

Replay Attack on Kerberos V and LDAPv3

Last updated: 9th of May 2003

The vulnerability was analyzed by:

- Kimmo Kasslin, kimmo.kasslin@hut.fi
- Antti Tikkanen, antti.tikkanen@hut.fi

Vulnerability Background

This attack is very similar to the SMB replay attack we have already described in [1]. Here we try to launch the replay attack against the LDAPv3 protocol which also uses Kerberos V protocol for authentication by default on Windows 2000 environment. LDAPv3 protocol is used to access the Active Directory which contains configuration information about the domain structure, computer, user and group objects.

Attack Infrastructure

Our environment will consist of:

- Windows 2000 Professional SP3 workstation (the victim)
- Windows 2000 Server SP3 (Kerberos KDC + Active Directory)
- Red Hat Linux 8.0 (the attacker)

The network is switched. The victim and attacker will be in the same logical network segment and the server in another segment.

The servers will have basic configurations regarding Kerberos. No encryption will be used in the network layer (IPSEC).

Description of the Attack

The attack is very similar than described in [1]. The only difference is that here we catch the security blob from the LDAP bind request and use it with a modified LDAP client to launch the replay attack. Below is a description of the attack:

First we have to enable IP-packet forwarding:

```
echo '1' > /proc/sys/net/ipv4/ip_forward
```

Next we configure the kernel to redirect LDAP packets to our proxy software:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp -s <victim ip> -d <server ip> --dport 389 -j REDIRECT  
-to-port 389
```

Then we launch the ARP spoofing attack to redirect the victim's network traffic to the attacker's machine:

```
arp spoof -t <victim ip> <gateway ip>
```

Finally we start our LDAP proxy software to catch the security blob. The source code is available from [3]:

```
ldap_catchblob -s <server ip> -l <attacker's external ip> -p 389
```

After we have captured the security blob, we launch the attack by running our modified LDAP client. The patch against the samba-3.0-alpha23 is available from [4]:

```
net ads search cn=<canonical name of the user object>
```

Analysis

The attack was conducted successfully but we encountered some problems. We managed to catch the security blobs from the LDAP bind requests as easily as before and we could authenticate to the server by using the victim's identity. When we ran the LDAP search request, problems were encountered. The server did not send any response to our search query. It seems that the LDAP client used in Windows 2000 uses packet signing provided by the GSS-API framework and this information is inside the encrypted security blob, so we are not able to tamper with it. We checked this feature by trying the same attack with the Windows XP Professional, which has the option to turn off LDAP packet signing. When the signing was turned off from the client, we were able to launch the attack successfully.

Next we experimented with the scenario and made some quite interesting observations. We were able to do the LDAP replay attack without any problems by using the security blob captured from a SMB Session Setup AndX packet! A similar observation was also made for the SMB replay attack: we could launch the attack successfully by using security blobs captured from the LDAP bind requests.

Our research showed that replay attacks against LDAPv3 can be mounted in a Windows 2000 environment. A successful attack against a privileged account (domain administrator) enables the attacker to elevate his privileges, modify directory objects and even destroy the domain altogether.

References

- [1] K. Kasslin, A. Tikkanen. Replay Attack on Kerberos V and SMB.
- [2] Netfilter Org, <http://www.netfilter.org> Referenced 11.4.2003.
- [3] K. Kasslin, A. Tikkanen. ldap_catchblob.c
- [4] K. Kasslin, A. Tikkanen. Patch against samba-3.0-alpha23 for replay attacks.