Intercepter-NG
sniffing since 2006...

Actuality of SMBRelay in Modern Windows Networks

intercepter.mail@gmail.com
http://sniff.su

Intro

I first came across SMBRelay in the middle of 2000s and the experience was unsatisfying.. At that time there were only few exploits, which didn't work as good as I wished them to, despite the fact that this vulnerability is known since the end of 90s. The interest was completely lost, because I didn't get any luck with it.

But several weeks ago I got an idea to research this field once again. It appeared that nothing really changed since the last time, however new exploits emerged on the scene, so I took another attempt to test them.

For those who don't know much about this vulnerability of SMB, lets make a short introduction. An attacker is able to redirect credentials of the victim to the victim's PC itself by luring the victim to attacker's SMB resource. Thus he gets an ability to remotely execute arbitrary code via administrative service IPC$

Note that such serious vulnerability existed in it's original form till the end of 2008, up until the moment when a normally working exploit was developed.

Microsoft released a patch that prevents accepting incoming smb connection with a challenge key already used by an outgoing smb connection. It means that an attacker is no longer able to authenticate to the victim with victim's own credentials. However no patch can prevent an attack against some third-party host in the network. So if the victim has access to another host in the network, it is possible to authenticate with victim's credentials there .

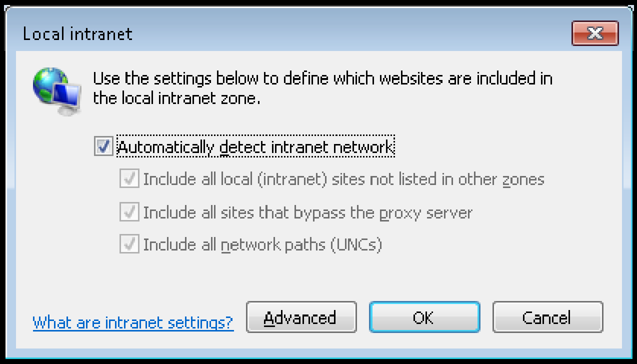
A closer look

Tarasco Security had developed an exploit called smbrelay3 (as a continuation of original smbrelay and smbrelay2). Besides the classic scheme of attack - SMB->SMB, some additional methods were added. This tool can handle NTLM authorization from such services as: HTTP\IMAP\POP3\SMTP.

With smbrelay3 I was able to run cmd.exe on unpatched Windows XP SP3 (MS08-068 was not released by that time).
No problems occurred during redirection of Windows XP on Windows 2003 (in WORKGROUP with proper credentials). Taking into account that XP is almost a part of the history the point of my interest was exploiting something more contemporary like Windows 7, which is widely used in modern networks.

With Windows 7 I faced some problems and nuances, which inspired me to write this paper. The first problem was that by default Windows 7 has a "LAN Manager authentication level" option set to "Send NTLMv2 response only". It appears that existing tools (including smbrelay3 and corresponding module of Metasploit) do not support relaying of NTLMv2. Obviously, it was not necessary earlier, so later no one found time to make the changes.

After making some changes to the source code of smbrelay3, I was able to redirect NTLMv2 authorization from Windows 7 to Windows XP. One nuance appeared, however. Windows 7 is distributed with new IE 8.0 and the problem here corresponds to the notion of ‘Intranet’. Previously, it simply meant an area of local network segment where any PC names in a view ‘my_home_pc’ were resolved to the local subnet’s IP addresses by means of NetBIOS or DNS thus making such PCs trusted to do auto-authorization with credentials of currently active session. Security settings of ‘Local Intranet’ zone in IE 8.0 have a new default option: ‘Automatically detect intranet network’. This means that the behavior and algorithm of recognizing internal network have changed. From now on the Intranet zone is not affiliated with pure local network or even Workgroup which are treated as untrusted zone. On the other hand, if a workstation is in Domain, Windows 7 automatically sends it's credentials to other members of local network, since they are marked as trusted ones.



Local intranet

Use the settings below to define which websites are included in the local intranet zone.

☑ Automatically detect intranet network

☑ Include all local (intranet) sites not listed in other zones

☑ Include all sites that bypass the proxy server

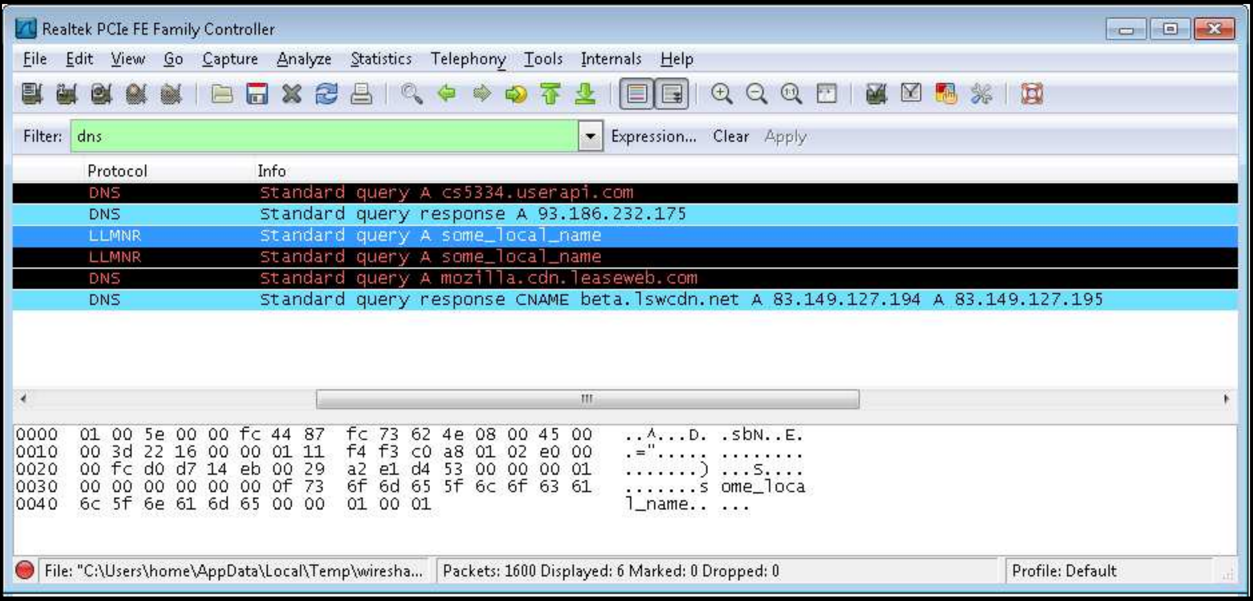
☑ Include all network paths (UNCs)

Hereby Windows 7 is not vulnerable in a Workgroup by default, but it is after joining the Domain. You may think that smbrelay allows to attack Domain Controller by redirecting credentials of user with administrative privileges to the server as a third-party host. Unfortunately, that's not possible with default configuration of Domain Controller. The reason for this is that DC requires SMB Signing for everyone who requests shared resources. In this case an attacker is unable to sign packets because he doesn't know the password and as a result NTLM hash which is needed to generate the Session Key. Domain Controller refuses this kind of unsigned connection and denies access. However sometimes administrators disable SMB Signing to increase the bandwidth and DC becomes defenseless to smbrelay.

The success of attack depends on several conditions. Victim's privileges should be able to provide access to the administrative resources IPC$ and ADMIN$. Otherwise it would not be possible to execute arbitrary code. Also as it was said before, the target host should not require SMB Signing. I think there is no reason to dig deeply into details of SMB relaying attack itself, because it had already been well described years ago, I just wanted to actualize information about it taking into account new conditions.

In addition

The only thing I have to mention additionally is that during the attack we obtain victim’s NTLM challenge\response hash (does not correspond to NTLMv2), which is suitable for bruteforce attack. Hash grabbing also can be performed by means of NBNS-Spoofing or (if we are talking about some modern Windows OS) by means of LLMNR-Spoofing. Wikipedia inform us on it: “The Link Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link. It is included in Windows Vista, Windows Server 2008 and Windows 7”. Simply stated, this is some kind of hybrid of DNS and NBNS protocols. It is used when local names need to be resolved. When the user puts ‘somename’ on the address bar, the system first attempts to resolve it using LLMNR, then by means DNS and after that using old NBNS as a last resort. So LLMNR also can be used for MiTM attacks in the local area. Although it works only with enabled ‘Network Discovery’ option.


Realtek PCIe FE Family Controller
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

Filter: dns

```
Protocol    Info
DNS         Standard query A cs5334.userapi.com
DNS         Standard query response A 93.186.232.175
LLMNR       Standard query A some_local_name
LLMNR       Standard query A some_local_name
DNS         Standard query A mozilla.cdn.leaseweb.com
DNS         Standard query response CNAME beta.lswcdn.net A 83.149.127.194 A 83.149.127.195
```

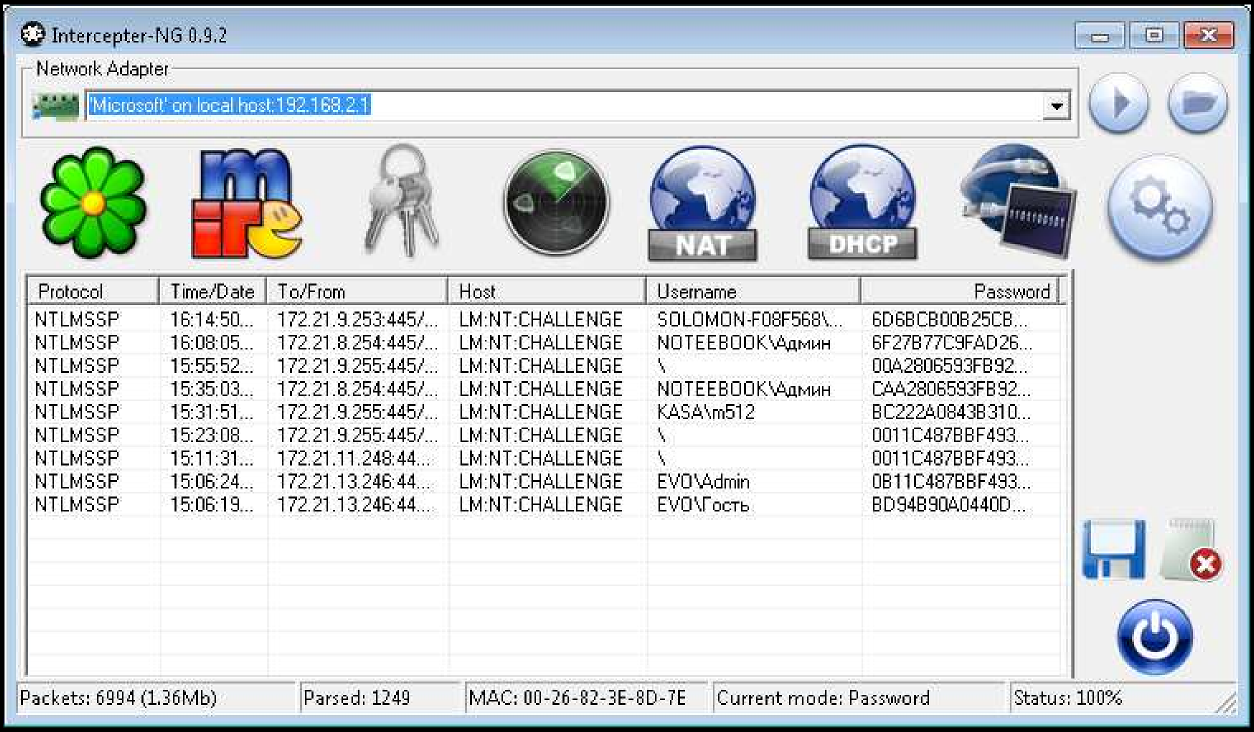
```
0000  01 00 5e 00 00 fc 44 87  fc 73 62 4e 08 00 45 00   ..^...D. .sbN..E.
0010  00 3d 22 16 00 00 01 11  f4 f3 c0 a8 01 02 e0 00   .="..... ........
0020  00 fc d0 d7 14 eb 00 29  a2 e1 d4 53 00 00 00 01   .......) ...S....
0030  00 00 00 00 00 00 0f 73  6f 6d 65 5f 6c 6f 63 61   .......s ome_loca
0040  6c 5f 6e 61 6d 65 00 00  01 00 01                  l_name.. ...
```

File: "C:\Users\home\AppData\Local\Temp\wiresha... Packets: 1600 Displayed: 6 Marked: 0 Dropped: 0 Profile: Default

What’s done

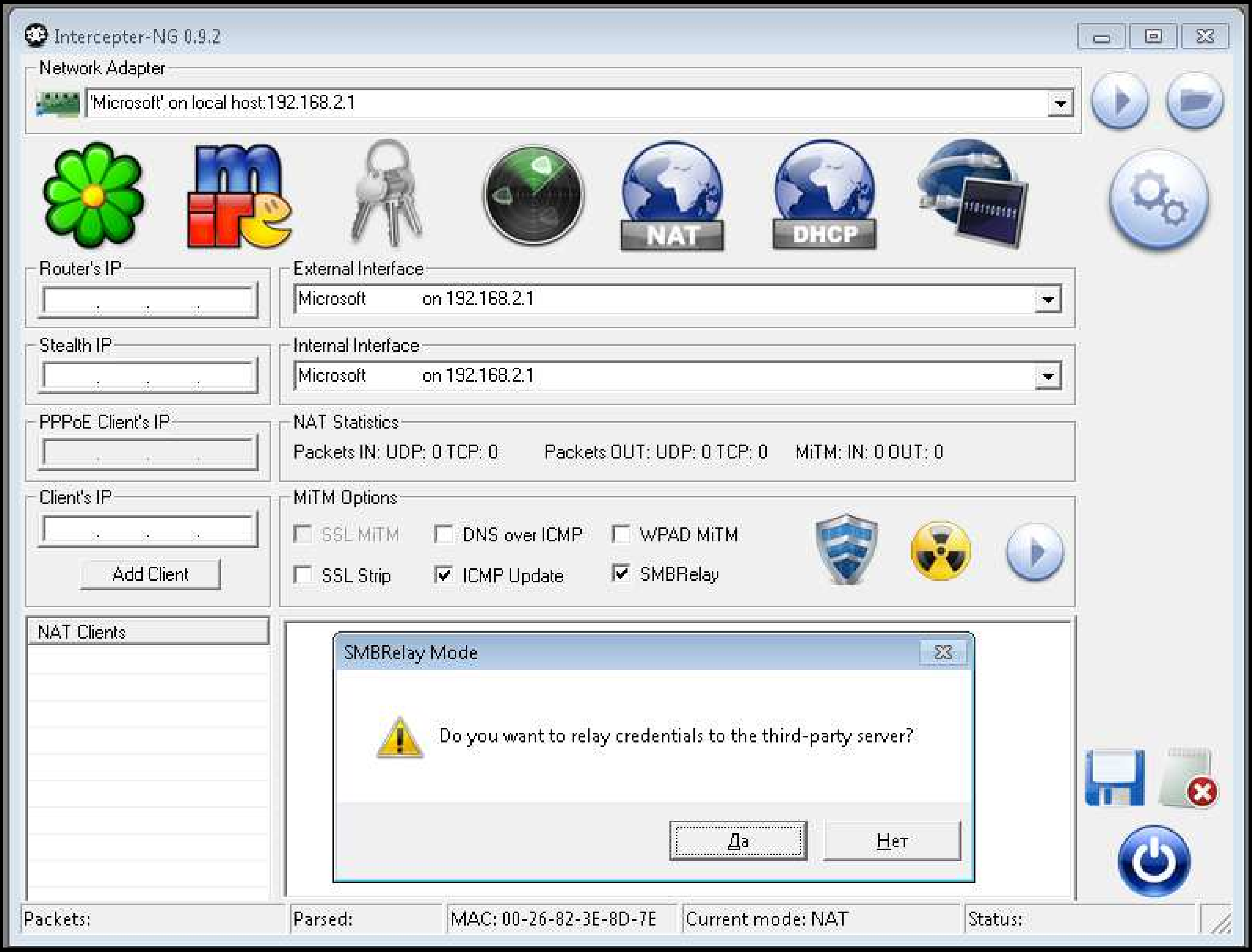
The result of this research is a modern and stable tool to perform SMBRelay against both old and new versions of Windows. It has become a part of Intercepter-NG amongst other MiTM attacks. To avoid difficulties with running the “Server” service on 445 port, Intercepter-NG uses HTTP->SMB method to accept incoming connection from the web browser and offer NTLM authorization which is then relayed either onto the victim himself or to the third-party host.

The basic problem has always been luring the victim into a malicious resource of the attacker. Usually it’s done by sending an e-mail message with malicious link or by uploading malicious file on a public shared resource. Rarely it is achieved by injecting a link into the victim’s http traffic (by means of MiTM attack). In case of Intercepter-NG, the last method is selected as the fastest and most effective. To perform an smbrelay attack with Intercepter-NG you have to choose target host (-s) or, if needed, a third-party host, and then run the process (an example is shown on the video demonstration). Next steps are done automatically: start arp-poison attack, inject malicious link into the victim’s http traffic, redirect authorization and execute cmd.exe. Note that by default NTLM auto-authorization works only with IE\Chrome, and in FireFox it has to be enabled manually.



Protocol	Time/Date	To/From	Host	Username	Password
NTLMSSP	16:14:50...	172.21.9.253:445/...	LM:NT:CHALLENGE	SOLOMON-F08F568\...	6D6BCB00B25CB...
NTLMSSP	16:08:05...	172.21.8.254:445/...	LM:NT:CHALLENGE	NOTEEBOOK\Админ	6F27B77C9FAD26...
NTLMSSP	15:55:52...	172.21.9.255:445/...	LM:NT:CHALLENGE	\	00A2806593FB92...
NTLMSSP	15:35:03...	172.21.8.254:445/...	LM:NT:CHALLENGE	NOTEEBOOK\Админ	CAA2806593FB92...
NTLMSSP	15:31:51...	172.21.9.255:445/...	LM:NT:CHALLENGE	KASA\m512	BC222A0843B310...
NTLMSSP	15:23:08...	172.21.9.255:445/...	LM:NT:CHALLENGE	\	0011C487BBF493...
NTLMSSP	15:11:31...	172.21.11.248:44...	LM:NT:CHALLENGE	\	0011C487BBF493...
NTLMSSP	15:06:24...	172.21.13.246:44...	LM:NT:CHALLENGE	EVO\Admin	0B11C487BBF493...
NTLMSSP	15:06:19...	172.21.13.246:44...	LM:NT:CHALLENGE	EVO\Гость	BD94B90A0440D...

Packets: 6994 (1.36Mb) | Parsed: 1249 | MAC: 00-26-82-3E-8D-7E | Current mode: Password | Status: 100%



Network Adapter: 'Microsoft' on local host:192.168.2.1

Router's IP: . . .

Stealth IP: . . .

PPPoE Client's IP: . . .

Client's IP: . . .

External Interface: Microsoft on 192.168.2.1

Internal Interface: Microsoft on 192.168.2.1

NAT Statistics

Packets IN: UDP: 0 TCP: 0 Packets OUT: UDP: 0 TCP: 0 MiTM: IN: 0 OUT: 0

MiTM Options

□ SSL MiTM □ DNS over ICMP □ WPAD MiTM

□ SSL Strip ☑ ICMP Update ☑ SMBRelay

SMBRelay Mode

Do you want to relay credentials to the third-party server?

Packets: | Parsed: | MAC: 00-26-82-3E-8D-7E | Current mode: NAT | Status:

Conclusion

SMBRelay is an actual security problem even today, and in evil hands it can be a serious weapon for network invasion. To protect ordinary users from this attack it is necessary to enable SMB Signing option by editing the registry values: “EnableSecuritySignature" and "RequireSecuritySignature”. Information presented here is only for educational purposes. The author is not responsible for any kind of injury caused by this material.

References

1. Basic knowledge about SMBRelay
http://en.wikipedia.org/wiki/SMBRelay

2. smbrelay3 by Tarasco Security
http://www.tarasco.org/security/smbrelay/index.html

3. NTLM is Dead – nice paper about smbrelay
http://code.google.com/p/squirtle/

4. Intercepter-NG
http://sniff.su/

Thanks to Alex S. for correction work. Take care.