Incident Response

Prepearation

In the wake of an incident, your client will give you the news that a suspicious activity is taking place on a machine in their system.
The preparation phase involves preparing the following

```
- One laptop with kali linux, windows and SIFT installed where you can switch between systems at boot
- A bunch of external hard drives
- Bootable USB keys for linux and windows OS
- Another set of USB keys for forensic tools both on linux and windows.
- Toolkit containing tools such as screwdrivers
- USB adapters of all kinds
- Ethernet cables
- Physical write blocker for forensic copies.
```

Gathering Details

Gather details about the incident from the staff who noticed it. Collect documents about the system architecture and network topology in addition to the contact details of the IT department. It's also important to understand the role of the machine that was under the attack to make a preliminary assessment about the nature of the situation.

Conducting the investigation

Never do the following below:

```
- Its important not to perform any
operation on the machine before you do a
full memory and disk copy according to
forensic standards. Forensic standards
state that a full bit by bit copy of the
RAM and disk should be performed in
addition to any available snapshots.

- Never use any of the tools on the
infected machine while its in live state.
```

[Two scenarios are possible]
1- The machine is an endpoint machine and not a public facing server
2- The machine is a public facing server for business operations

The machine is an endpoint machine and not a public facing server

Perform full forensic analysis

The steps below are taken in order to conduct full forensic analysis

```
1- Full bit by bit copy of the RAM should be performed in addition to any available snapshots.
2- A usb key with forensic tools to grap open files, running processes, network connections,etc should be available to start the live forensics. Make sure all artifacts are hashed and timestamped so that evidence will be admissible in court and also make sure to document all steps taken in the forensic analysis so that you make an admissible chain of custody.
```

```
3- Full physical disk copy. On Linux that
corresponds to /dev/sda and on windows it
corresponds to \\.\PHYSICALDRIVE0/. The
physical copy can be taken after shutting
down the computer by unplugging the power
cable.Physical copies are taken bit by bit
using a software such as FTK Imager or
Encase. Make sure you connect the hard
drive to external write blocker to
preserve the integrity while connecting it
to your investigation computer using a USB
cable.
4- Once RAM is copied and once artifacts
are collected, you can use the USB on a
clean machine prepared for this purpose.
5- Make sure to have backups copies of the
collected data stored in additional USB
keys.
6- Start the analysis with the live
captured data. System configs, network
configs,etc.
```

Regarding [step 2] Dumplt is preferable to have for RAM acquisition. You can use this tool to take a memory dump of the machine as well.

[About Live System Forensics]
Don't perform any live machine forensics untill you take a bit by bit copy of the physical Disk and RAM using acquisition and imaging tools. The output of live forensic tools such as netstat,process hacker,etc is not reliable on an infected machine. Some malwares and rootkits operate on the kernel mode which means they can alter the state of any process or tool installed on the operating system. That's why we do a bit by bit copy then we do live system forensics using our own tools installed on an external USB. To reveal malware behaviour, we compare the output of the analysis between the two methods to decide whether the malware was tampering with OS data.
[Artifcats to collect when doing live forensic]

```
1- System info
2- network configs
3- Users
4- Active and listening connections
5- Running processes
6- Jouranl events
```

These artifacts are stored in a USB drive and copied into another three USB drives. Don't connect the

USB into a production machine. Remember to use a freshly installed machine for only analysis purposes.
[How to spot a suspicious process]

```
1- Process running with wrong parent process. Example would be the authentication manager lsass.exe running as a child process of explorer.exe

2- Process executable running from suspicious locations such as c:\temp or c:\users\

3- Misspelled processes.

4- Process with long command line containing weird or encoded characters and URLs.
```

#Note What if the machine infected is a virtual machine part of a Hyper-V or ESXi Node?
In the above case, we follow the below steps

```
1- Use Vsphere client to connect to the main ESXi node and list all the available virtual machines
2- Copy The VMDK file which is a full copy of the hard drive of the targeted virtual machine
3- Suspened the virtual machine to create a snapshot file VMSS that you can merge with the paging file VMEM.
```

To achieve step 3 above, issue the below command

```
vmss2core-sb.exe -W8 "machine.vmem" "machine.vmss"
```

The output of the above command is a memory dump you can inspect with Volatility.

Cut Internet access on the machine

Eradication and Recovery

After you have discovered how the incident occured and created your infection timeline, you have two set of steps to follow for the eradication. #The below steps can be taken in order if the

attacker managed to get access only to one machine which is the infected machine

```
- Identify backdoors first. Could be reverse shells or bind shells. Reverse shells can be found easily in firewall logs. Just look for a pattern of an outgoing connection to a recurring IP address. For bind shells, it is usually a listening point or active listening connection therefore nmap scan of the infected machine should reveal all open listening ports. Correlate nmap scan results with netstat issued on the machine to look for common points or discrepanies. If you find a weird listening port, then see if it's listed to start on boot which raises the chacnes of it being a bind shell.Lastly shut down the port and disable the service that was running on it.
- Look for files modified around the time of the incident with two hours difference.
-Revoke any unauthorized account created
-Patch all vulnerabilities that caused
```

privileged escalation or foothold access
-Reset passwords for all accounts in the machine
-Perform full rootkit and antivirus scan. In some instances, you may need to fully resotre from a previous safe state or do a full format
- If you have discovered IOCs, then look them up on all machines and domain controllers. Use powershell to retrieve events containing one of the IOCs so you can decide on which machines need eradication and recovery.Also lookup firewalls and network devices with C2C2 addresses to find which machines on the network communicated with the attacker's C2C.
- Create a blacklist of C2C IPs and block it using the firewall.
- Create and Install fresh windows copies for infected machines.Be very careful when copying important documents before installing fresh windows copies. Exculde dangerous extension from you backup such

```
as the below ones
.cs','*.ps1','*.psm','*.exe','*.com','*.dl
l','*.vbs','*.vbe','*.js','*.hta','*.msi',
'*.msp','*.csh','*.cpl','*.bat
- Reset all users' passwords especially in
Windows Active directory including the
KRBTGT and DSRM account twice.
- Clone AD into a new clean windows server
domain controller.
```

The machine is a public facing server for business operations

Perform full forensic analysis

The steps below are taken to conduct full forensic analysis

```
1- Full bit by bit copy of the RAM should
be performed in addition to any available
snapshots.
2- A usb key with forensic tools to grap
open files, running processes, network
connections,etc should be available to
start the live forensics. Make sure all
```

artifacts are hashed and timestamped so that evidence will be admissible in court and also make sure to document all steps taken in the forensic analysis so that you make an admissible chain of custody.
3- Full physical disk copy. On Linux that corresponds to /dev/sda and on windows it corresponds to \\.\PHYSICALDRIVE0/. The physical copy can be taken after shutting down the computer by unplugging the power cable.Physical copies are taken bit by bit using a software such as FTK Imager or Encase. Make sure you connect the hard drive to external write blocker to preserve the integrity while connecting it to your investigation computer using a USB cable.
4- Once RAM is copied and once artifacts are collected, you can use the USB on a clean machine prepared for this purpose.
5- Make sure to have backups copies of the collected data stored in additional USB keys.
6- Start the analysis with the live

```
captured data. System configs, network
configs,etc.
```

Regarding [step 2] Dumplt is preferable to have for RAM acquisition. You can use this tool to take a memory dump of the machine as well.

Interact with the machine using telnet,ssh,RDP,etc

Extract all traffic inbound to the target machine in the last 72 hours

Logs are firewall logs, machine logs, windows event logs, syslogs,etc.
#Focus on system logs such as failed logins, access violations,etc
#In network logs, focus on traffic coming to the infected machine, file transfer logs, http logs,etc.
#Enumerate tasks current and scheduled ones and pay special focus on those create by unknown users.

Have one of the sys admins with you all the time in case you needed credentials or explanation on something

Find out how the incident occured

This includes a premilinary analysis of the below

```
1- Find if there are newly created account on the machine
2- Try to inspect all tasks/jobs ran by the unrecognized account
3- Find the root cause of how the attacker managed to get access. This includes inspecting files that were modified around the time of the incident, inspecting tasks/jobs created by the unrecognized account, investigating startups,etc.
4- Don't disable the attacker's account untill you found the root cause and performed the full forensic analysis.
```

Create an infection time line

After you found the root cause of the hack, create an infection timeline outlining with timestap the steps taken starting from the first malicious action [privilege escalation] untill the moment when the team declared an incident [weird event happened like CPU overload].

Containment and Eradication

After you have discovered how the incident occured and created your infection timeline, you have two set of steps to follow for the eradication. #The below steps can be taken in order if the attacker managed to get access only to one machine which is the infected machine

```
- Identify backdoors first. Could be reverse shells or bind shells. Reverse shells can be found easily in firewall logs. Just look for a pattern of an outgoing connection to a recurring IP address. For bind shells, it is usually a listening point or active listening connection therefore nmap scan of the infected machine should reveal all open listening ports. Correlate nmap scan results with netstat issued on the machine to look for common points or discrepanies. If you find a weird listening port, then see if it's listed to start on boot which raises the chacnes of it being a bind shell.Lastly shut down the port and
```

disable the service that was running on it.
- Look for files modified around the time of the incident with two hours difference.
-Revoke any unauthorized account created
-Patch all vulnerabilities that caused privileged escalation or foothold access
-Reset passwords for all accounts in the machine
-Perform full rootkit and antivirus scan. In some instances, you may need to fully resotre from a previous safe state or do a full format
- Create a blacklist of C2C IPs and block it using the firewall.
- Create and Install fresh windows copies for infected machines.Be very careful when copying important documents before installing fresh windows copies. Exculde dangerous extension from you backup such as the below ones
.cs','*.ps1','*.psm','*.exe','*.com','*.dll','*.vbs','*.vbe','*.js','*.hta','*.msi','*.msp','*.csh','*.cpl','*.bat

```
- Reset all users' passwords especially in
Windows Active directory including the
KRBTGT and DSRM account twice.
- Clone AD into a new clean windows server
domain controller.
```

#One step I omitted from the above steps which is cutting internet access on the machine. Obviously if the infected machines is either a mainframe or a business critical machine where it handles most of your business operations such as serving content or services to clients, then cutting internet access immediately may not be a wise choise.

#If the attacker hacked the subject machine after compromising another machine or account then the below steps are taken in order:

```
- Repeat steps 1 and 2 and 3 from the
above scenario witout taking any action
like shutting down the port or revoking an
account access. We don't want to draw the
attacke's attention untill we are able to
neutralize the first root cause
```

- Start collecting data on the root cause. If the attacker managed to get access to the hacked machine via a hacked account or hacked machine then start collecting information about that machine very first. Make sure you follow privacy laws and take approvals from legal and HR to keep the evidence admissible.
- Gather the ip addresses and computer names of the infected machines and put them in a group you create in the firewall. Then start filtering the firewall logs for all communications between the infected machines including the DC or the public facing server. Filter for traffic on port 135 RCP and Ports 5985-5986 for Winrm to be able to spot the first machine from which the attacker established the first foothold and pivoted into other infected machines. Establish baselines of traffic before, during and after the incident to see the trends.

Establishing new firewall rules and logging configs

Just as the incident occured, you knew how it occured and what artifacts the attacker left. Make sure to do the following

```
- Create a firewall or IDS rule to raise an alert once a connection is attempted against the backdoor port
- Raise an alert using syslog or windows event logs whenever an account belonging to the attacker or used by the attacker was under the attempet of being accessed.
- Create a honeypot with interesting files and raise an alert upon a connection is made to it.
- Create an alert for any login made outside business hours.
```

Analysis and lessons learned

In this stage of IR, we create a report outlining the following

```
Total Assets Impacted by the incident
Type of data leaked if any
```

Attacks Detection Strategies

DNS Tunneling

A technique used by attackers especially advanced persisten groups to exfilterate data through DNS queries. Attackers prefer this method because DNS can't be blocked.
DNS Tunneling attack detection methods

```
1- Examine long DNS queries usually they
come in TXT query type. Wireshark or any
packet analyzer can be used.

2- Look also for uncommon DNS query types.

3- DNS tunneling usually use bot traffic
and algorithms so while looking into the
packers, pay attention to any consisten
and repeated long algorithm characters in
DNS queries.

4- Examine the destination host or server
```

```
to which the suspected traffic is sent. If
the host or server doesn't receive othe
traffic, it means the sole purpose of it
is to receive tunneling traffic.
```