Investigation of Authentication Abuse

Degree programme : MAS Digital Forensics & Cyber Investigation

By reproducing case studies of authentication abuse techniques targeting a Windows domain environment, this Master Thesis aims to answer the following questions: Which current attack methods are relevant? What kind of traces and artifacts can be recovered? Which Indicators of Compromise can be detected and how?

Introduction

A cybersecurity advisory released by the National Security Agency (NSA) and an activity alert released by the Cybersecurity & Infrastructure Security Agency (CISA), both focus on recently discovered authentication abuse techniques targeting government agencies, critical infrastructure, and private sector organizations. Based on these publications, this report aims to document and forensically analyze the most prevalent and currently used authentication abuse techniques targeting a Windows domain environment.

Lab Environment

To reproduce the authentication abuse case studies, a dedicated Windows domain lab environment was deployed, including a domain controller, a fileserver with restricted domain resources and a compromised member server. To forensically analyze the conducted authentication abuse techniques, a centralized logging system was implemented using a dedicated Splunk indexer. To simplify the management of the server infrastructure, the lab environment was built and run on a ESXi hypervisor using virtual machines.

Windows Authentication Architecture

To understand the capabilities of a deployed authentication abuse technique, basic knowledge of the Windows Authentication Architecture and the process of a Kerberos authentication is required. Therefore, a chapter was dedicated to conveying this knowledge.

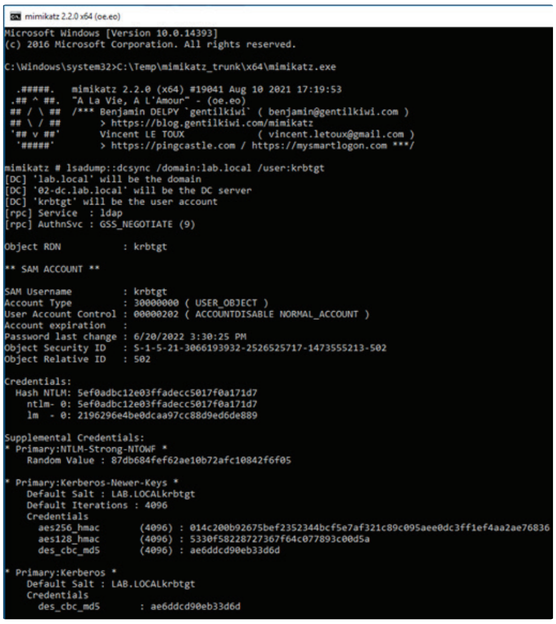
Case Studies

Relevant authentication abuse techniques and their functionality were researched and documented using the MITRE ATT&CK knowledge base and other viable resources. Potential procedure examples and the respective case studies were evaluated and replicated on the dedicated Windows domain lab environment. The case studies conducted include techniques such as Pass the Hash, Pass the Ticket, Golden & Silver Ticket, Kerberoasting, DCSync and other prevalent attack procedures.

Detection & Conclusion

By focusing on behavioral analysis of the techniques instead of searching for malware or toolkit specific traces, it is possible to detect the deployed technique independent of the used procedure or obfuscation techniques. Locard‘s exchange principle, which states that a criminal will always leave a trace behind when entering a crime scene, also holds true for authentication abuse techniques. Most of the techniques were detectable by log correlation of either suspicious or wrongfully missing events. Where log forensics was not viable, traces were detectable by other means, e.g., network forensics during a DCSync attack.

Severin Hintermann



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>C:\Temp\mimikatz_trunk\x64\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::dcsync /domain:lab.local /user:krbtgt
[DC] 'lab.local' will be the domain
[DC] '02-dc.lab.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 6/20/2022 3:30:25 PM
Object Security ID   : S-1-5-21-3066193932-2526525717-1473555213-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 5ef0adbc12e03ffadecc5017f0a171d7
    ntlm- 0: 5ef0adbc12e03ffadecc5017f0a171d7
    lm  - 0: 2196296e4be0dcaa97cc88d9ed6de889

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 87db684fef62ae10b72afc10842f6f05

* Primary:Kerberos-Newer-Keys *
    Default Salt : LAB.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 014c200b92675bef2352344bcf5e7af321c89c095aee0dc3ff1ef4aa2ae76836
      aes128_hmac       (4096) : 5330f58228727367f64c077893c00d5a
      des_cbc_md5       (4096) : ae6ddcd90eb33d6d

* Primary:Kerberos *
    Default Salt : LAB.LOCALkrbtgt
    Credentials
      des_cbc_md5       : ae6ddcd90eb33d6d
```

Mimikatz DCSync