

HI!

My Name Is

WHAT?

Abusing Microsoft DHCP to
Take Over Active Directory

Ori David

whoami

Ori David

Security Researcher at  Akamai

Background in red teaming & threat hunting

BlueHat IL 2020 - Registration not approved ➔

Inbox



bluehatil 1/31/2020

to me ▾



"This is the third year in a row that my registration is not approved.."

"Everyone I know gets approved and I'm always rejected.."

Ori, 2020

"It really means a lot to me.. "

"what am I doing wrong?"

Hi Ori,

Thanks for reaching out.

We approved your request to attend the conference on day 1.

Best,

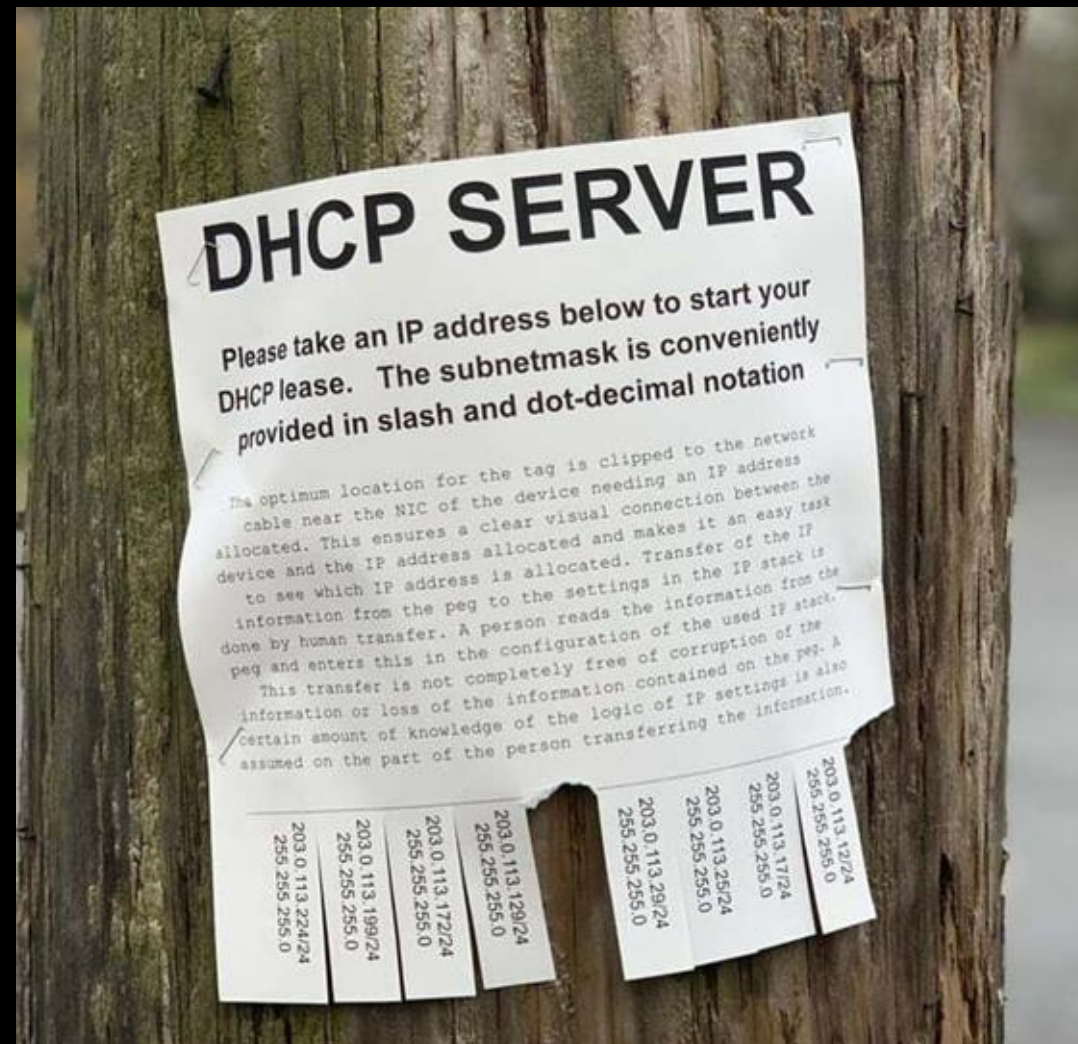
The BlueHat IL Team

Agenda

- Microsoft DHCP
- DNS Spoofing
- Privilege escalation
- Mitigations

Microsoft DHCP

- One of the most common DHCP servers on the market
- Decided to look at Active Directory integration



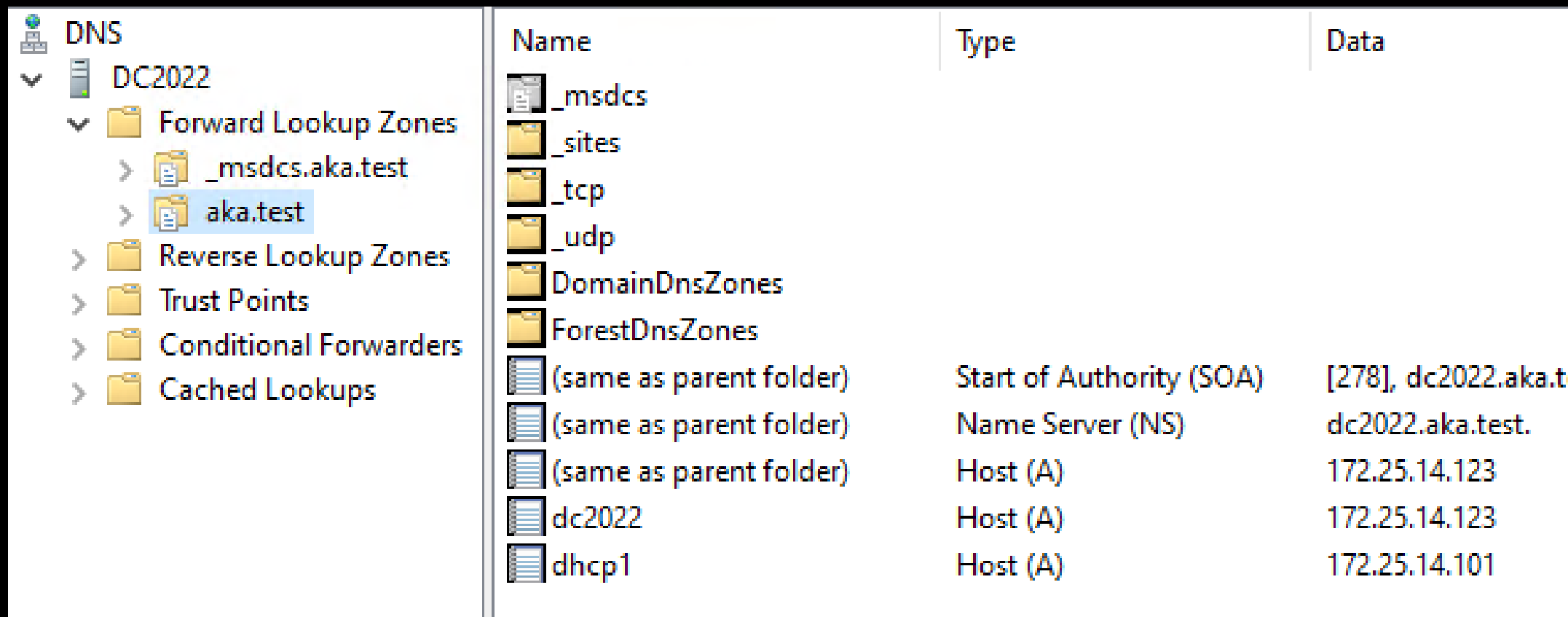
DHCP DNS Dynamic Updates

DNSUpdateProxy

DHCP Administrators

ADI-DNS

Every domain requires an Active Directory Integrated DNS zone



The screenshot shows the Windows DNS console for a server named DC2022. The left pane shows the tree structure: DNS > DC2022 > Forward Lookup Zones > aka.test. The right pane displays a table of DNS records for the aka.test zone.

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

```

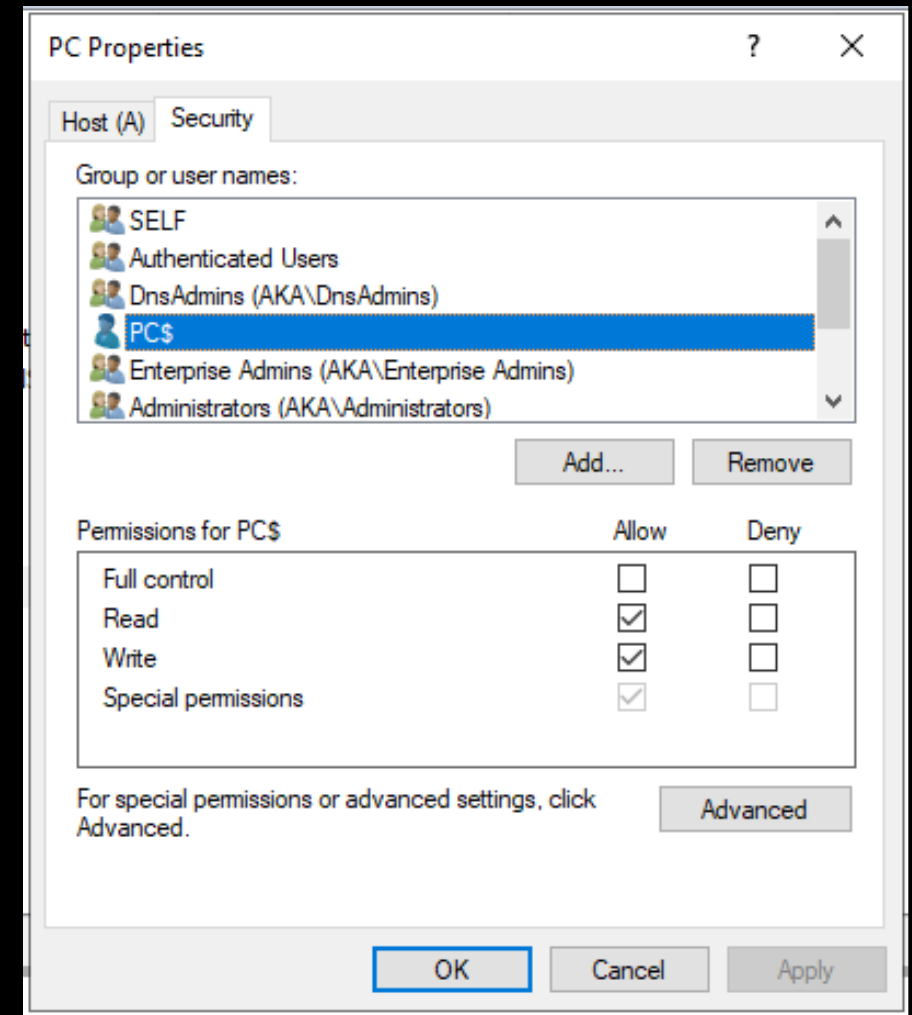
  v Key Data: 6082067706062b0601050502a082066b30820667a00d300b06092a864886f712010202a2...
  v GSS-API Generic Security Service Application Program Interface
    OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
  v Simple Protected Negotiation
    v negTokenInit
      > mechTypes: 1 item
    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

```

Secure Dynamic Updates

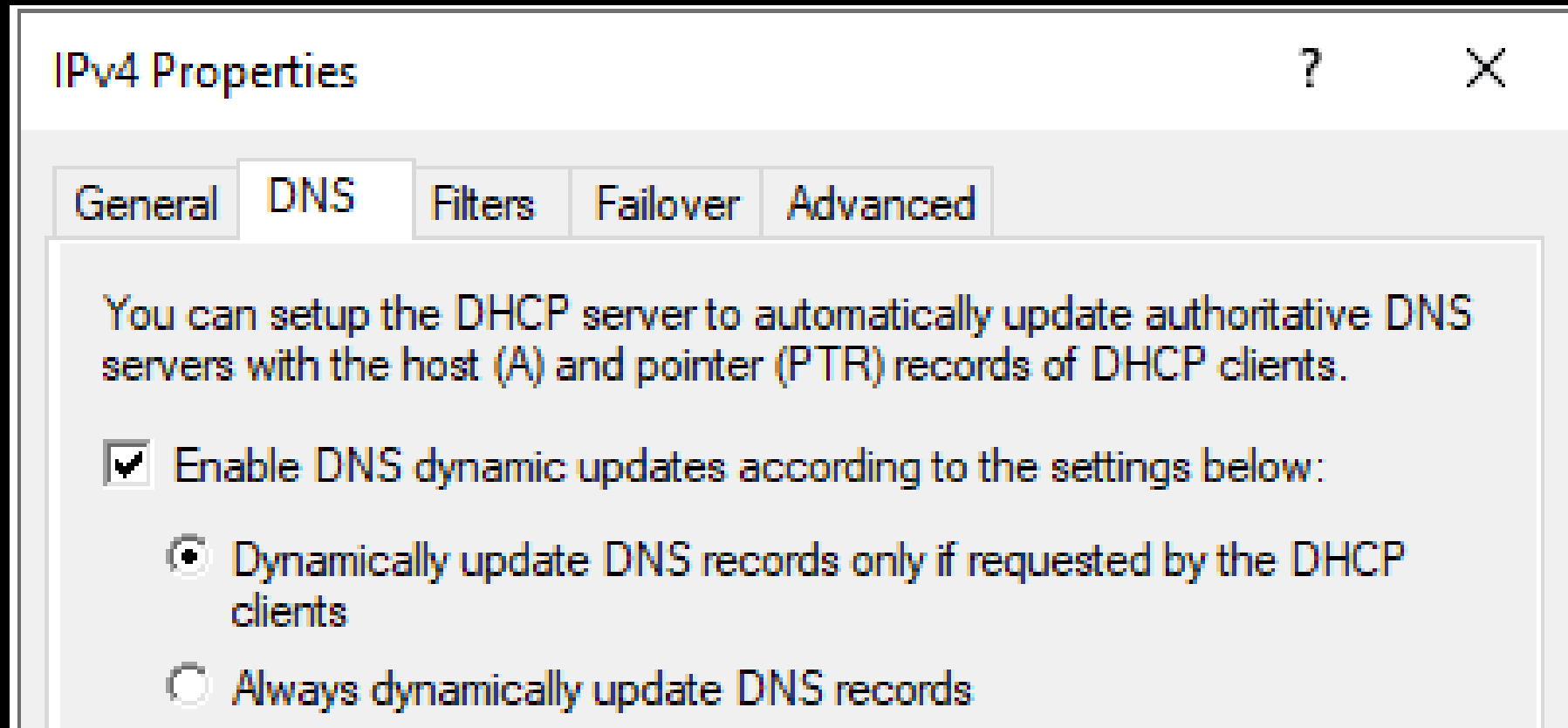
Updates are authorized based on ACLs

Once created - every machine controls its own record

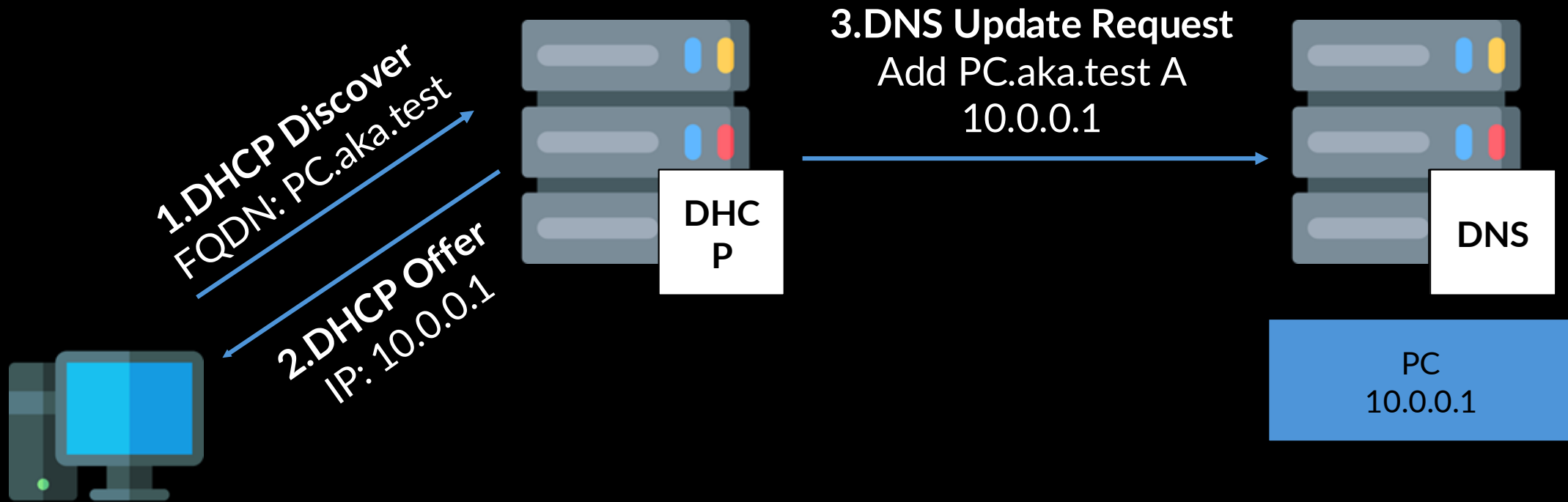


DHCP DNS Dynamic Update

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

Abusing DHCP DNS Dynamic Updates

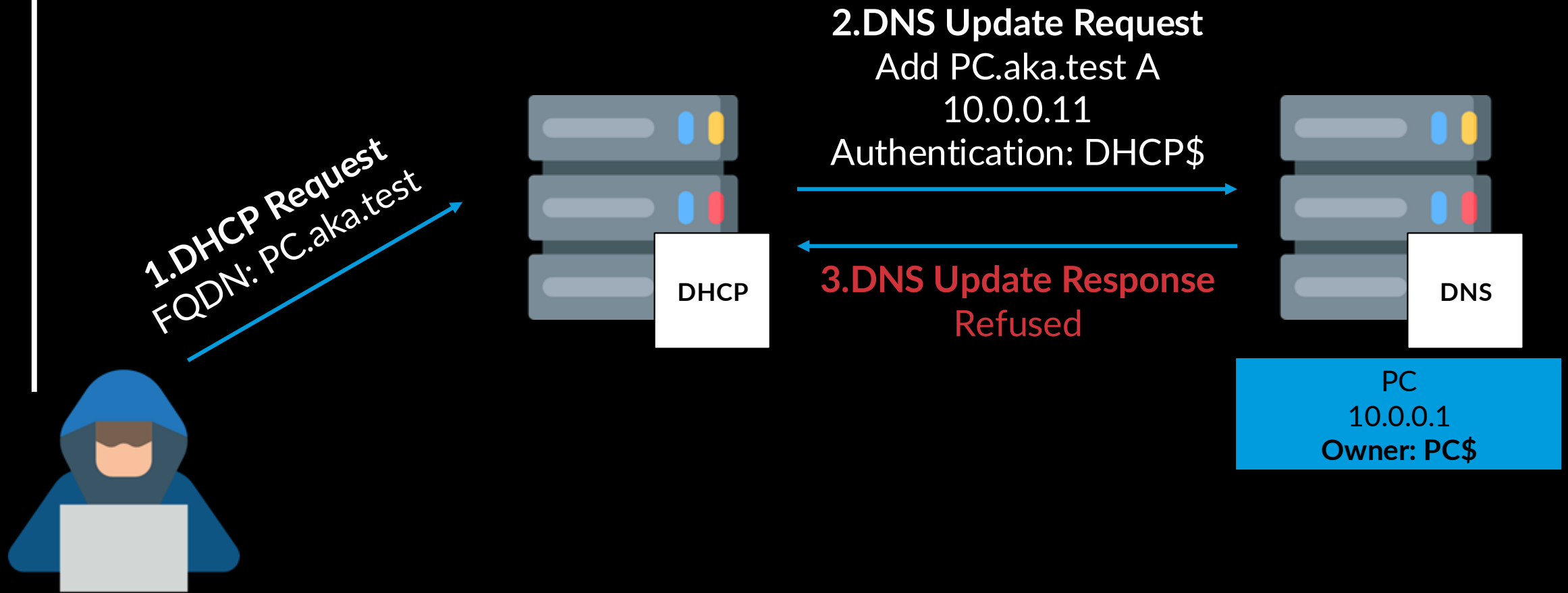
How can we abuse the ability to create DNS records?



Overwriting DNS Records



Working Towards Overwrites



Working Towards Overwrites

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

ACLs are meant to stop overwrites

Overwriting DNS Records

Records are owned by each individual client - DHCP server has no permissions

But what about the DHCP server own record?



DHCP Self-Overwrite

DHCP server
doesn't verify
the requested
FQDN

+

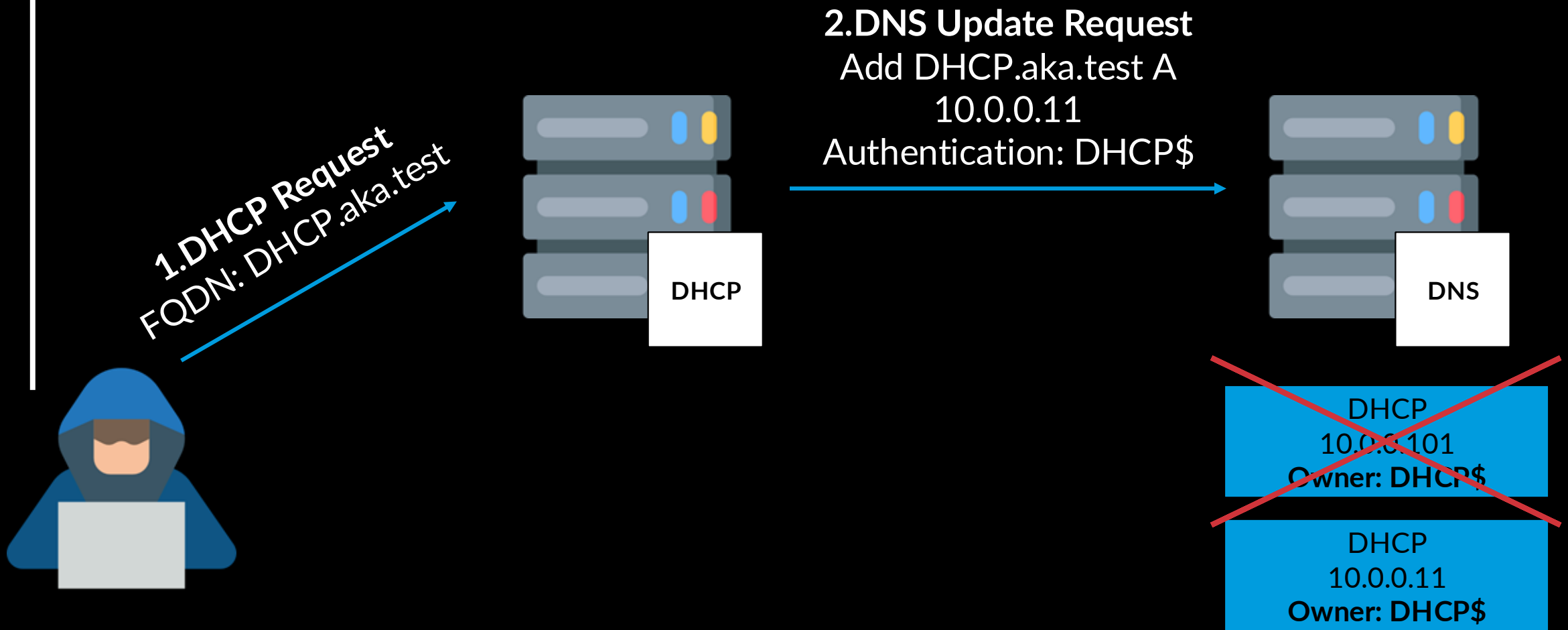
DHCP server
owns its own
DNS record

+

DHCP server
uses its own
permissions to
update records

We can make the DHCP server overwrite its
own record!

DHCP Self-Overwrite



DHCP Self-Overwrite

Intercept any communication destined for the DHCP server

Impact depends on other services hosted on the server



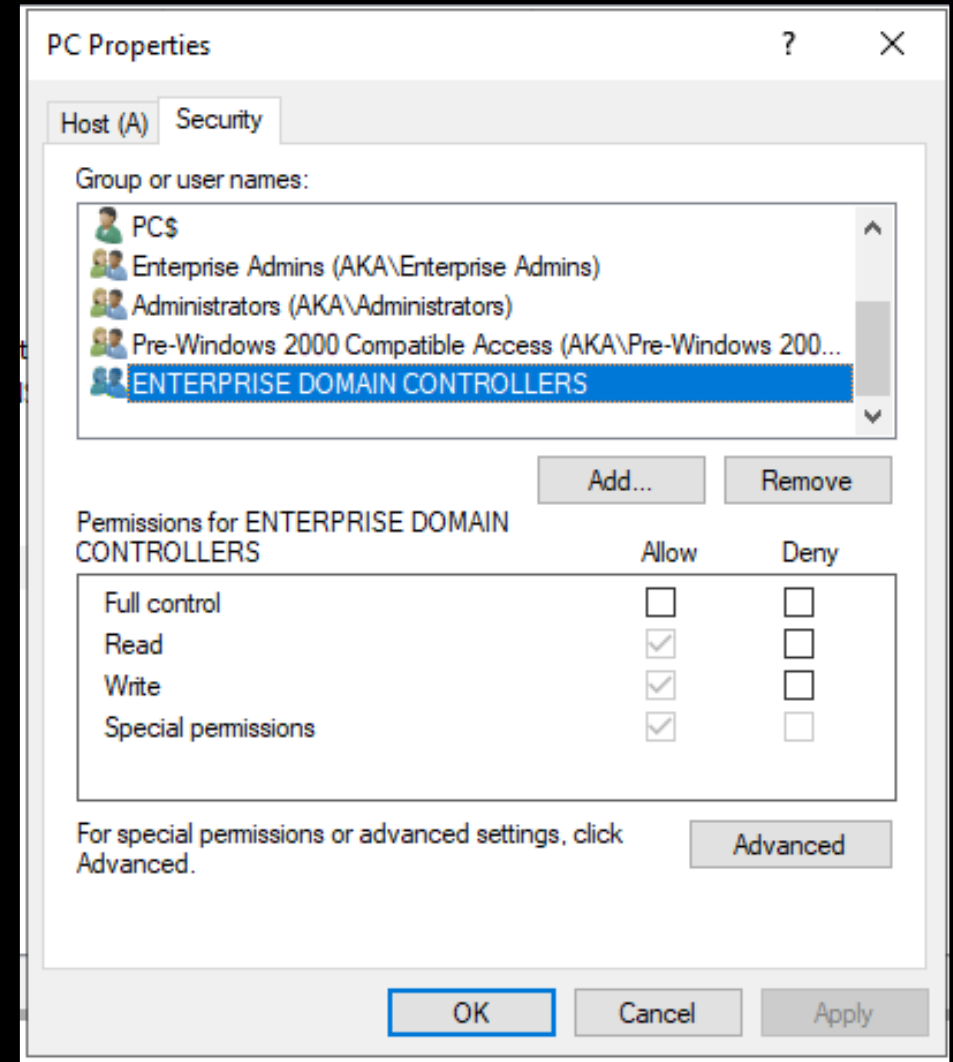
Domain Controller Self-Overwrite

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

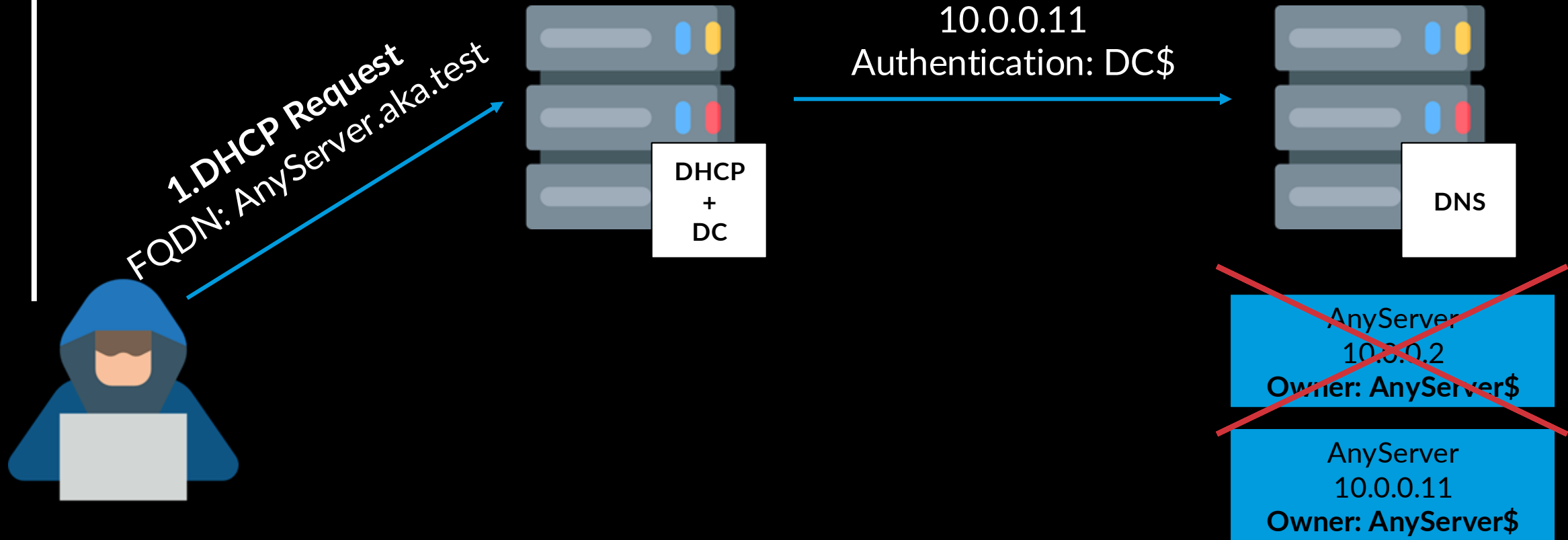


DC Arbitrary Overwrite

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



DC Arbitrary Overwrite



Attack Demo

DC Arbitrary Overwrite

Domain compromise from an **unauthenticated context**

Works with the **default configuration**

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

DHCP DNS Dynamic Updates

DNSUpdateProxy

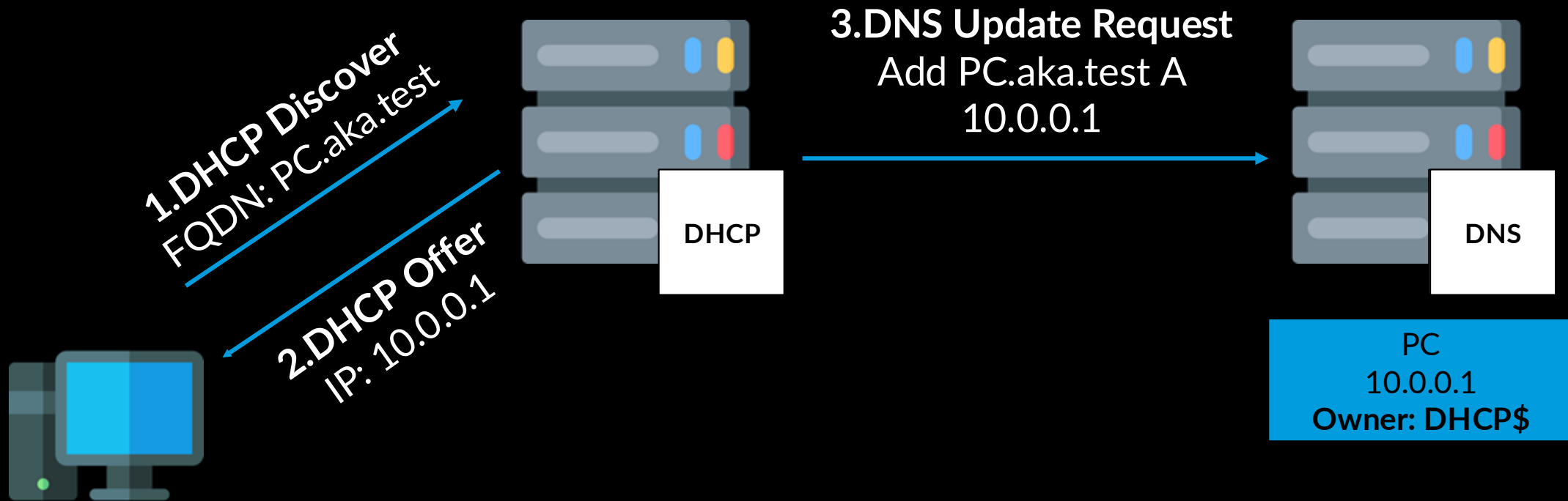
DHCP Administrators

DNSUpdateProxy

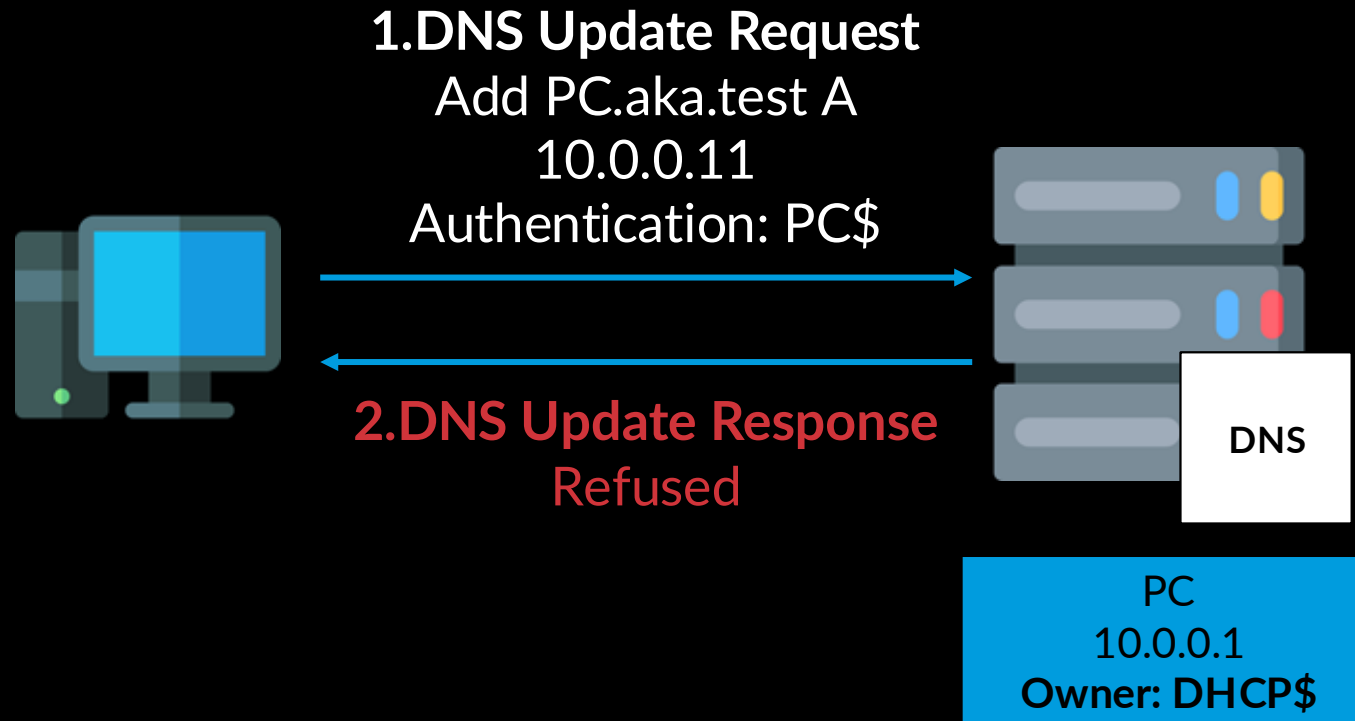
A group meant to solve permission-related issues

DHCP servers are added to the group

DNSUpdateProxy - Upgraded Client Problem



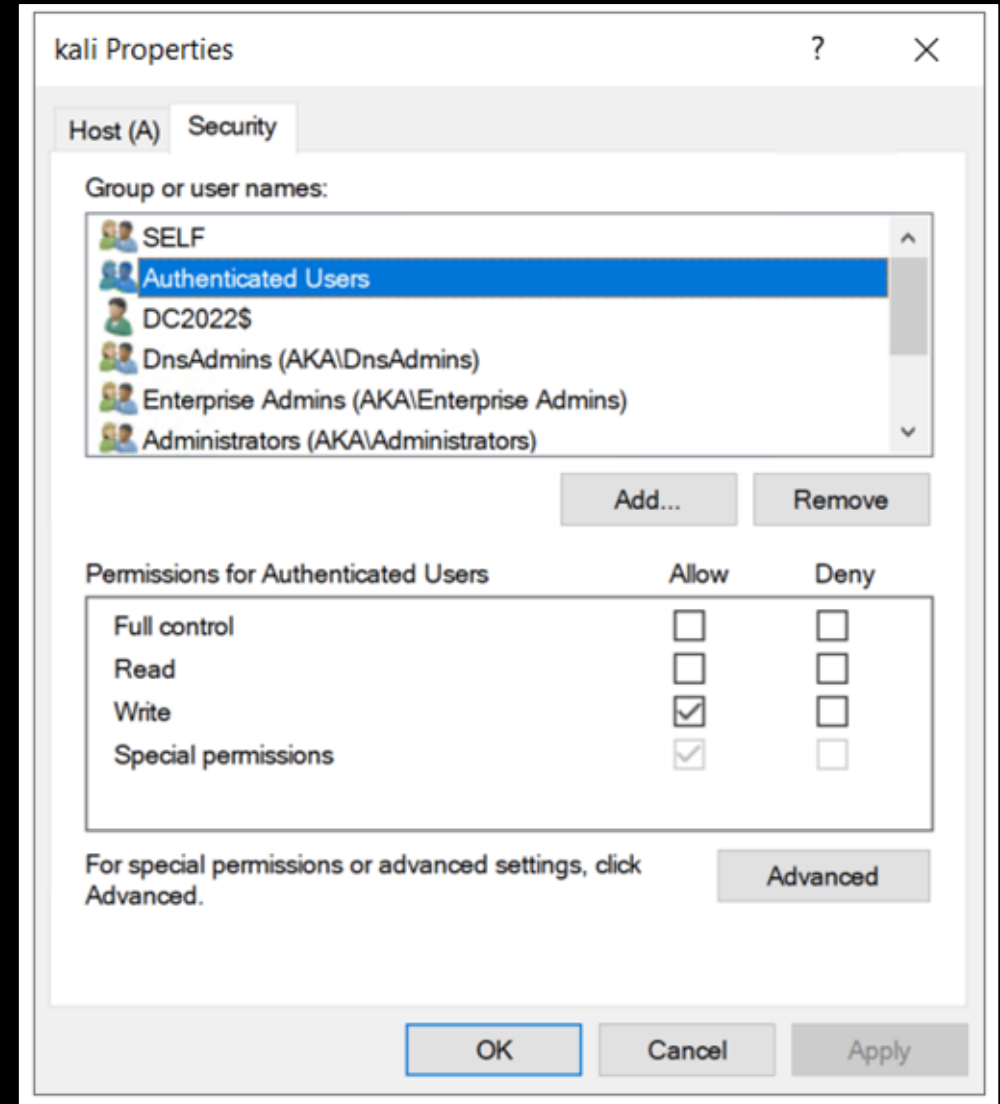
DNSUpdateProxy - Upgraded Client Problem



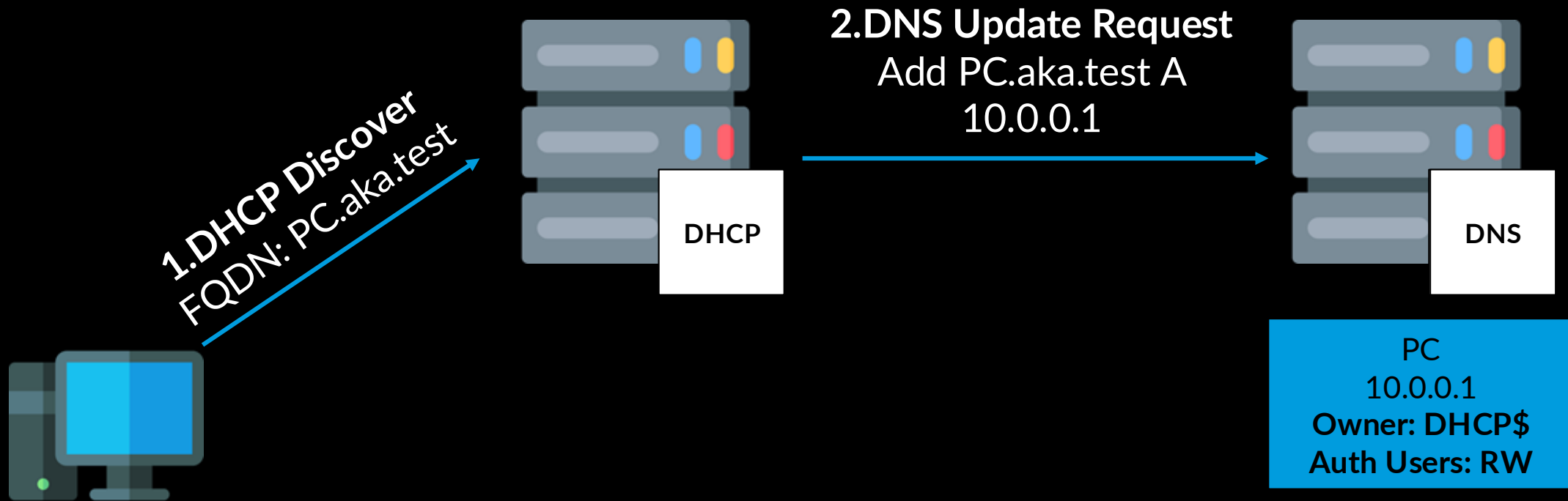
DNSUpdateProxy

Group members create "special"
DNS records

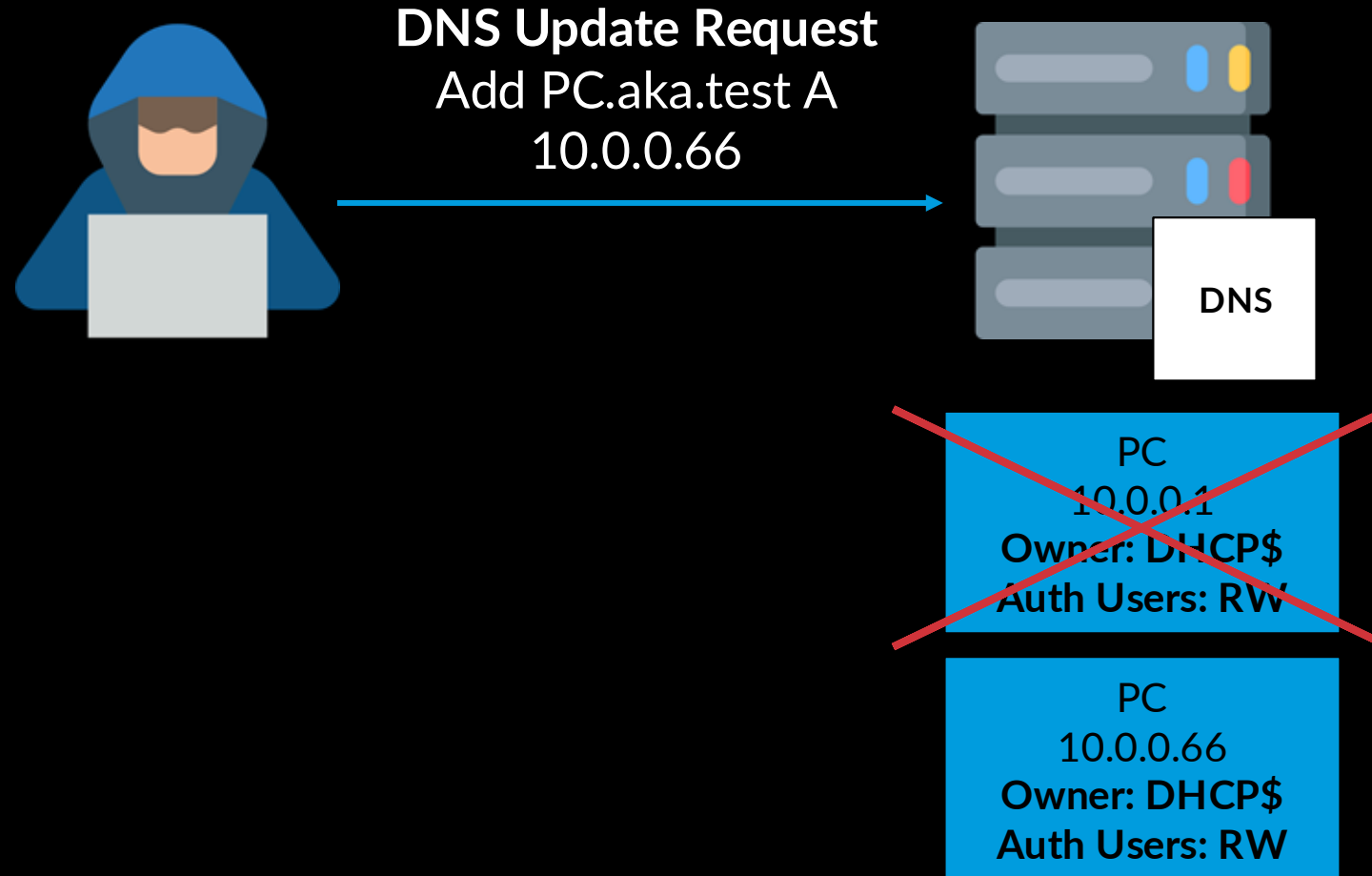
Authenticated Users have Write
permission over the record



DNSUpdateProxy

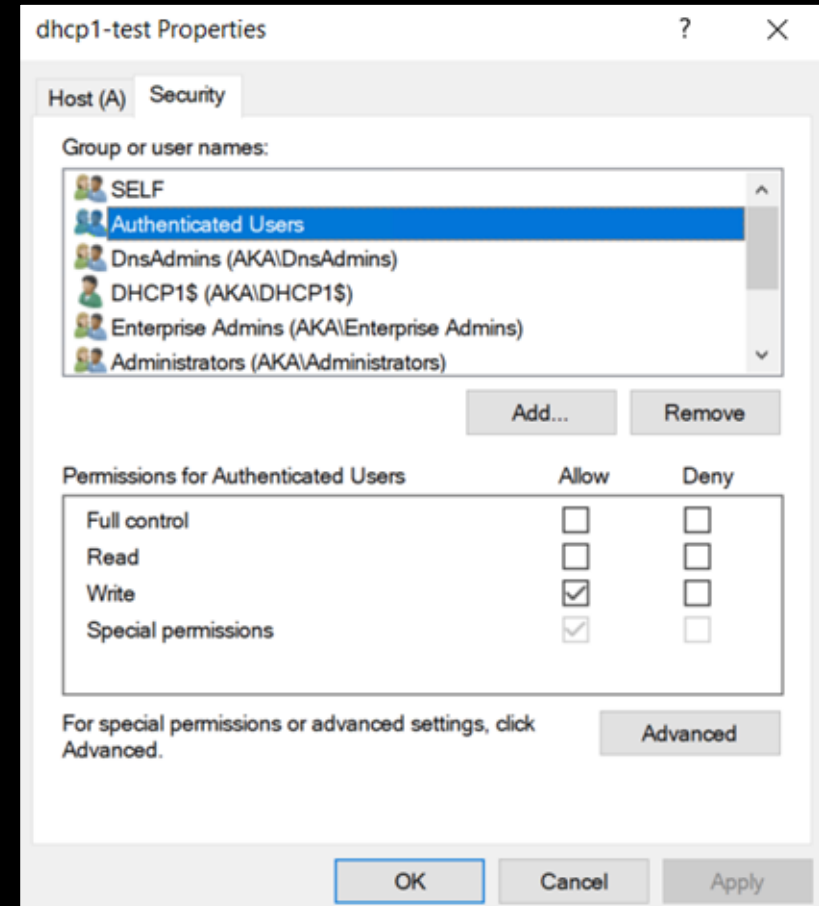
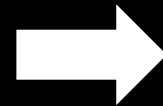
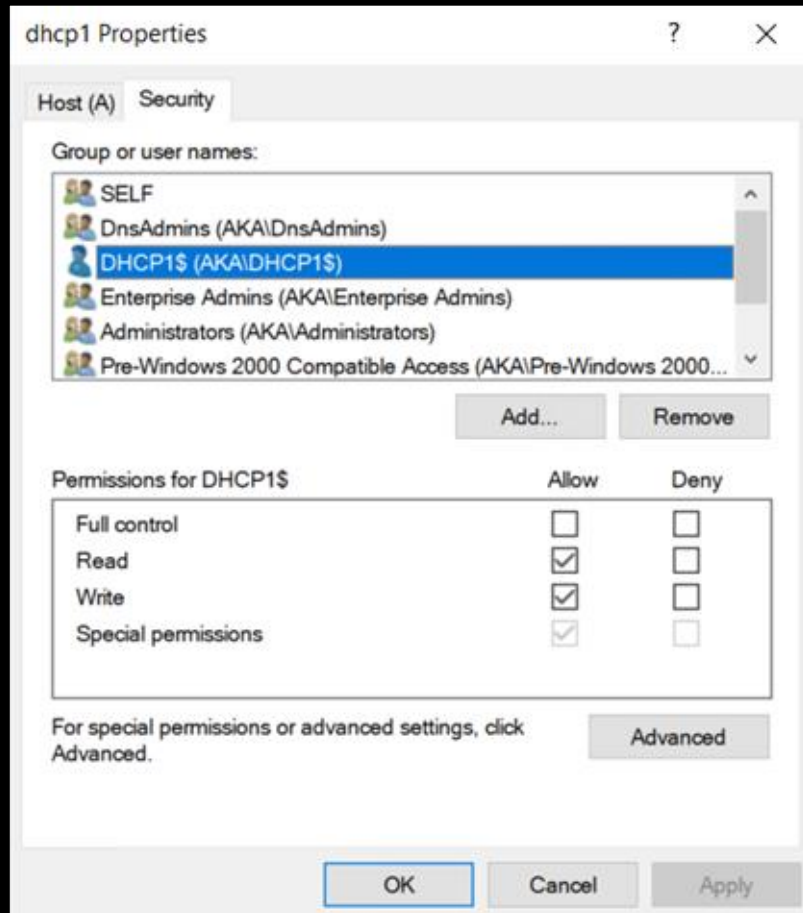


DNSUpdateProxy



DNSUpdateProxy Bug

When DNSUpdateProxy members create their own records - they are also vulnerable



DHCP DNS Dynamic Updates

DNSUpdateProxy

DHCP Administrators

DHCP Administrators

AD group that is used to manage DHCP server configurations

DHCP Admins to Domain Admins?

Feature, not bug: DNSAdmin to DC compromise in one line



Shay Ber · [Follow](#)

7 min read · May 8, 2017

Abusing DHCP Options

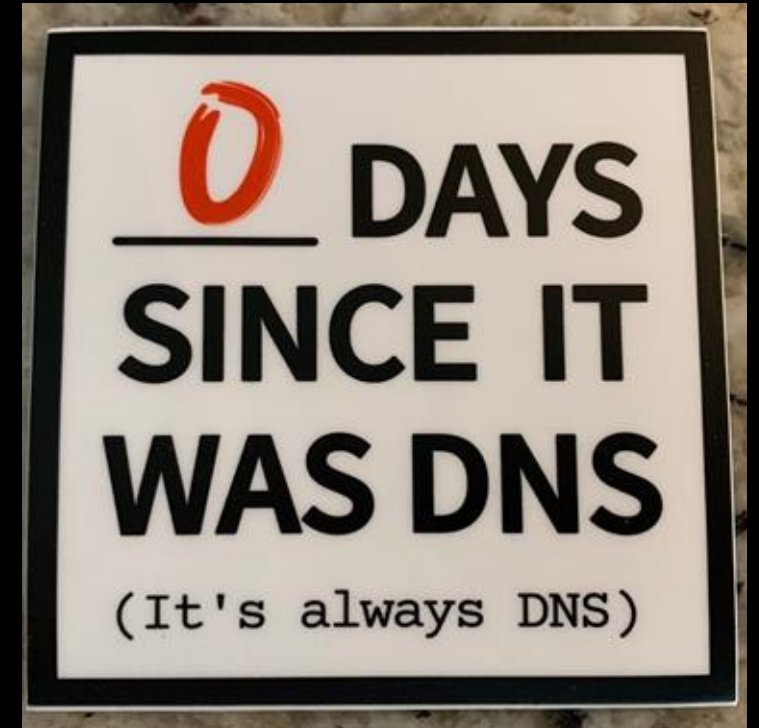
The different configurations requested by DHCP clients

```
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (43) Vendor-Specific Information
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (119) Domain Search
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (252) Private/Proxy autodiscovery
```

DNS Server Option

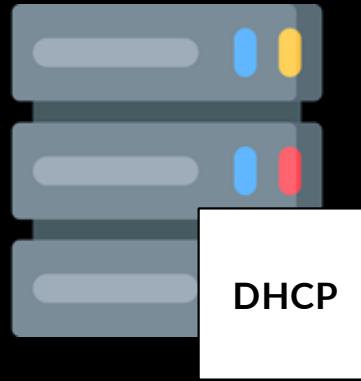
Defines the DNS server to be used by the DHCP Client

Also determines the server to be used for DHCP DNS Dynamic Updates!

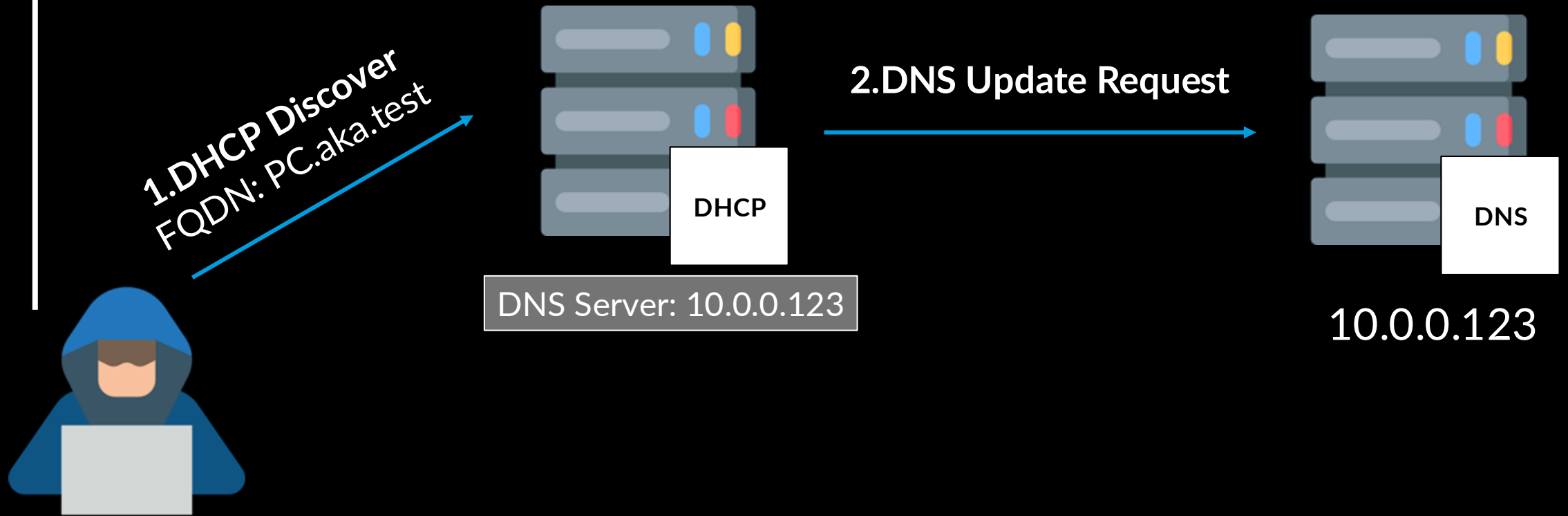


DNS Server Option

1. Set DHCP Option
DNS Server: 10.0.0.123

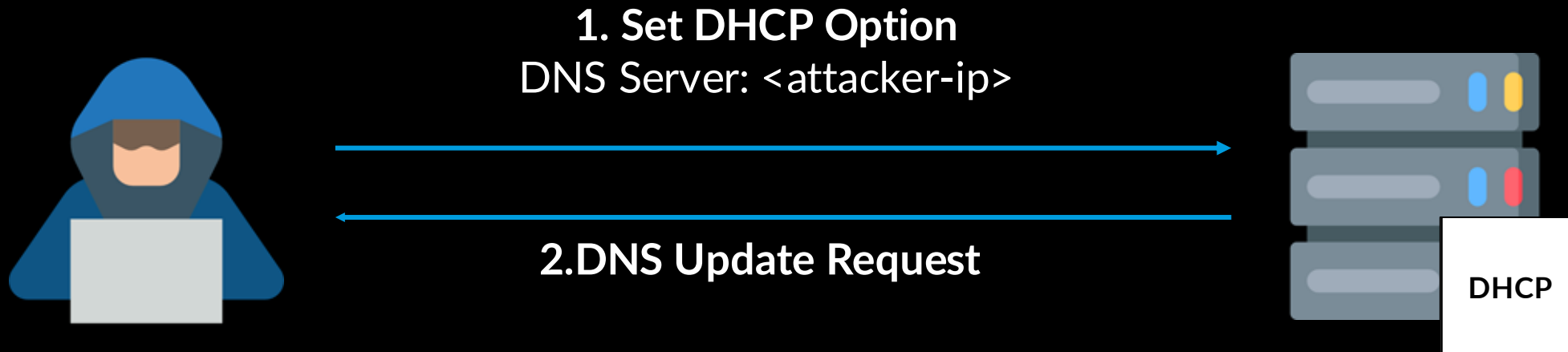


DNS Server Option



DHCP Coerce

Set our own machine as the DNS server



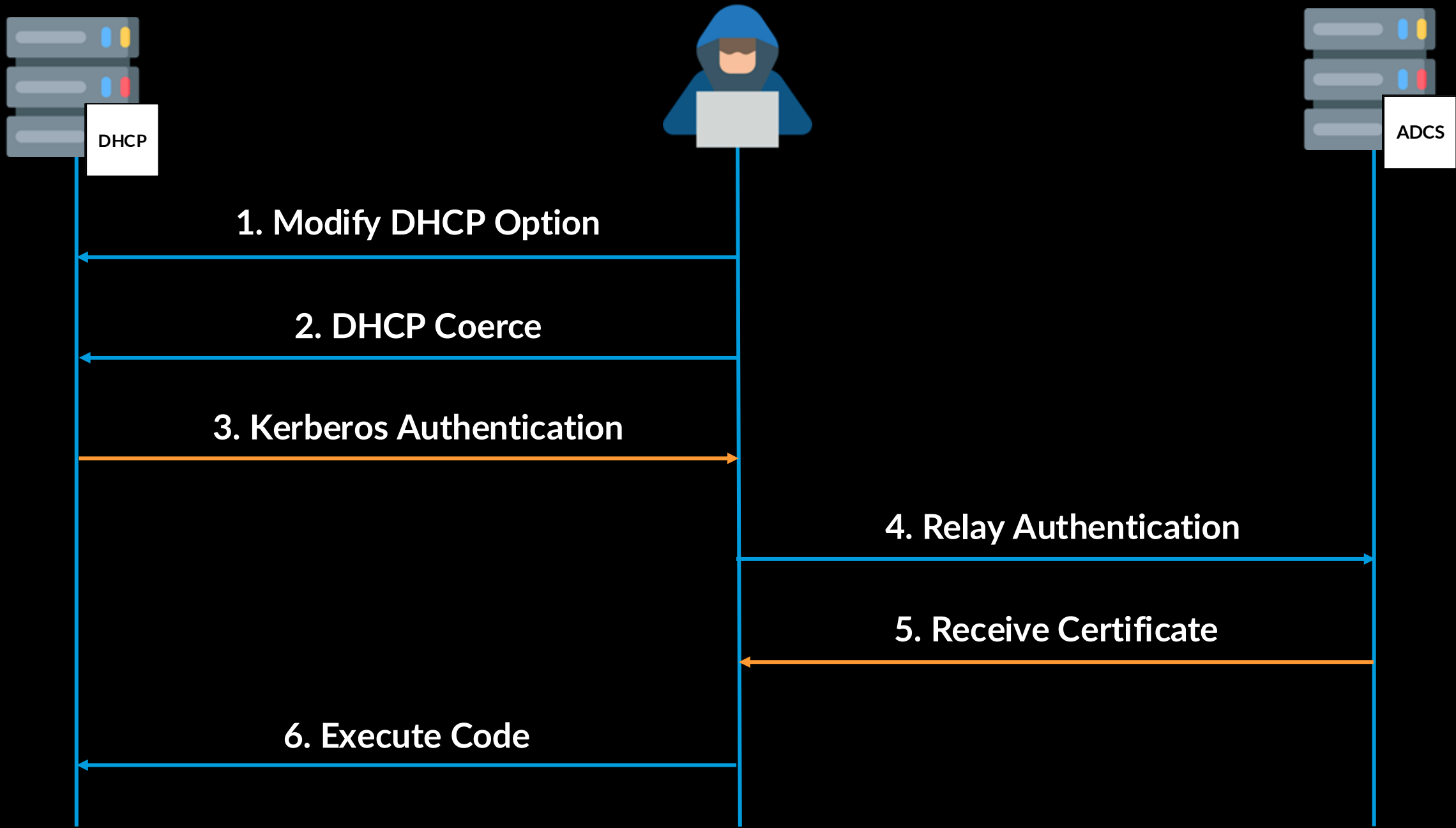
Coerce Kerberos authentication!

Kerberos Relay

Kerberos authentication
can be relayed to certain
targets

ADCS - Web enrollment
service





DHCP Coerce -> Kerberos Relay

- DHCP Administrators can compromise the machine account of the DHCP server (Given vulnerable ADCS)
- If the DHCP server is a DC - DHCP Admin == Domain Admin

Mitigations

Mitigating DHCP DNS Spoofing

- Disable DHCP DNS Dynamic Updates
- Name Protection: Prevent overwriting names that were already created by the DHCP server
 - Doesn't work
- DNS Credential: Specify an alternative credential to be used when sending updates
 - Does work! Use it
- Don't install Microsoft DHCP on a DC

Mitigating DNSUpdateProxy Risks

- Don't use DNSUpdateProxy.

Mitigating DHCP Administrators abuse

- DHCP Admins group hygiene
- Employ relay mitigations
- Don't install Microsoft DHCP on a DC

Microsoft's Response

```
PS C:\Users\Administrator> Import-Module .\Desktop\Invoke-DHCPCheckup.ps1
PS C:\Users\Administrator> Invoke-DHCPCheckup -domainName aka.test
```

Invoke-DHCPCheckup

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

```
DDSpoofer (172.25.14.123)>write-record file-server.aka.test
[*] Attempting to write DNS record for file-server.aka.test
[*] Requesting the IP 172.25.14.13 from the server
[*] Server offered 172.25.14.13
[*] Successfully leased IP 172.25.14.13 with FQDN file-server.aka.test
[*] Waiting for DNS record to update ...
[*] Successfully overwritten record
[*] Spoofing was successful, new record: file-server.aka.test → 172.25.14.13
DDSpoofer (172.25.14.123)>
```

Thank you!

@oridavid123

