Cloud Forensics

Team: Josh Mpere, Sam Mendimasa, Nikola Slavov

Sponsor: Al Holt with National Security Agency

Advisor: Dr. Haibin Zhang

Agenda

- Problem Statement
- Project Overview & Plan
- Cloud Computing
- Memory Forensics
- Results and Findings
- Future Work

Introduction / Problem Statement

- Problem: When a cloud instance is terminated all the data that was stored locally on that instance is deleted. So in the case of a compromise no evidence is preserved.
- Goal: To provide a way to perform digital forensics on instances in the cloud.

Project Description

- Design a framework that collects memory and data from VMs before the instance gets terminated

- Conduct forensics analysis and determine what malicious activities occurred.

- Develop metrics of amount of information that is collected from a cloud environment with different forensic tools

Tools & Background

- Devstack Rocky and Stein
- Virtualbox
- Kali linux
- Volatility
- Dumpit

Our Ideal Setup

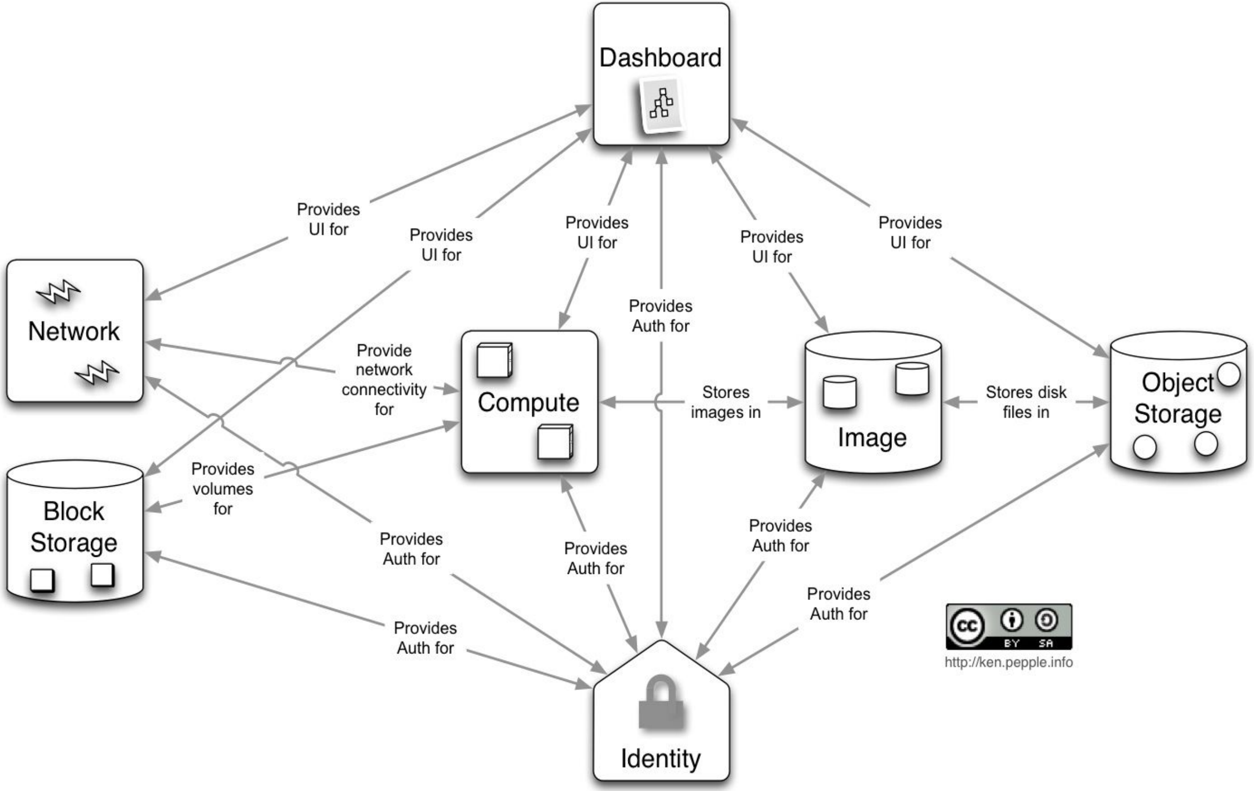
1. In practice we would have 3 virtual machines setup.
   a. End user
   b. Attacker
   c. Forensic analyst
2. The end user on a
3. The forensic analyst will be on a separate network offline.

Cloud Computing

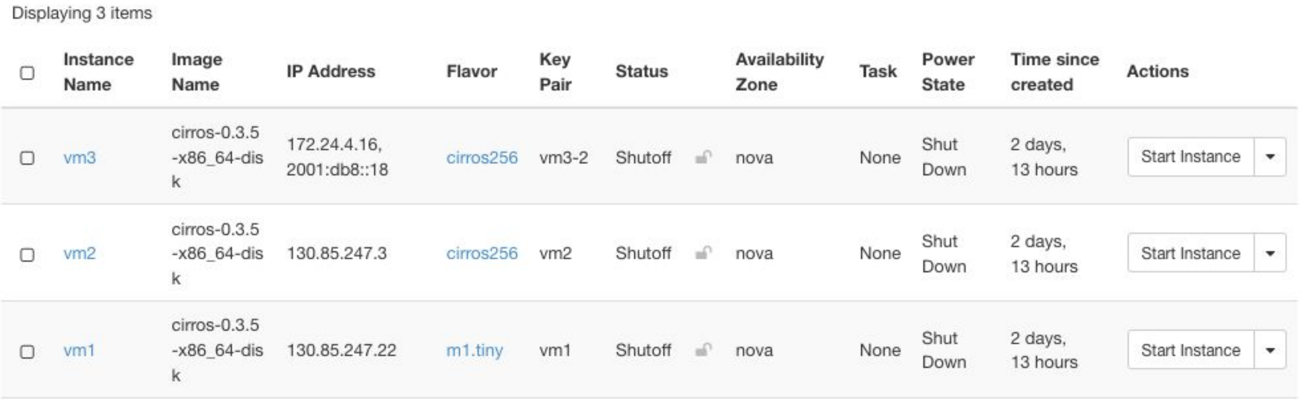
- Delivery of computing services, ex. virtualization, servers, storage, databases, software, and more.
- IaaS (Infrastructure as a Service), SaaS(Software as a Service), PaaS(Platform as a Service)
- Examples: Amazon AWS, OpenStack, Google Cloud Platform
- Benefits:
  - Flexibility, Full control, Scalability, and Security

Devstack Framework

- Open source platform for cloud computing
- Used by over 500+ companies as basis for their private cloud
- Devstack is single server variant of Openstack

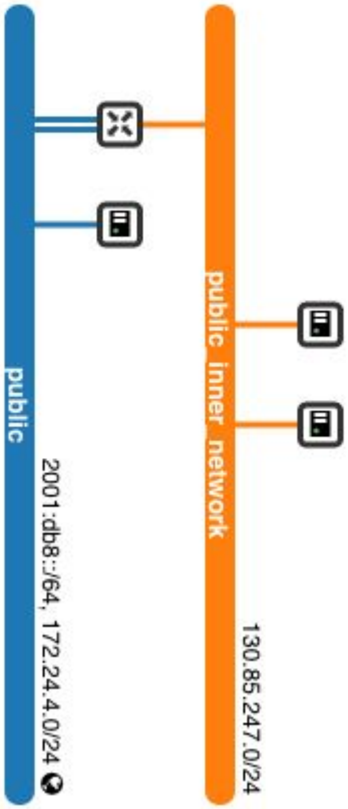


Cloud Framework



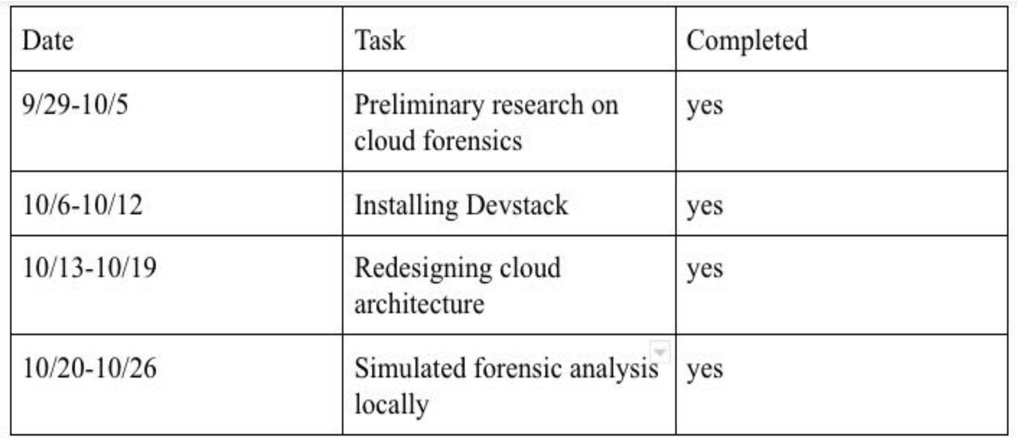
Displaying 3 items

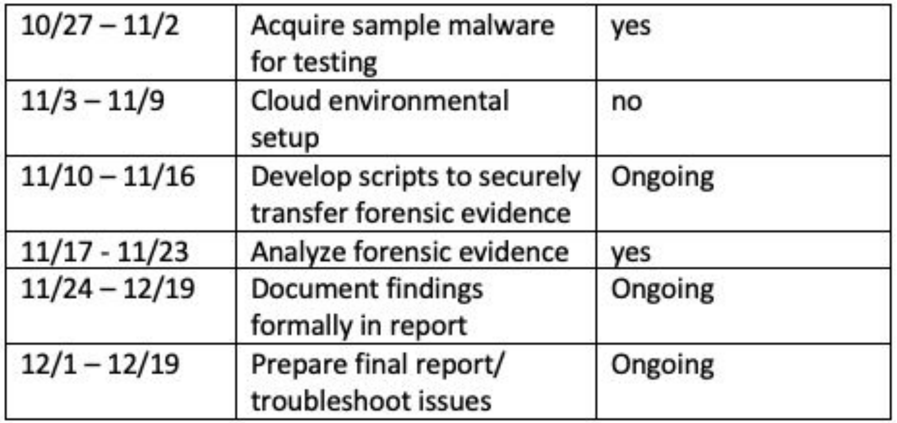
□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status		Availability Zone	Task	Power State	Time since created	Actions
□	vm3	cirros-0.3.5-x86_64-disk	172.24.4.16, 2001:db8::18	cirros256	vm3-2	Shutoff		nova	None	Shut Down	2 days, 13 hours	Start Instance ▾
□	vm2	cirros-0.3.5-x86_64-disk	130.85.247.3	cirros256	vm2	Shutoff		nova	None	Shut Down	2 days, 13 hours	Start Instance ▾
□	vm1	cirros-0.3.5-x86_64-disk	130.85.247.22	m1.tiny	vm1	Shutoff		nova	None	Shut Down	2 days, 13 hours	Start Instance ▾



Resources: 100+ gb storage, 6 gb RAM

What we did?



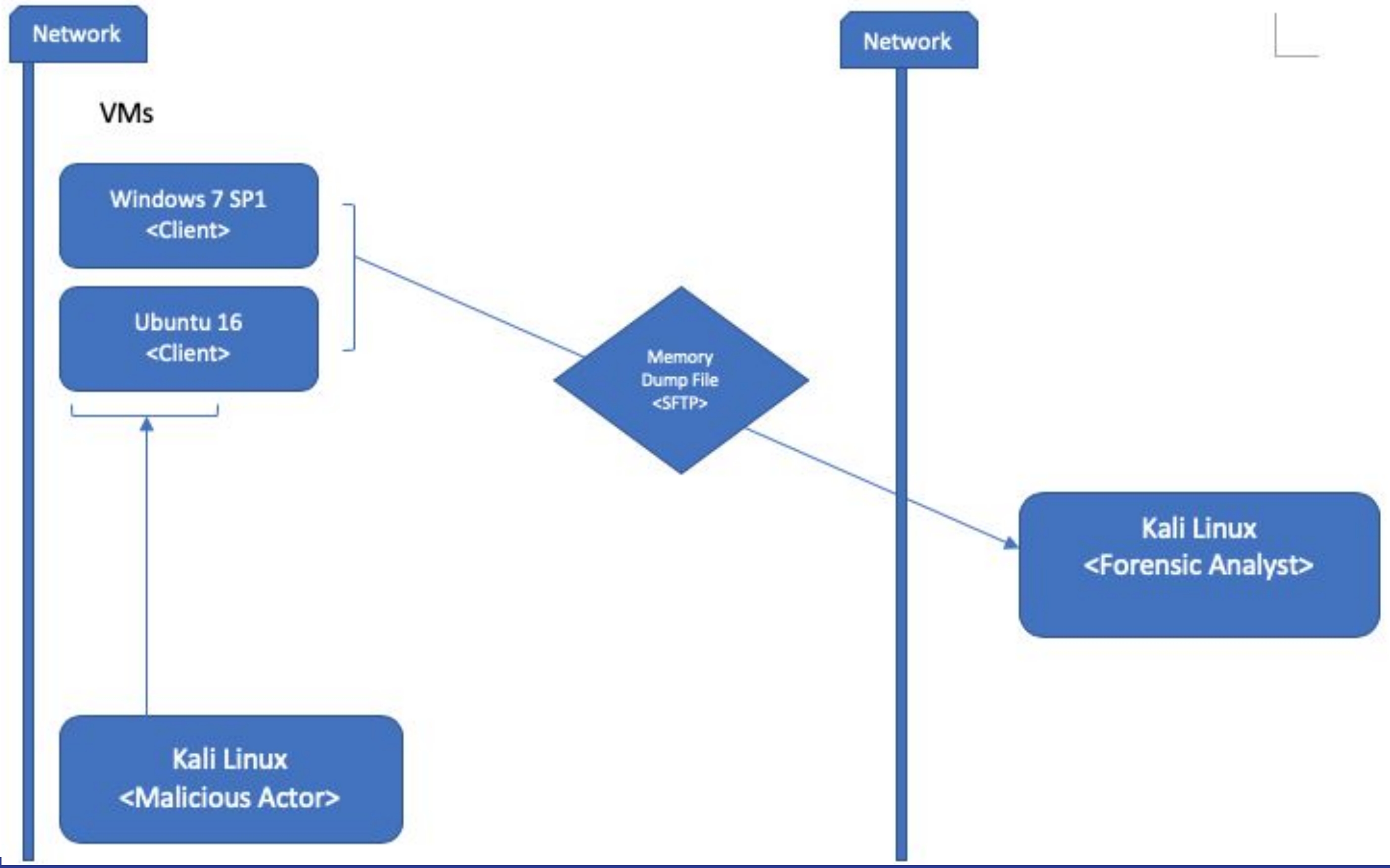


Date	Task	Completed
9/29-10/5	Preliminary research on cloud forensics	yes
10/6-10/12	Installing Devstack	yes
10/13-10/19	Redesigning cloud architecture	yes
10/20-10/26	Simulated forensic analysis locally	yes
10/27 – 11/2	Acquire sample malware for testing	yes
11/3 – 11/9	Cloud environmental setup	no
11/10 – 11/16	Develop scripts to securely transfer forensic evidence	Ongoing
11/17 - 11/23	Analyze forensic evidence	yes
11/24 – 12/19	Document findings formally in report	Ongoing
12/1 – 12/19	Prepare final report/ troubleshoot issues	Ongoing

Cloud Framework Concerns

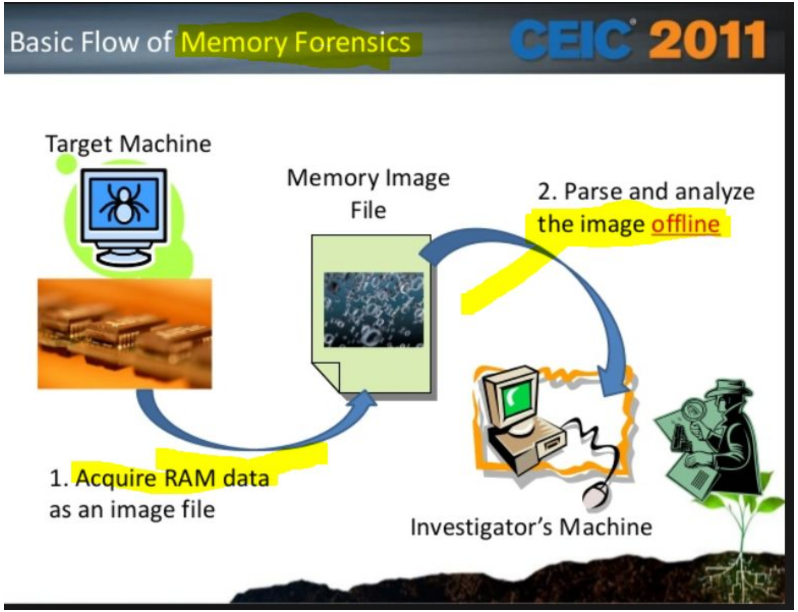
- Failed instance loading
- No connection to the outside Internet (UMBC Network blocks ICMP and connections to outside networks)
- Attempted workarounds:
  - Load malicious image to attack other instances
  - Load a compromised image from a snapshot
- Solution: use VirtualBox to simulate a cloud

Virtual Box Design



What is Memory Forensics?

- Memory forensics refers to the analysis of the volatile data of a computer contained it its memory dump.
- This occurs when one acquires the ram from a machine and is able to analyze that file offline.

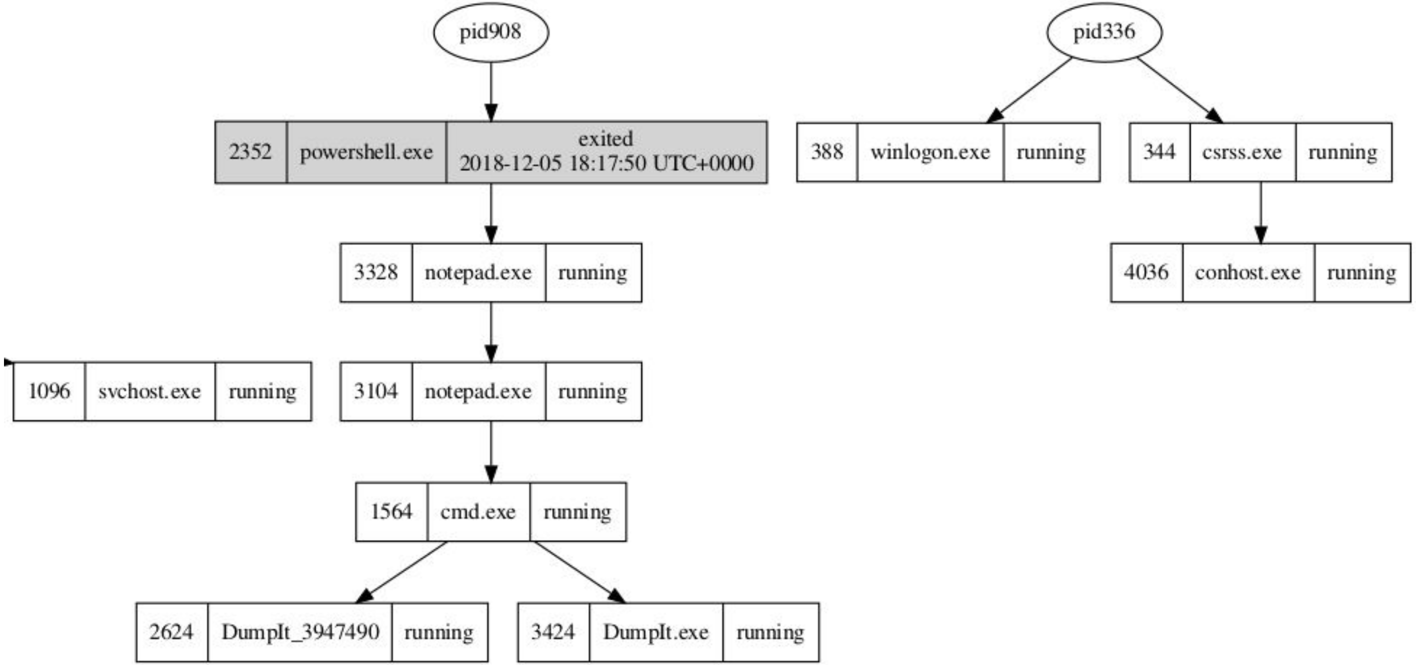

Basic Flow of Memory Forensics
CEIC 2011
Target Machine
Memory Image File
2. Parse and analyze the image offline
1. Acquire RAM data as an image file
Investigator's Machine

Why Forensics is important

- Processes must be loaded into memory(“you can run but you can’t hide”)
- The memory can provide insights into system activity at runtime.
- Some data related to the attack exists solely in memory

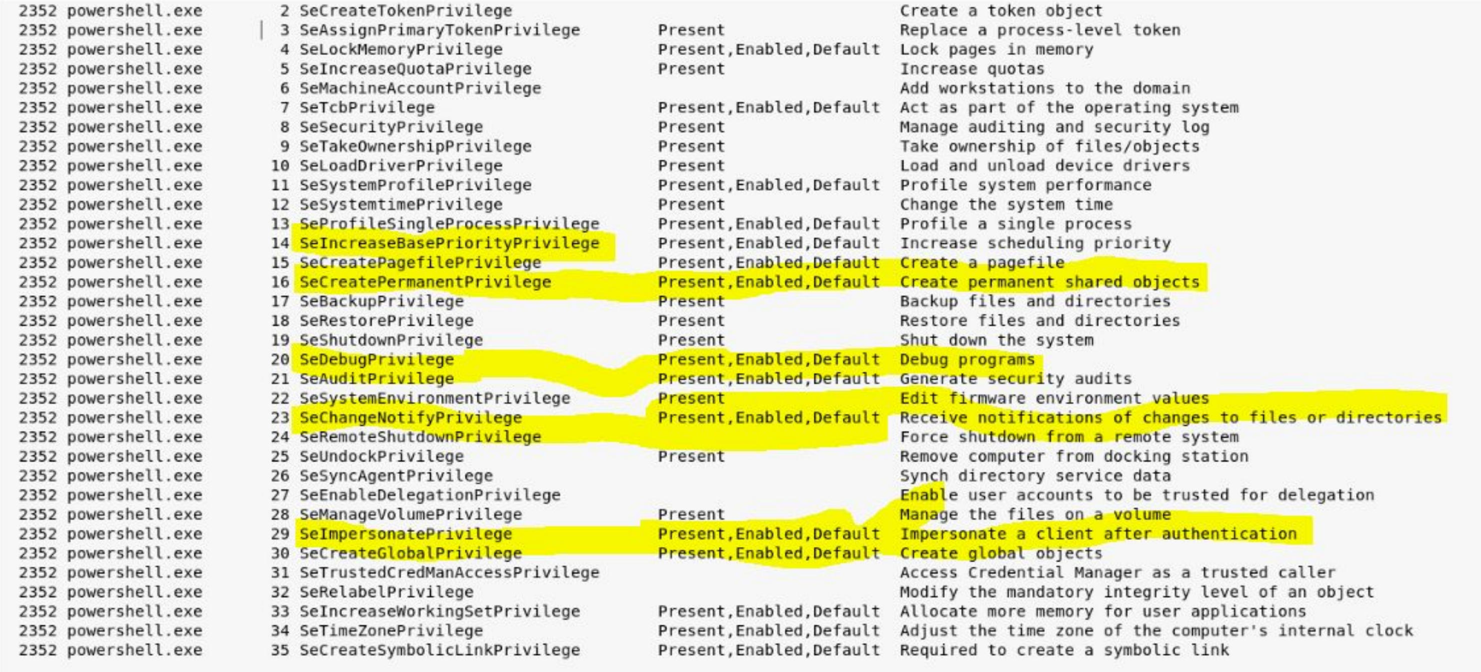
Results / Findings

This graph shows the parent-child relationship of the processes spawned by the malicious actor.


pid908
2352 | powershell.exe | exited 2018-12-05 18:17:50 UTC+0000
3328 | notepad.exe | running
3104 | notepad.exe | running
1564 | cmd.exe | running
2624 | DumpIt_3947490 | running
3424 | DumpIt.exe | running
1096 | svchost.exe | running
pid336
388 | winlogon.exe | running
344 | csrss.exe | running
4036 | conhost.exe | running

Results / Findings

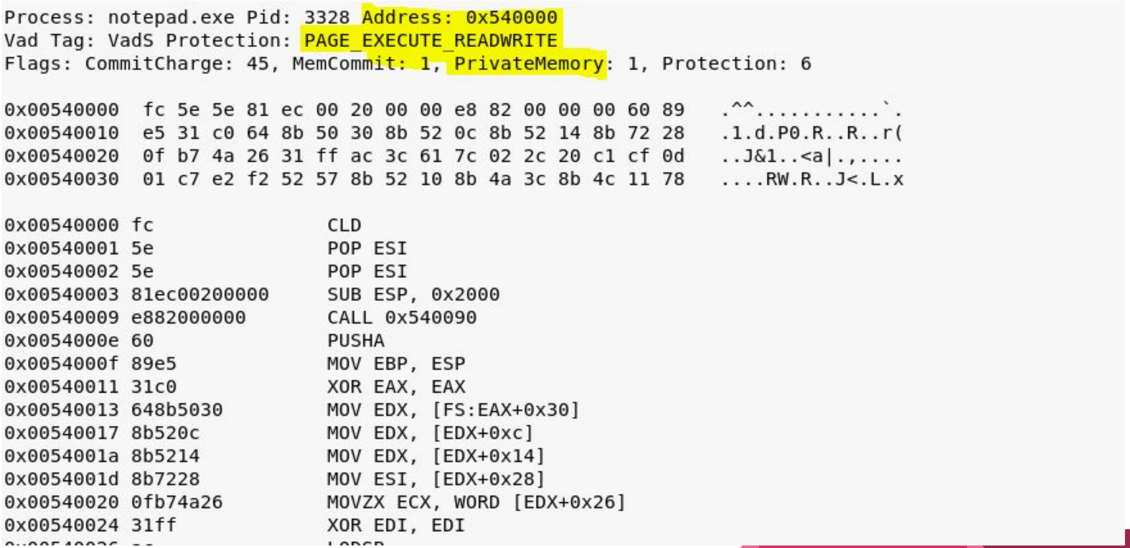
- Here we used the privs plugin to determine privileges gained by the attacker.



```
2352 powershell.exe        2 SeCreateTokenPrivilege                                         Create a token object
2352 powershell.exe        3 SeAssignPrimaryTokenPrivilege        Present                   Replace a process-level token
2352 powershell.exe        4 SeLockMemoryPrivilege                Present,Enabled,Default  Lock pages in memory
2352 powershell.exe        5 SeIncreaseQuotaPrivilege             Present                   Increase quotas
2352 powershell.exe        6 SeMachineAccountPrivilege                                      Add workstations to the domain
2352 powershell.exe        7 SeTcbPrivilege                       Present,Enabled,Default  Act as part of the operating system
2352 powershell.exe        8 SeSecurityPrivilege                  Present                   Manage auditing and security log
2352 powershell.exe        9 SeTakeOwnershipPrivilege             Present                   Take ownership of files/objects
2352 powershell.exe       10 SeLoadDriverPrivilege                Present                   Load and unload device drivers
2352 powershell.exe       11 SeSystemProfilePrivilege             Present,Enabled,Default  Profile system performance
2352 powershell.exe       12 SeSystemtimePrivilege                Present                   Change the system time
2352 powershell.exe       13 SeProfileSingleProcessPrivilege      Present,Enabled,Default  Profile a single process
2352 powershell.exe       14 SeIncreaseBasePriorityPrivilege      Present,Enabled,Default  Increase scheduling priority
2352 powershell.exe       15 SeCreatePagefilePrivilege            Present,Enabled,Default  Create a pagefile
2352 powershell.exe       16 SeCreatePermanentPrivilege           Present,Enabled,Default  Create permanent shared objects
2352 powershell.exe       17 SeBackupPrivilege                    Present                   Backup files and directories
2352 powershell.exe       18 SeRestorePrivilege                   Present                   Restore files and directories
2352 powershell.exe       19 SeShutdownPrivilege                  Present                   Shut down the system
2352 powershell.exe       20 SeDebugPrivilege                     Present,Enabled,Default  Debug programs
2352 powershell.exe       21 SeAuditPrivilege                     Present,Enabled,Default  Generate security audits
2352 powershell.exe       22 SeSystemEnvironmentPrivilege         Present                   Edit firmware environment values
2352 powershell.exe       23 SeChangeNotifyPrivilege              Present,Enabled,Default  Receive notifications of changes to files or directories
2352 powershell.exe       24 SeRemoteShutdownPrivilege                                      Force shutdown from a remote system
2352 powershell.exe       25 SeUndockPrivilege                    Present                   Remove computer from docking station
2352 powershell.exe       26 SeSyncAgentPrivilege                                           Synch directory service data
2352 powershell.exe       27 SeEnableDelegationPrivilege                                    Enable user accounts to be trusted for delegation
2352 powershell.exe       28 SeManageVolumePrivilege              Present                   Manage the files on a volume
2352 powershell.exe       29 SeImpersonatePrivilege               Present,Enabled,Default  Impersonate a client after authentication
2352 powershell.exe       30 SeCreateGlobalPrivilege              Present,Enabled,Default  Create global objects
2352 powershell.exe       31 SeTrustedCredManAccessPrivilege                                Access Credential Manager as a trusted caller
2352 powershell.exe       32 SeRelabelPrivilege                                             Modify the mandatory integrity level of an object
2352 powershell.exe       33 SeIncreaseWorkingSetPrivilege        Present,Enabled,Default  Allocate more memory for user applications
2352 powershell.exe       34 SeTimeZonePrivilege                  Present,Enabled,Default  Adjust the time zone of the computer's internal clock
2352 powershell.exe       35 SeCreateSymbolicLinkPrivilege        Present,Enabled,Default  Required to create a symbolic link
```

Findings

- Using the malfind plugin we found code injected into other processes.



```
Process: notepad.exe Pid: 3328 Address: 0x540000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 45, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00540000  fc 5e 5e 81 ec 00 20 00 00 e8 82 00 00 00 60 89   .^^...........`.
0x00540010  e5 31 c0 64 8b 50 30 8b 52 0c 8b 52 14 8b 72 28   .1.d.P0.R..R..r(
0x00540020  0f b7 4a 26 31 ff ac 3c 61 7c 02 2c 20 c1 cf 0d   ..J&1..<a|.,....
0x00540030  01 c7 e2 f2 52 57 8b 52 10 8b 4a 3c 8b 4c 11 78   ....RW.R..J<.L.x

0x00540000 fc               CLD
0x00540001 5e               POP ESI
0x00540002 5e               POP ESI
0x00540003 81ec00200000     SUB ESP, 0x2000
0x00540009 e882000000       CALL 0x540090
0x0054000e 60               PUSHA
0x0054000f 89e5             MOV EBP, ESP
0x00540011 31c0             XOR EAX, EAX
0x00540013 648b5030         MOV EDX, [FS:EAX+0x30]
0x00540017 8b520c           MOV EDX, [EDX+0xc]
0x0054001a 8b5214           MOV EDX, [EDX+0x14]
0x0054001d 8b7228           MOV ESI, [EDX+0x28]
0x00540020 0fb74a26         MOVZX ECX, WORD [EDX+0x26]
0x00540024 31ff             XOR EDI, EDI
```

Conclusion and Future Work

- Memory dumps proved to be an effective way to detect malware in cloud environments.
- Look into other forensics tools to analyze cloud related cyber crime
- Design another Framework to address problems faced by forensic investigators in cloud computing.
- Further looking into configuring Devstack

Questions?