Intercepter-NG
absolute capture

LDAP Relay. NTLM strikes back again.

Two years have passed since I implemented and described the so called LDAP Relay attack in Intercepter-NG, but only now I decided to write some words about it for English readers. It seems to me that this powerful vector isn't well known among information security communities outside Russia. Before we continue I suggest you to read my previous papers called ‘Actuality of SMBRelay in Modern Windows Networks’ and ‘SMB Hijacking. Kerberos is defeated’ to refresh your knowledge about NTLM stuff.

The backbone of LDAP Relay is the good old NTLM Relay with a little difference. The ‘Third Party Host’ to which we will replay credentials is the Domain Controller of the Windows Network and not a regular workstation. In case of classic SMBRelay the DC is immune and it can't be used as a target for an attack. This is due to ’SMB Signing’ option enabled by default in Group Policies. Although both attacks are almost identical, the LDAP edition is way more powerful. I was really curious why it had been left unknown for years.

In 2012 at Defcon Zack Fasel described and released his own tool for various NTLM-related attacks. One of its features was relaying to LDAP service. The ZackAttack tool was in a raw development state solely as a Proof of Concept and I wasn't able to get positive results concerning LDAP. The most interesting thing for me however was a detail he mentioned stating that Active Directory (which works as LDAP service) does not require Signing! This inspired me to make my own implementation of LDAP Relay in Intercepter-NG (though in fact this is Active Directory Relay because attack is oriented specifically for AD). I was really satisfied with the result because it works well and it is stable.

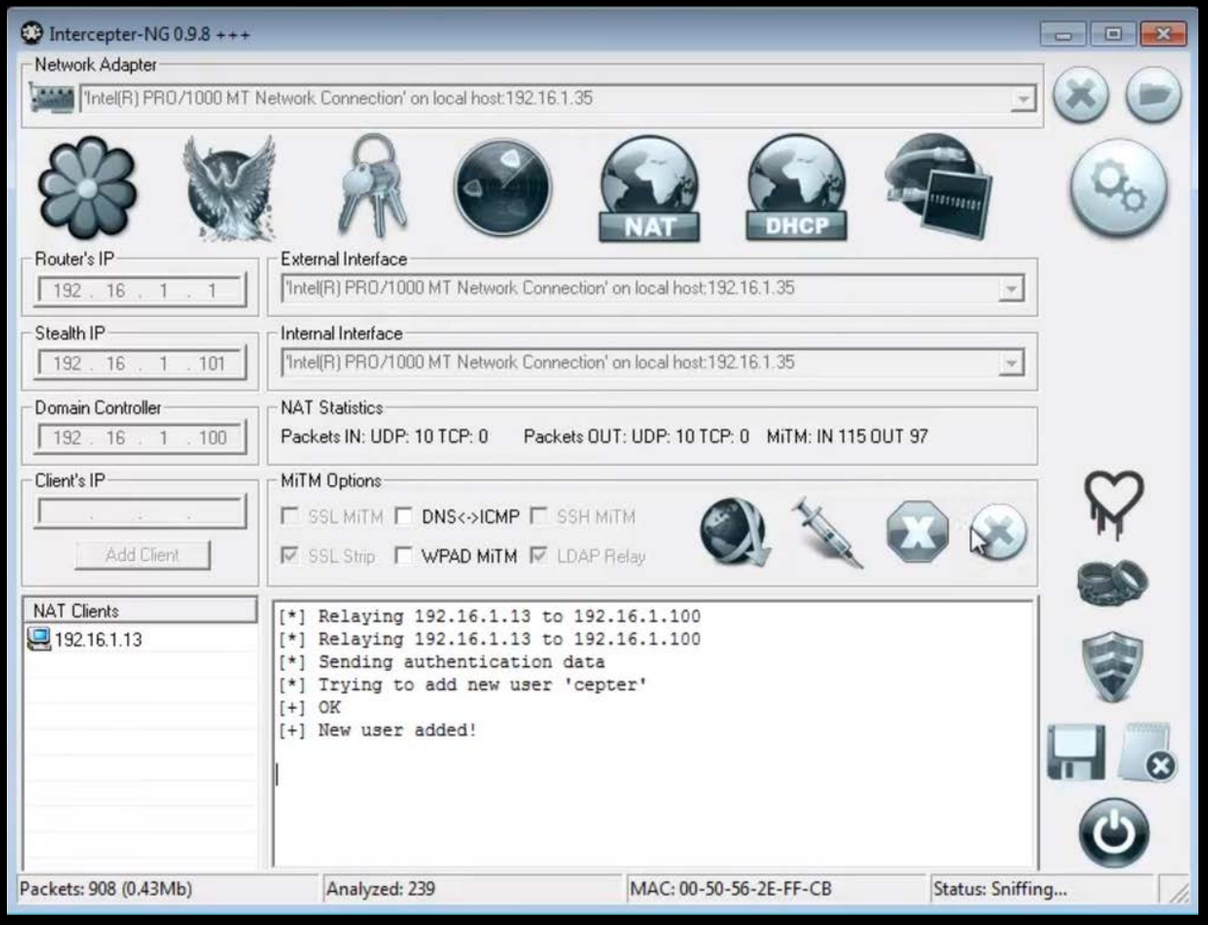
So what do we actually get by applying LDAP Relay? No matter how much I want to make a separate technical part there is actually not much to say. First we have to find the administrator’s workstation in the network and perform ARP poisoning between the admin's PC and the gateway. The searching process lies on the attacker's shoulders because there is no guaranteed automated way to find the logged in administrator if you are an unprivileged user. Then we inject a hidden link in the web traffic to our custom HTTP listener that asks for NTLM authentication. Once we get the response with credentials we redirect them to the Active Directory. After a successful attack AD is 0wned and we can do a lot of things. Currently however, Intercepter-NG only adds a new user named 'cepter' to the Domain Admins group.

LDAP Relay. NTLM strikes back again.

It was tested on different Windows Server editions (2003, 2008, 2012). To defend your own server try playing with **«Domain controller: LDAP server signing requirements»** option.

Demonstration video: https://www.youtube.com/watch?v=lexALI8Tphk

As you can see it is very elegant and easy to use and does not harm DC since it doesn't exploit critical bugs such as memory corruption. Enjoy!



LDAP Relay. NTLM strikes back again.

Contacts:

Site: http://sniff.su

Twitter: @IntercepterNG

Email: intercepter.mail@gmail.com

Blog: http://intercepter-ng.blogspot.ru

Forum: http://intercepterng.boards.net

Mirror: intercepter-ng.github.io