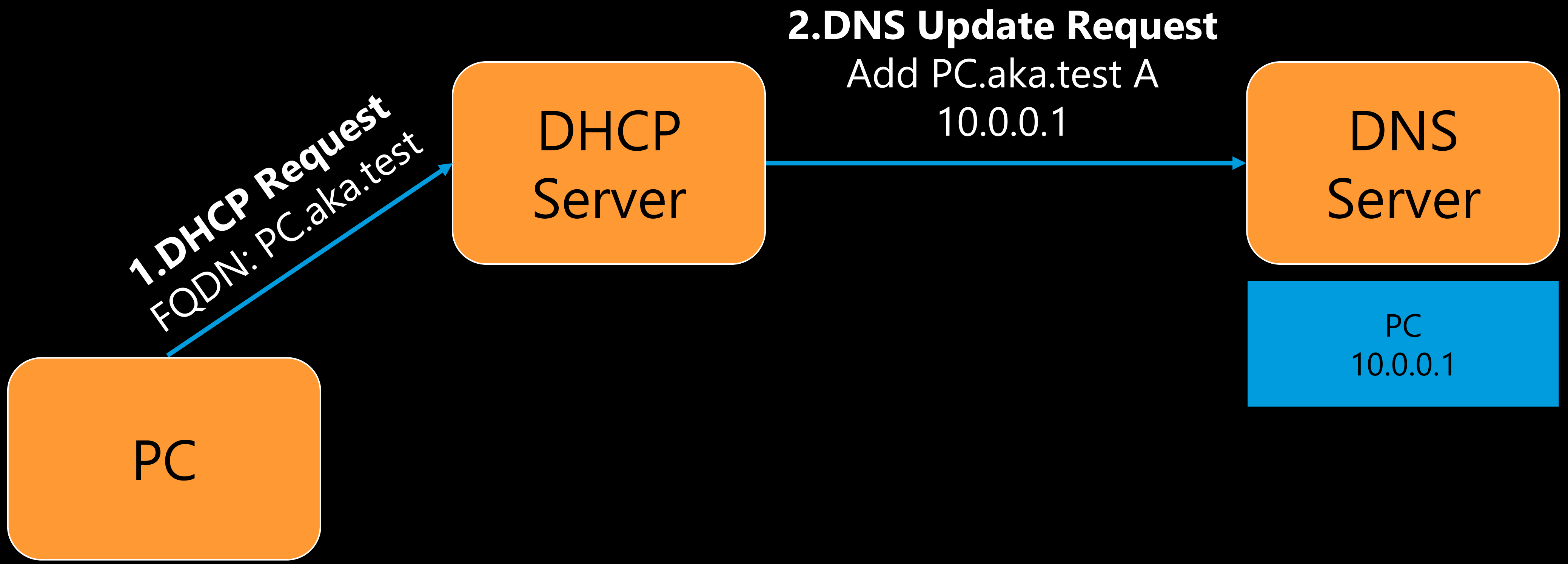
DHCP

provide a unique IP address and other network configuration for network clients

DHCP DNS Dynamic Update

DHCP feature to create a DNS record on behalf of DHCP clients

DHCP DNS Dynamic Update



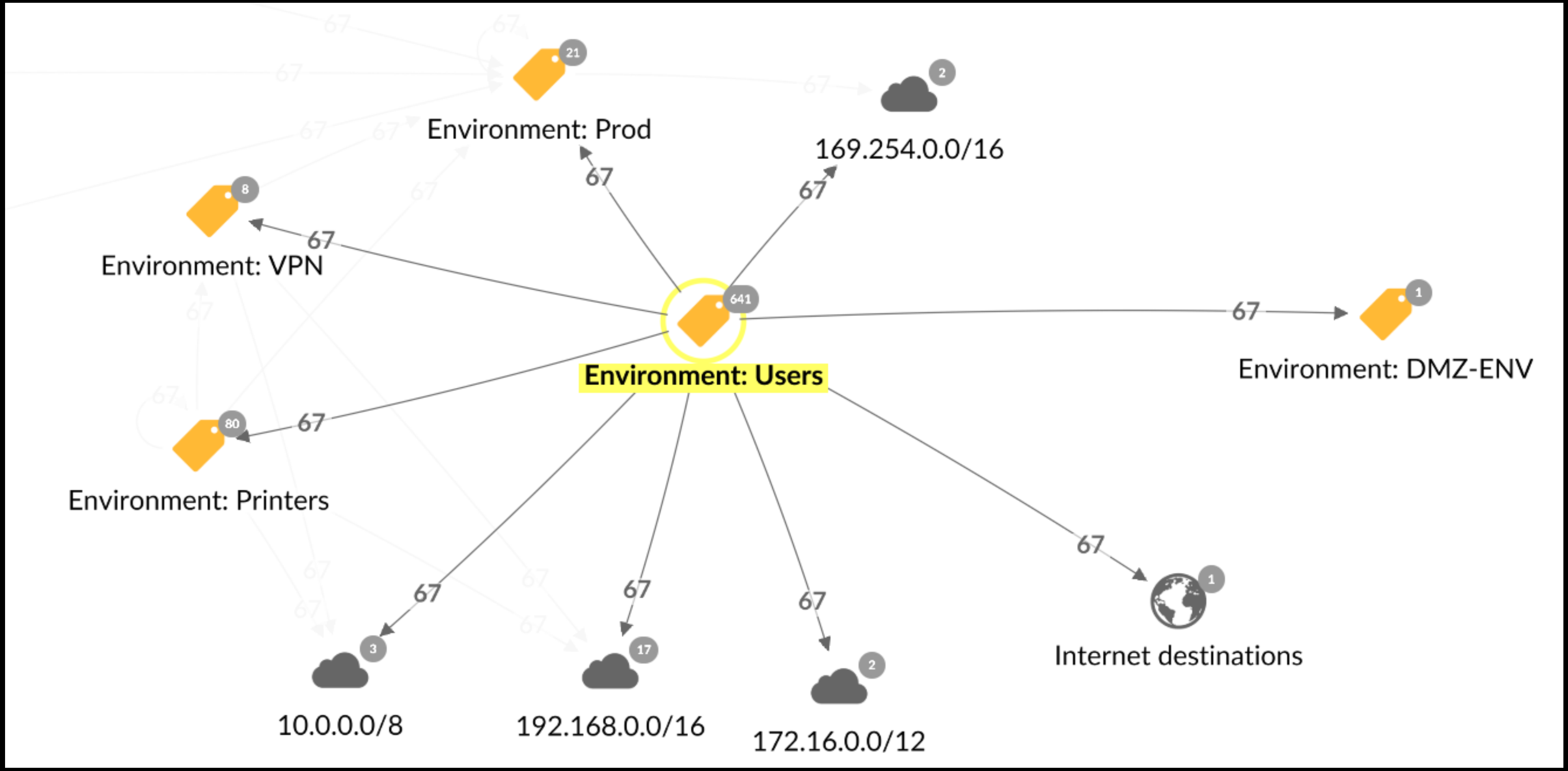
Performing Updates - Demo

DHCP DNS Dynamic Update Potential Impact

Unauthenticated	Bypass ADI-DNS authentication requirement - any client can lease an IP address from the DHCP server
Default	Enabled by default on Microsoft DHCP
Popular	Microsoft DHCP server is very common

Microsoft DHCP server

We saw Microsoft DHCP in 40% of the networks that we monitor

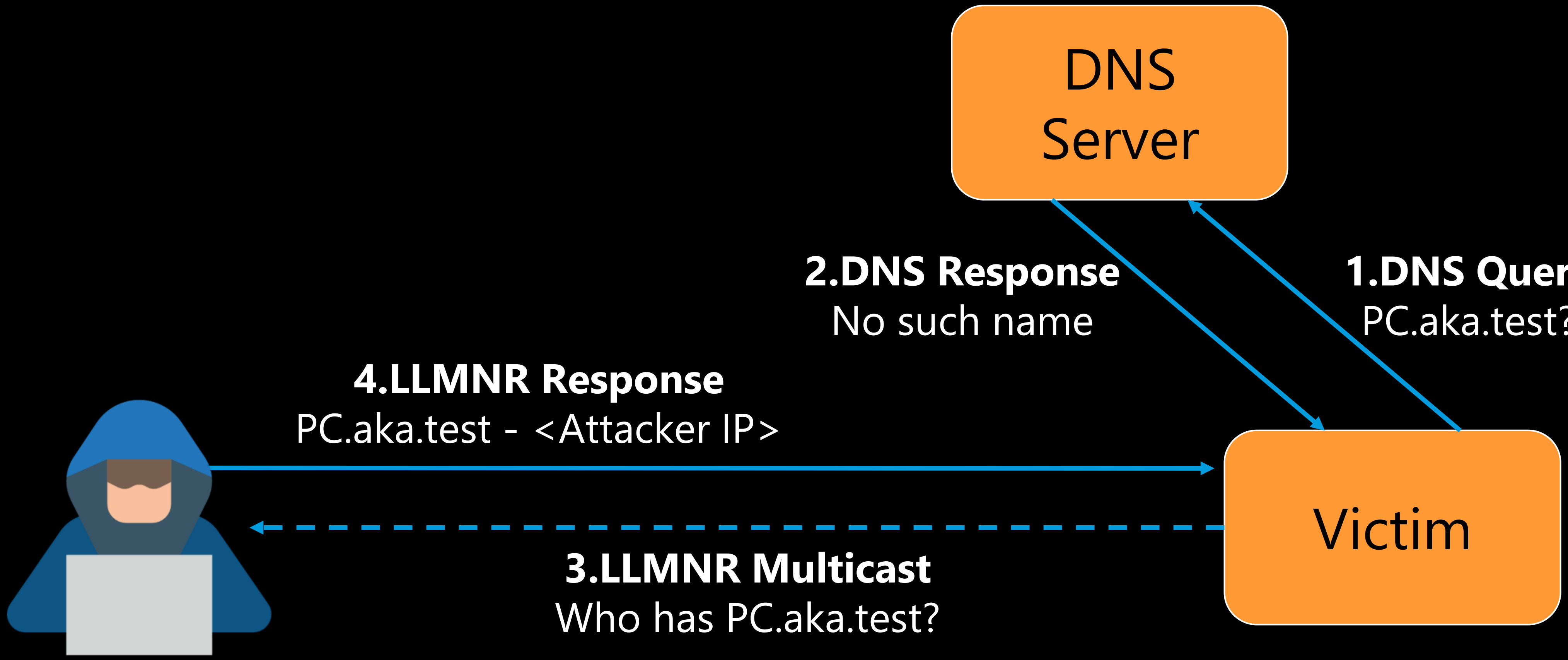


Abusing DHCP DNS Dynamic Updates

- How can we abuse the ability to create DNS records?

- Previous name resolution attacks:
  - LLMNR/NBNS Spoofing
  - ADI-DNS Spoofing

LLMNR/NBNS Spoofing



DNS Server

Victim

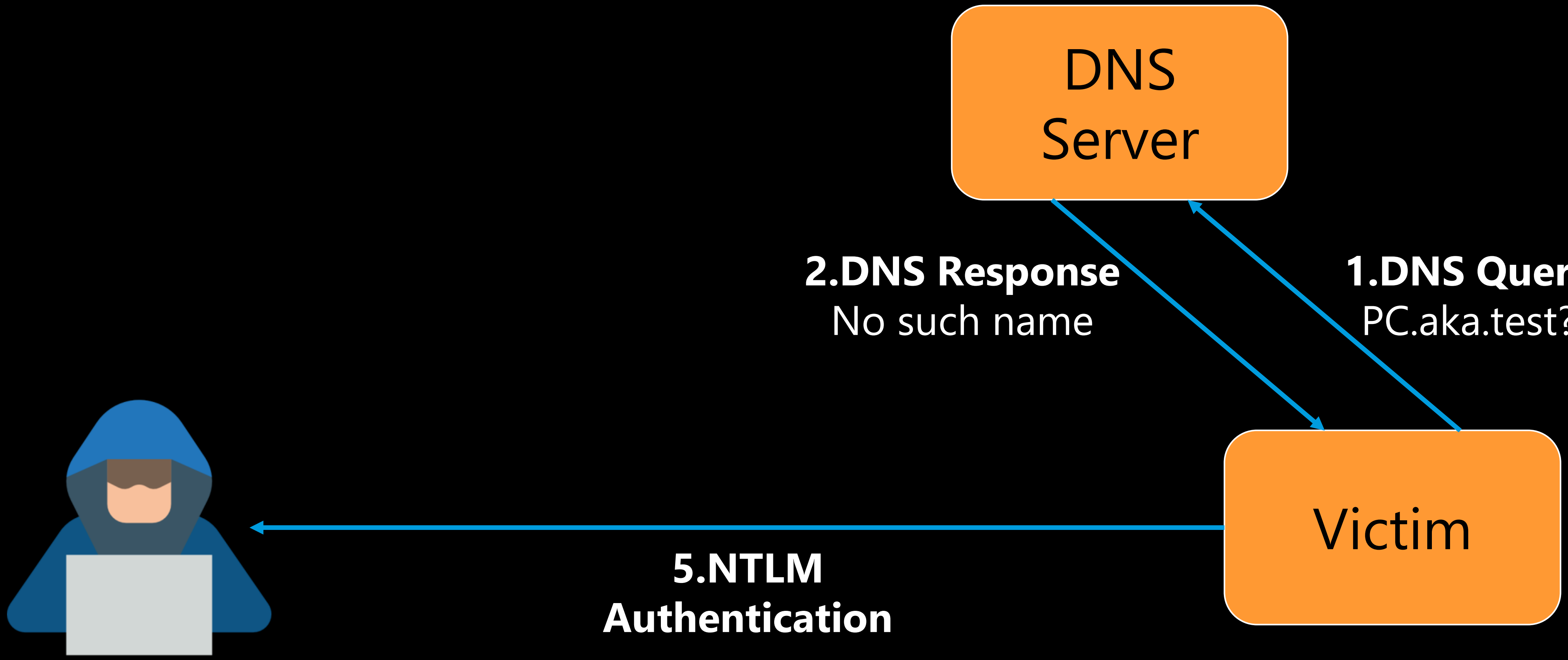
1.DNS Query
PC.aka.test?

2.DNS Response
No such name

3.LLMNR Multicast
Who has PC.aka.test?

4.LLMNR Response
PC.aka.test - <Attacker IP>

LLMNR/NBNS Spoofing



DNS Server

2.DNS Response
No such name

1.DNS Query
PC.aka.test?

Victim

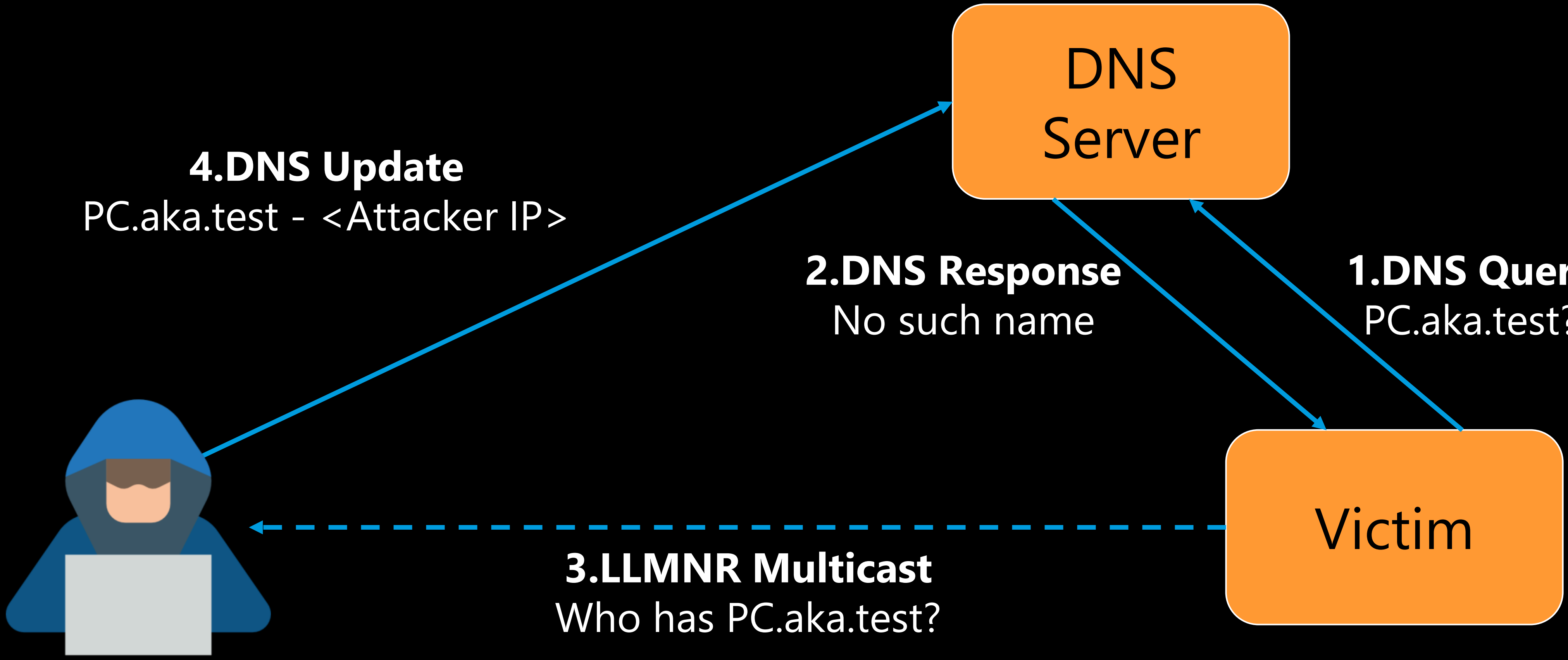
5.NTLM Authentication

LLMNR/NBNS Spoofing

✓ Doesn’t require authentication

✗ Only works against targets in the same LAN

ADI-DNS Spoofing



DNS Server

Victim

1.DNS Query
PC.aka.test?

2.DNS Response
No such name

3.LLMNR Multicast
Who has PC.aka.test?

4.DNS Update
PC.aka.test - <Attacker IP>

ADI-DNS Spoofing

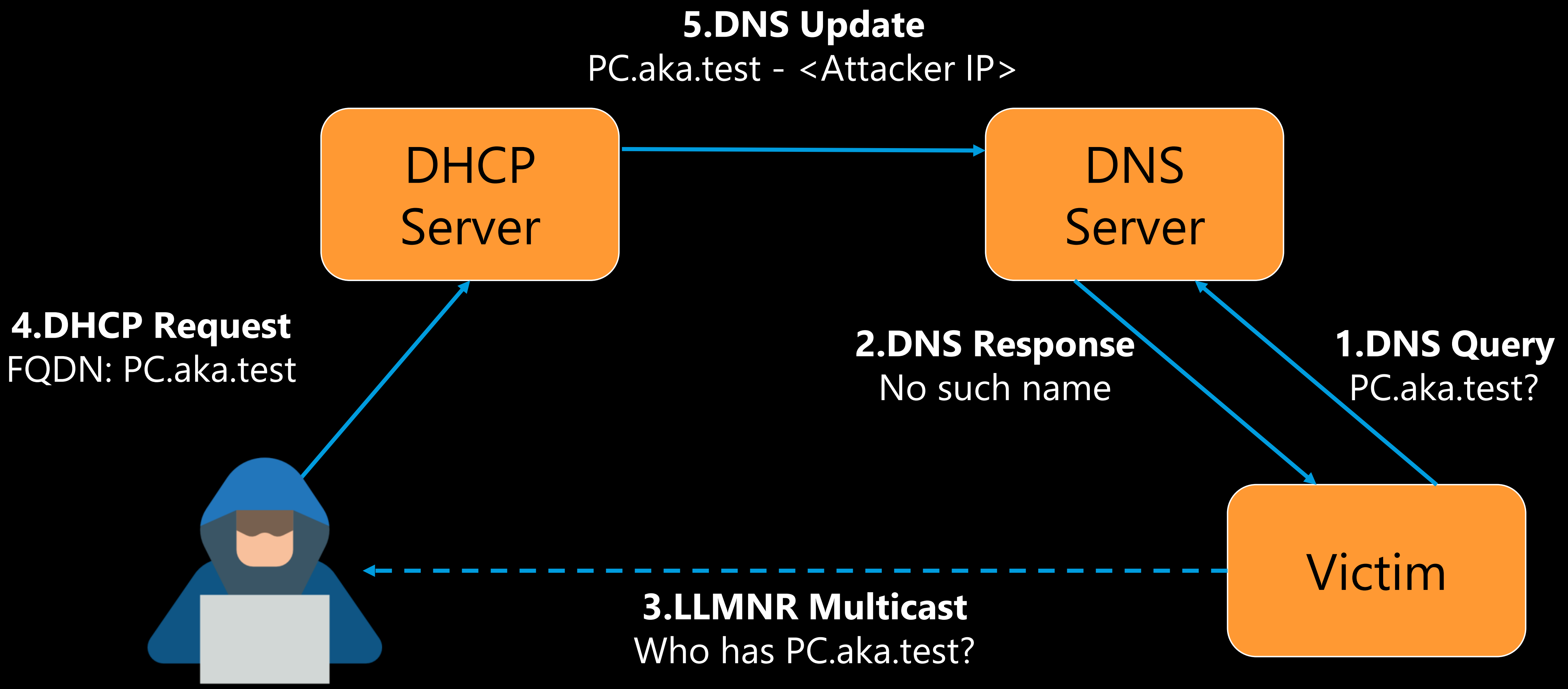
✓ Works against all targets in the domain

✗ Requires authentication

DDSpoofing

DHCP DNS Spoofing

DHCP DNS Spoofing

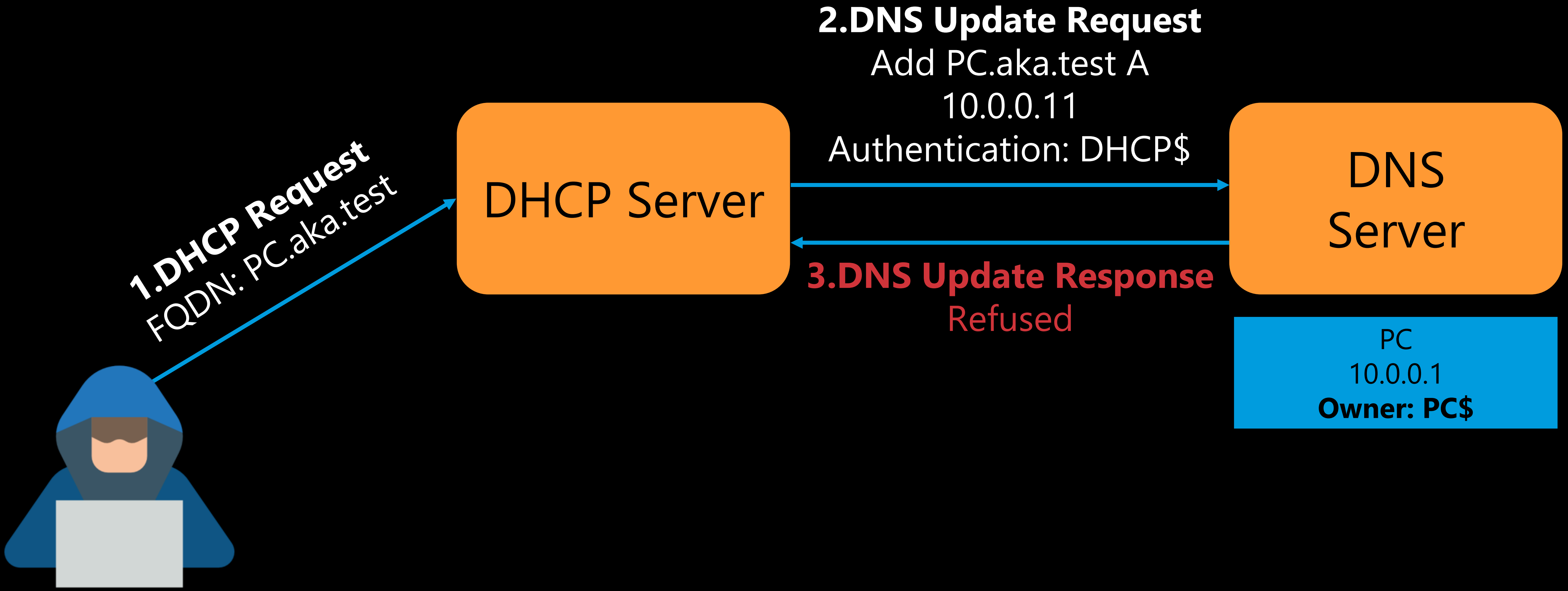


Comparing to existing attacks

Attack	Works Without Credentials	Works Across Subnets
LLMNR/NBNS Spoofing	✓	✗
ADI-DNS Spoofing	✗	✓
DHCP DNS Spoofing	✓	✓

Working Towards DNS Overwrites

Working Towards Overwrites



1.DHCP Request
FQDN: PC.aka.test

DHCP Server

2.DNS Update Request
Add PC.aka.test A
10.0.0.11
Authentication: DHCP$

DNS
Server

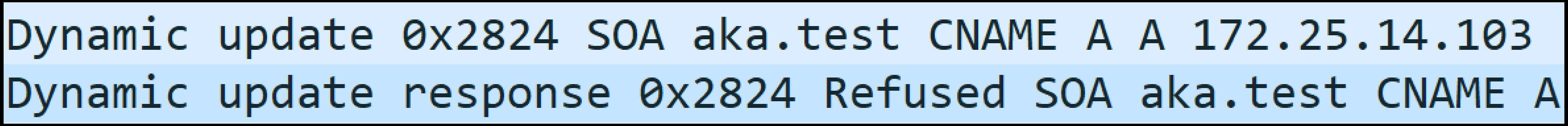
3.DNS Update Response
Refused

PC
10.0.0.1
Owner: PC$

Working Towards Overwrites

- The DHCP server will send a DNS Dynamic Update even if the record exists

- ACLs are meant to stop overwrites

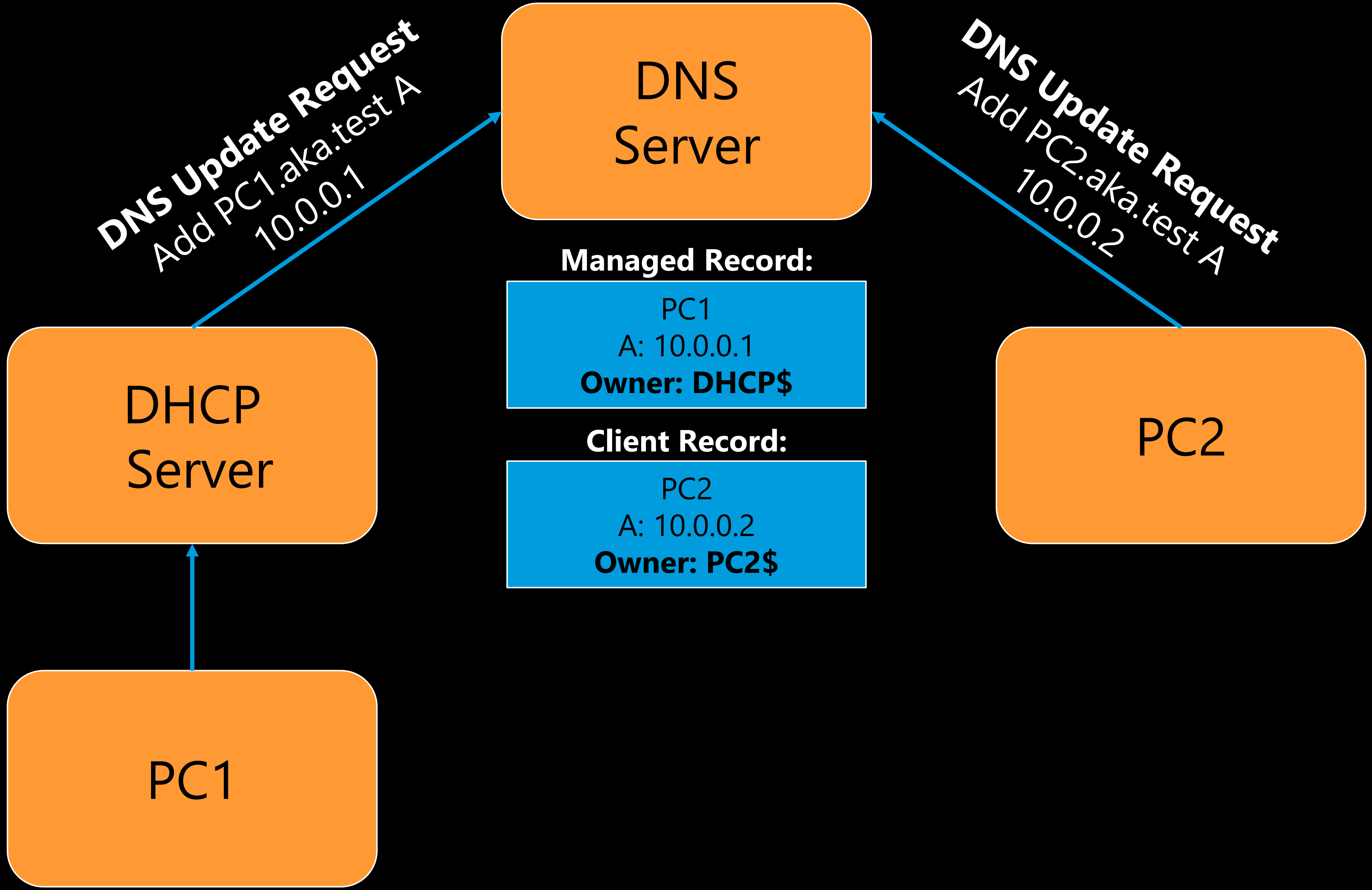


```
Dynamic update 0x2824 SOA aka.test CNAME A A 172.25.14.103
Dynamic update response 0x2824 Refused SOA aka.test CNAME A
```

DNS Record Types

- “Client Records” - records that were created by Windows hosts directly
- “Managed Records” - records that were created by the DHCP server

Main difference - record ownership



DNS Update Request
Add PC1.aka.test A
10.0.0.1

DNS
Server

DNS Update Request
Add PC2.aka.test A
10.0.0.2

Managed Record:

PC1
A: 10.0.0.1
Owner: DHCP$

Client Record:

PC2
A: 10.0.0.2
Owner: PC2$

DHCP
Server

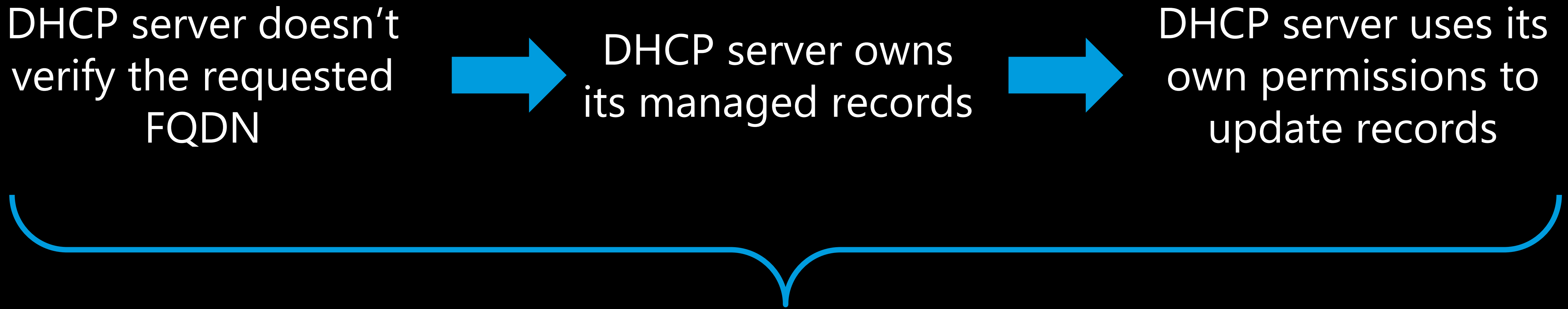
PC2

PC1

DDOverwrite

DHCP DNS Overwrite

Managed Record Overwrite



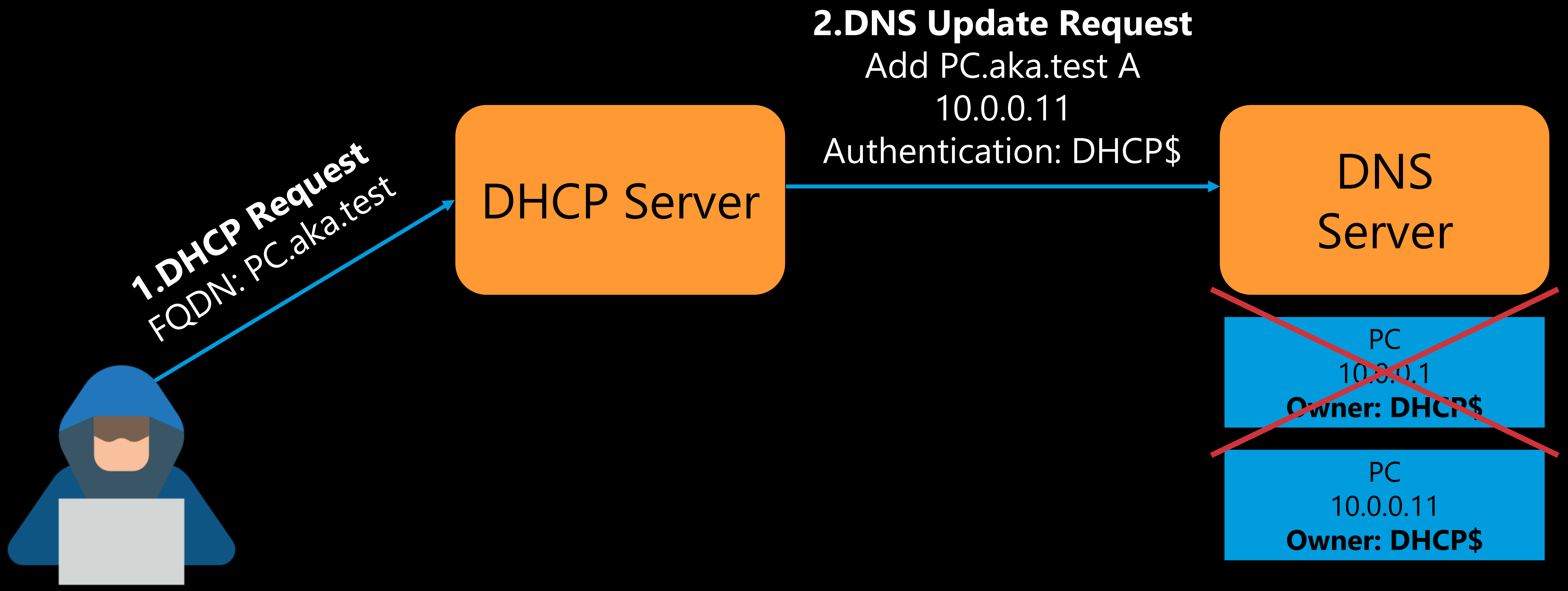
DHCP server doesn't verify the requested FQDN

DHCP server owns its managed records

DHCP server uses its own permissions to update records

We can overwrite any managed record!

Managed Record Overwrite



1.DHCP Request
FQDN: PC.aka.test

DHCP Server

2.DNS Update Request
Add PC.aka.test A
10.0.0.11
Authentication: DHCP$

DNS Server

~~PC~~
~~10.0.0.1~~
~~**Owner: DHCP$**~~

PC
10.0.0.11
Owner: DHCP$

Managed Record Overwrite

- By default, modern Windows hosts will not have a Managed Record

- The attack could be useful for:

Non-Windows clients

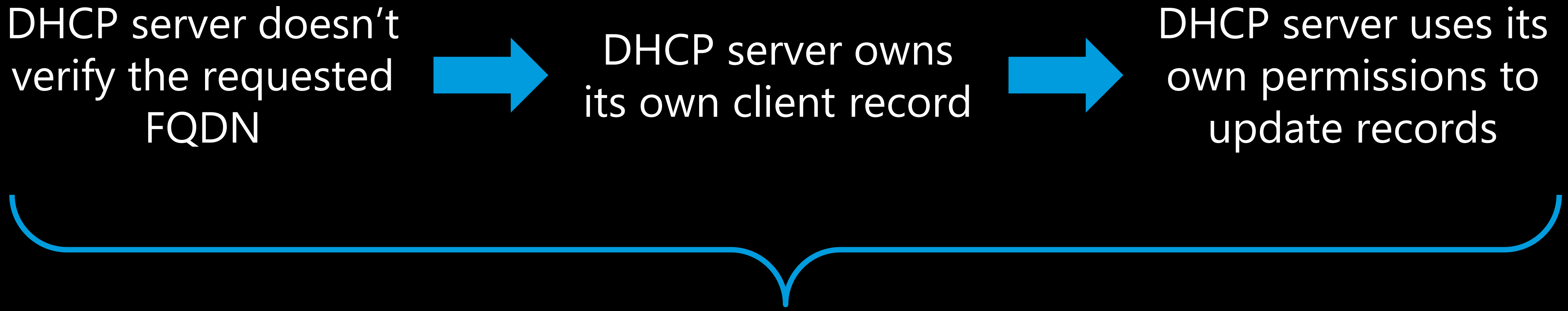
Legacy Windows hosts
(<Windows 2K)

Disabled client updates

Overwriting Client Records

- Owned by each individual client - DHCP server has no permissions
- But what about the DHCP server own client record?

DHCP Self-Overwrite



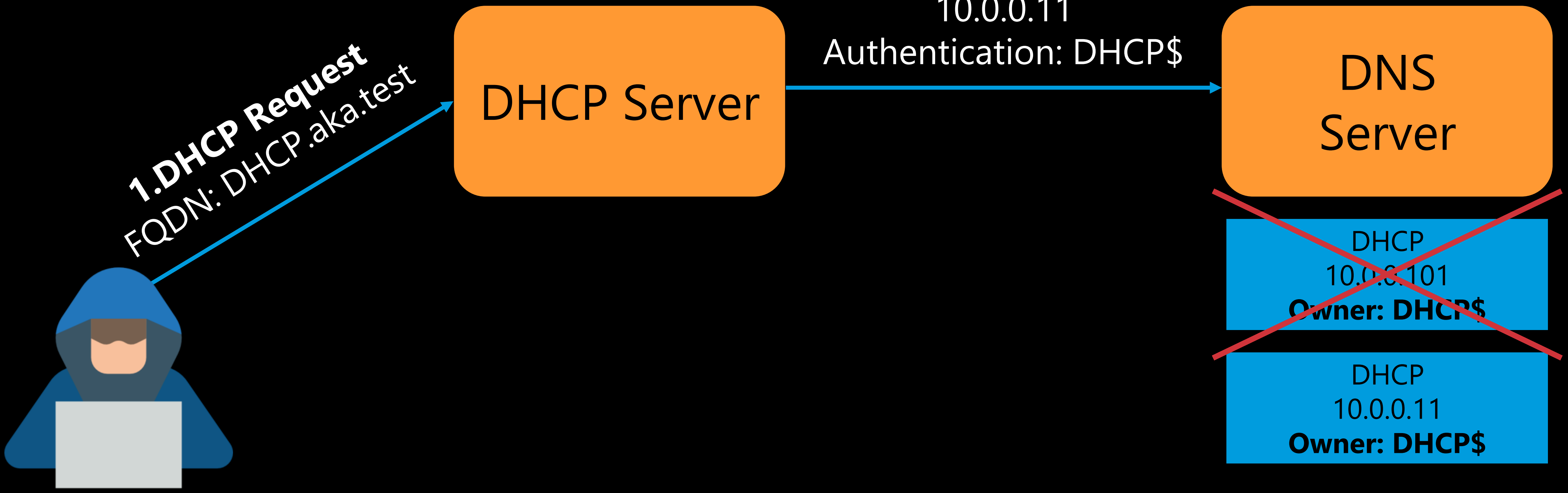
DHCP server doesn’t verify the requested FQDN

DHCP server owns its own client record

DHCP server uses its own permissions to update records

We can make the DHCP server overwrite its own record!

DHCP Self-Overwrite



1.DHCP Request
FQDN: DHCP.aka.test

DHCP Server

2.DNS Update Request
Add DHCP.aka.test A
10.0.0.11
Authentication: DHCP$

DNS
Server

~~DHCP~~
~~10.0.0.101~~
~~**Owner: DHCP$**~~

DHCP
10.0.0.11
Owner: DHCP$

DHCP Self-Overwrite

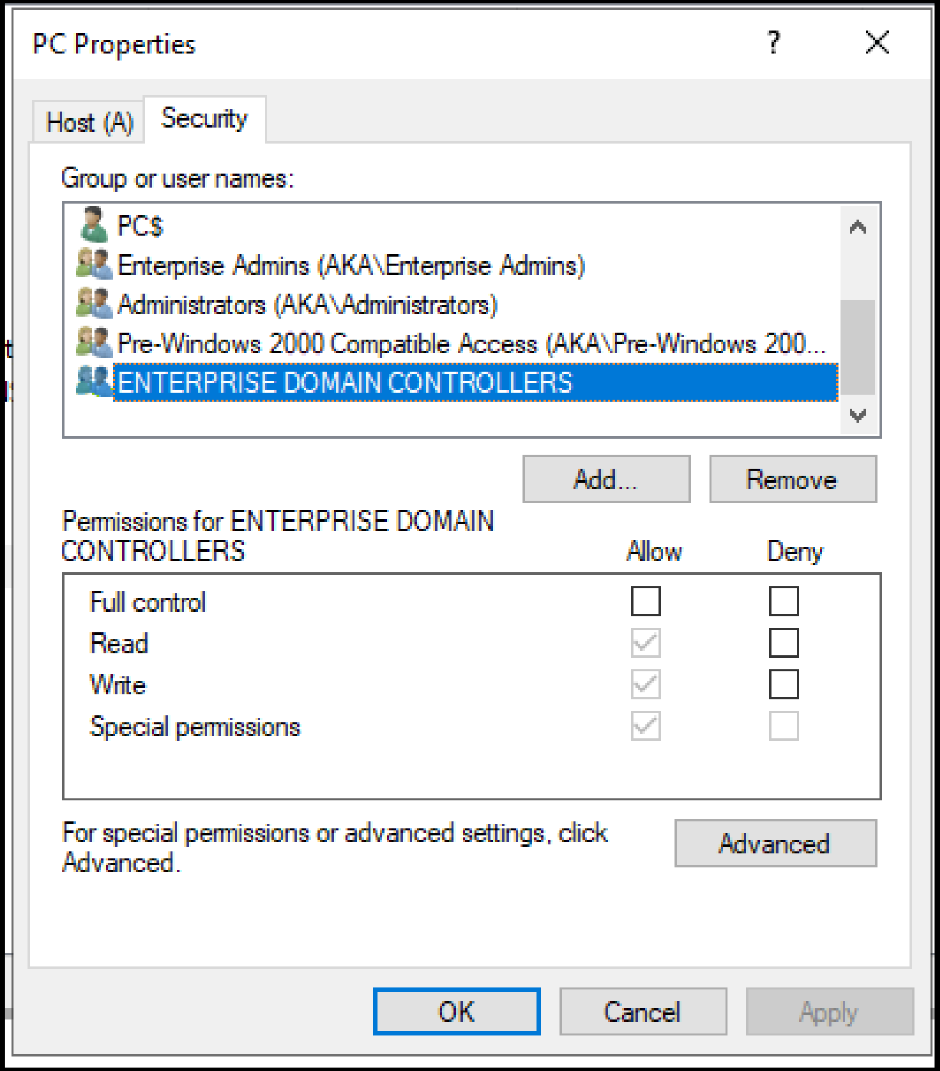
- Intercept any communication destined for the DHCP server
- Impact depends on other services hosted on the server

Domain Controller Self-Overwrite

- Overwrite the DC record if a DHCP server is installed on it

DC Arbitrary Overwrite

DCs have write permissions on all the records in the zone **- arbitrary DNS record overwrite!**



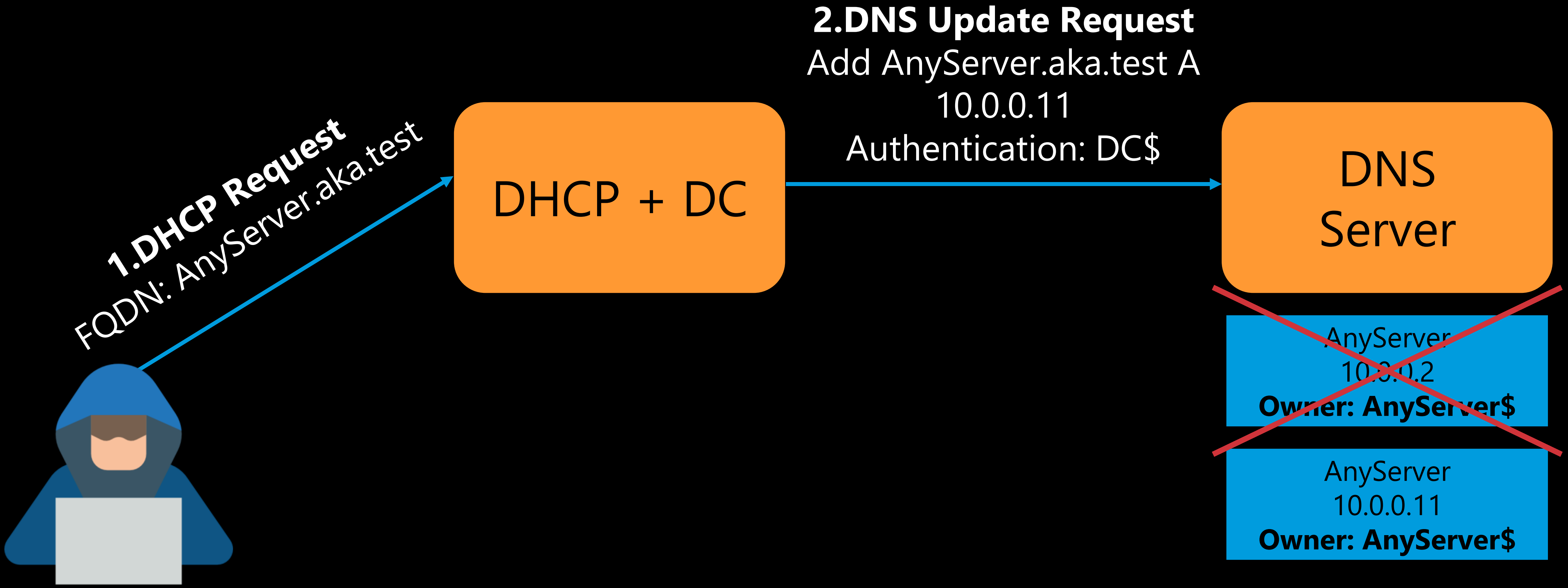
Group or user names:

- PC$
- Enterprise Admins (AKA\Enterprise Admins)
- Administrators (AKA\Administrators)
- Pre-Windows 2000 Compatible Access (AKA\Pre-Windows 200...
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for ENTERPRISE DOMAIN CONTROLLERS	Allow	Deny
Full control	□	□
Read	☑	□
Write	☑	□
Special permissions	☑	□

For special permissions or advanced settings, click Advanced.

DC Arbitrary Overwrite



1.DHCP Request
FQDN: AnyServer.aka.test

DHCP + DC

2.DNS Update Request
Add AnyServer.aka.test A 10.0.0.11
Authentication: DC$

DNS Server

~~AnyServer~~
~~10.0.0.2~~
~~**Owner: AnyServer$**~~

AnyServer
10.0.0.11
Owner: AnyServer$

Attack Demo

DNS Spoofing Impact

Relay Authentication

Capture Sensitive Information

Block Access to SIEM/EDR Servers

DC Arbitrary Overwrite

Domain compromise from an **unauthenticated context**

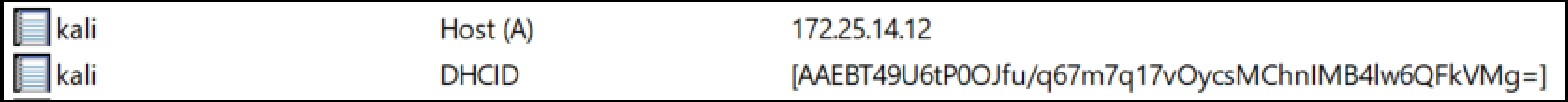
Works with the **default configuration**

Seen in **57% of the networks** that used Microsoft DHCP

Mitigations for DHCP DNS Attacks

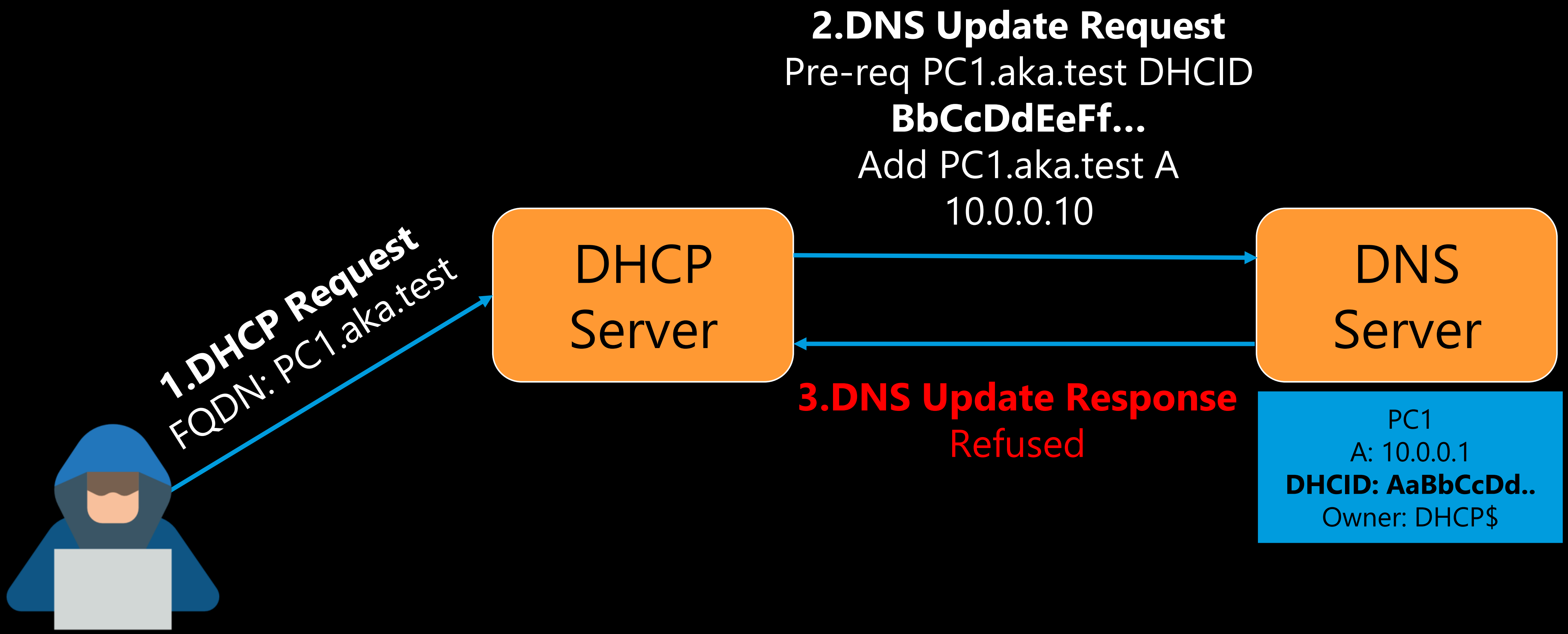
Name Protection

- Prevent overwriting names that were already created by the DHCP server
- Associate each Managed Record with its original creator
- Implemented using DHCID records - DHCP client identifier



kali	Host (A)	172.25.14.12
kali	DHCID	[AAEBT49U6tP0OJfu/q67m7q17vOycsMChnIMB4lw6QFkVMg=]

Name Protection



1.DHCP Request
FQDN: PC1.aka.test

DHCP Server

2.DNS Update Request
Pre-req PC1.aka.test DHCID
BbCcDdEeFf…
Add PC1.aka.test A
10.0.0.10

DNS Server

3.DNS Update Response
Refused

PC1
A: 10.0.0.1
DHCID: AaBbCcDd..
Owner: DHCP$

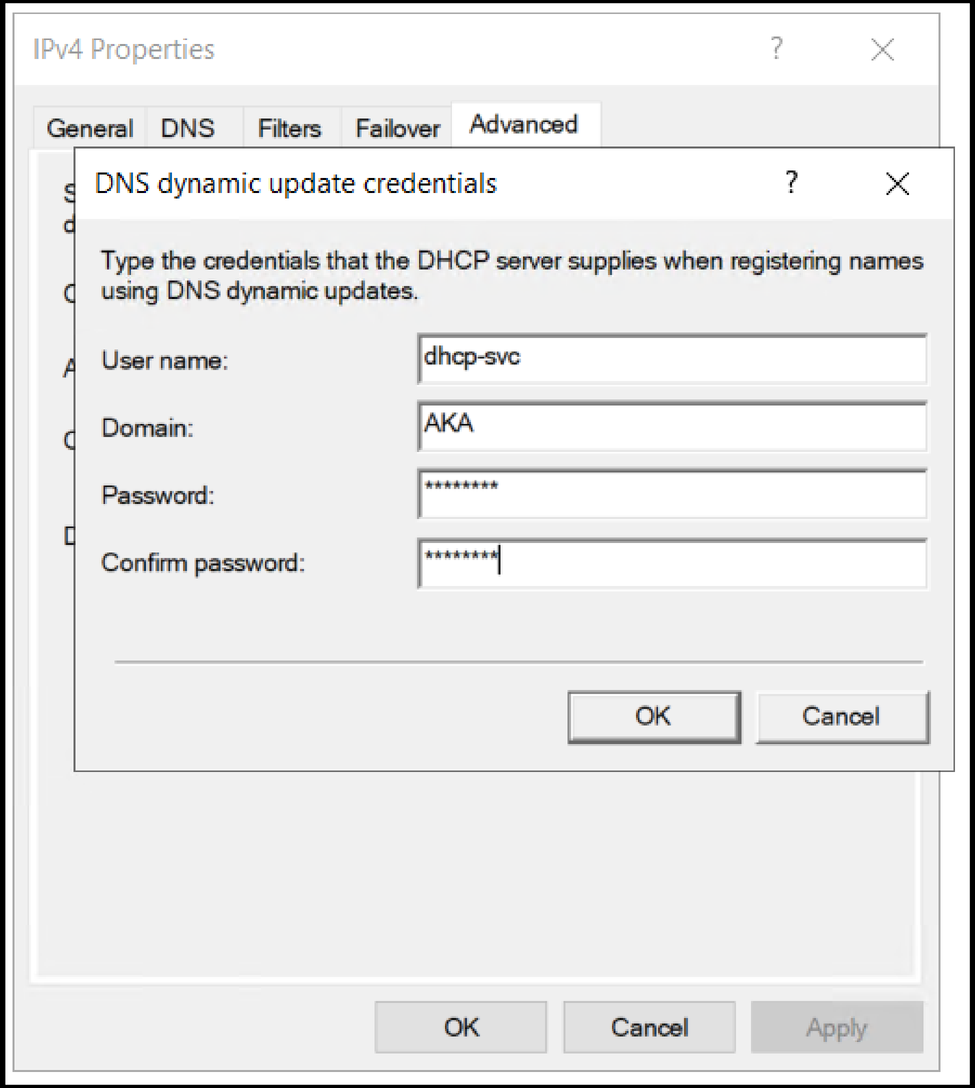
Name Protection Caveats

- Only meant to protect Managed records - prevent Managed Record Overwrite

- Could be bypassed even in this case by spoofing a DHCP Release

DNS Credential

- Specify an alternative credential to be used when sending updates



DNS dynamic update credentials

Type the credentials that the DHCP server supplies when registering names using DNS dynamic updates.

User name: dhcp-svc

Domain: AKA

Password: ********

Confirm password: ********

DNS Credential Caveats

- The credential used has to be weak

- Only meant to protect Client records - prevent DHCP Self-Overwrite & DC Arbitrary Overwrite

Attacks & Mitigations Summary

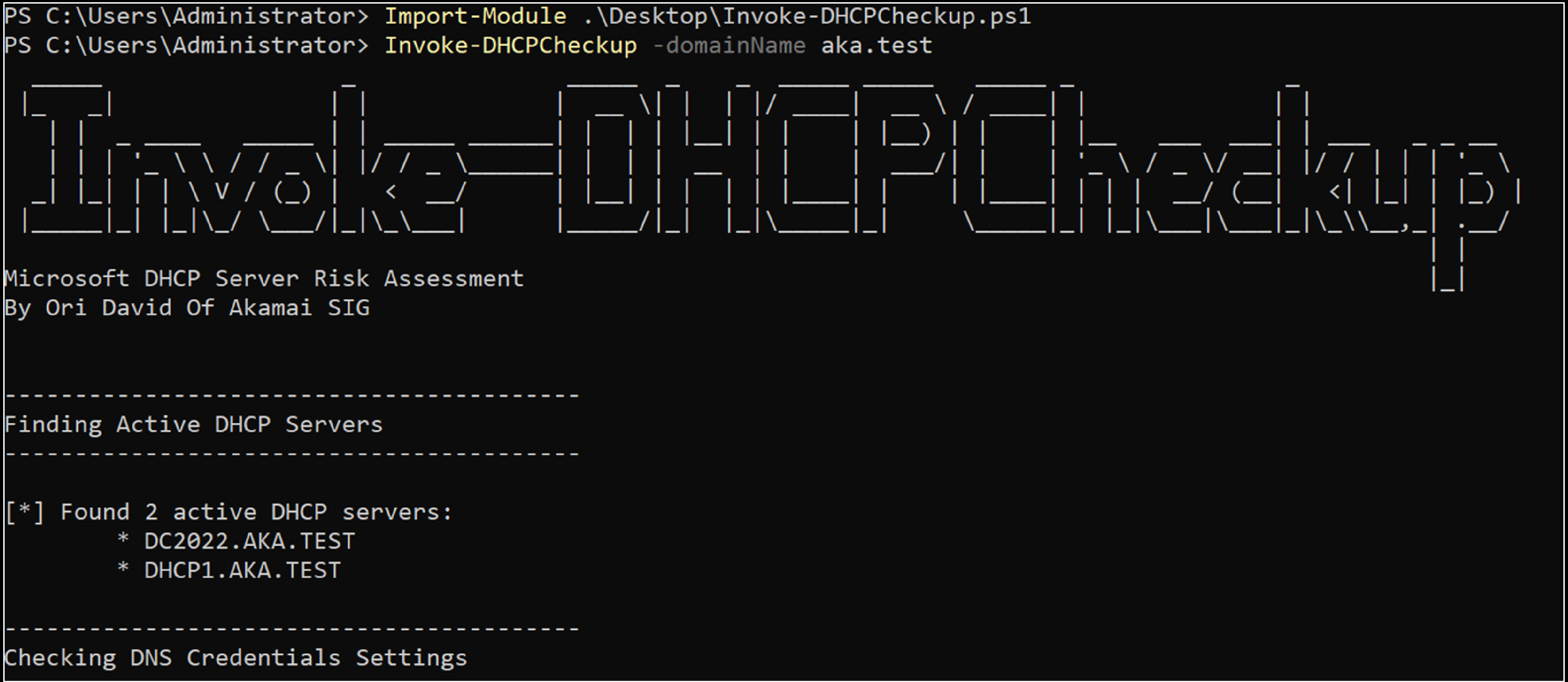
- DHCP DNS Spoofing
  - **Can't mitigate**

- Managed Record Overwrite
  - **Can't mitigate**
  - Name Protection could make this harder to perform
  - Use static DNS records instead if possible

- DHCP Self-Overwrite & DC Arbitrary Overwrite
  - Mitigate by configuring a weak user as a DNS credential
  - Especially critical for Domain Controllers

Microsoft’s Response

THIS IS FINE



```
PS C:\Users\Administrator> Import-Module .\Desktop\Invoke-DHCPCheckup.ps1
PS C:\Users\Administrator> Invoke-DHCPCheckup -domainName aka.test
  _____                 _               _____  _    _  _____ _____   _____ _               _
 |_   _|               | |             |  __ \| |  | |/ ____|  __ \ / ____| |             | |
   | |  _ ____   _____ | | _____ ______| |  | | |__| | |    | |__) | |    | |__   ___  ___| | ___   _ _ __
   | | | '_ \ \ / / _ \| |/ / _ \______| |  | |  __  | |    |  ___/| |    | '_ \ / _ \/ __| |/ / | | | '_ \
  _| |_| | | \ V / (_) |   <  __/      | |__| | |  | | |____| |    | |____| | | |  __/ (__|   <| |_| | |_) |
 |_____|_| |_|\_/ \___/|_|\_\___|      |_____/|_|  |_|\_____|_|     \_____|_| |_|\___|\___|_|\_\\__,_| .__/
                                                                                                     | |
Microsoft DHCP Server Risk Assessment                                                                |_|
By Ori David Of Akamai SIG



-----------------------------------------
Finding Active DHCP Servers
-----------------------------------------

[*] Found 2 active DHCP servers:
        * DC2022.AKA.TEST
        * DHCP1.AKA.TEST

-----------------------------------------
Checking DNS Credentials Settings
```

Black Hat Europe Sound Bytes

- DHCP DNS Dynamic Updates provide a significant attack surface

- Avoid risky configuration
  - Configure a weak user as the DNS credential on all DHCP servers
  - Enable DHCP Name Protection

- Disable DHCP DNS Dynamic Updates if they aren’t required

Akamai

Thank you

Questions?

@oridavid123