

Incident Response Plan & Execution Process

1. Alert Triggered

- An alert is generated by the SIEM (e.g., **Splunk**, **OSSIM**) based on predefined correlation or directive rules.
- Common alert types:
 - Suspicious login attempts
 - Malware activity
 - Data exfiltration
 - SQL injection (SQLi)
 - Cross-site scripting (XSS)

2. Alert Validation – True Positive

- The L1 SOC Analyst reviews and investigates the alert.
- The analyst confirms it is a true positive by:
 - Analyzing logs from endpoints, firewalls, and servers
 - Correlating data across network and host layers
 - Leveraging internal and external threat intelligence sources

3. Ticket Creation (**OSSIM**)

- A ticket is created in the **OSSIM ticketing system** to formally document the incident.
- The ticket includes:
 - Alert summary (type, source, timestamp)
 - Impacted assets (IP addresses, hostnames, users)
 - Initial investigation details
 - Severity level (low, medium, high)

- The ticket is assigned to a specific member of the Incident Response Team (IRT) to ensure timely and accountable handling of the incident.

1: Generating Tickets for Incidents in OSSIM

Lab Objective

The objective of this lab is to help to create a ticket from a generated alarm which needs to be opened as an incident ticket.

Introduction to Ticketing

- Tickets represent alerts needing action.
- Simplify communication, tracking, and escalation.
- Help assign tasks, measure resolution time, and document actions.

Why Ticketing Matters in SOCs

Organizations can use ticketing systems to simplify the incident response and handling process. Tickets are requests made by users regarding different issues. In an incident response scenario, tickets represent suspicious events observed across networks, applications, systems, and devices.

The ticketing system also helps in tracking the event, victim, damage, time to solve the issue, members allocated, and methods implemented to find a solution. It helps maintain communication between IRT members and simplifies the process of seeking permissions from relevant authorities by presenting the details saved on a ticket.

As a SOC analyst, creating incident tickets is part of your daily job routine. After an initial investigation of alerts, you must be able to efficiently use ticketing systems to facilitate incident tracking and resolution.

Initial Setup

Systems Involved

- OSSIM Server: SIEM platform (access via browser).
- WinServer2012: Target machine.
- SIEM: Analyst machine.

Setup Steps

- Start OSSIM Server, WinServer2012, and SIEM

- Access OSSIM web interface and complete initial setup.

Create IRT User

- Navigate to CONFIGURATION > ADMINISTRATION > USERS.
- Create a user assigned to the Incident Response Team (IRT).
- Save and configure access as needed.

Deploy HIDS Agent on WinServer2012

- Go to ENVIRONMENT > ASSETS & GROUPS.
- Ensure the asset representing WinServer2012 is correctly added.
- Deploy HIDS agent to monitor the machine.
- Verify HIDS connection in OSSIM.

The screenshot shows the OSSIM web interface with the following details:

- Header:** WELCOME ADMIN | ALIENVAULT 192.168.1.55 | SETTINGS | SUPPORT | LOGO
- Top Navigation:** DASHBOARDS, ANALYSIS, ENVIRONMENT (highlighted), REPORTS, CONFIGURATION
- Sub-navigation:** ASSETS & GROUPS (selected), ASSETS, ASSET GROUPS, NETWORKS, NETWORK GROUPS, SCHEDULE SCAN
- Asset Details:** Assets > Asset Details for 'WinServer2012' (IP: 10.10.10.12, Microsoft Windows Server 2012 R2 Standard Edition). The asset has an icon of a server tower.
- Asset Properties:**
 - Asset Value: 0 1 2 3 4 5 (with '2' highlighted)
 - Device Type: Unknown
 - Networks: Pvt_010 (10.0.0.0/8)
 - Sensors: alienvault (192.168.1.55)
 - Model: Unknown
- Actions Menu:** A context menu is open over the asset, listing:
 - Edit
 - Delete
 - Run Asset Scan
 - Run Vulnerability Scan
 - Enable Availability Monitoring
 - Disable Availability Monitoring
 - Deploy HIDS Agent
- Bottom Right:** A small window asking 'Do you own this website?' with a '+' button.

Create a Correlation Directive

Objective: Detect brute force attacks on admin accounts.

- Navigate to CONFIGURATION > THREAT INTELLIGENCE > DIRECTIVES.
- Create a new directive:
 - **Name:** Brute Force Attempt - Admin Account
 - **Intent:** Environmental Awareness
 - **Strategy:** Suspicious Behaviour
 - **Method:** Brute Force Attempt

- Priority: 4

Directive Rules

- Rule 1: Failed Login Attempts
 - Detect multiple failed login attempts.
- Rule 2: Successful Logon
 - Detect successful login following failed attempts.

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
Brute Force Attempt-Admin Account	1	None	1	ANY	ANY	AlienVault HIDS- win_authentication_failed (7085)	SIDs: 18106 18130 18132 18136	
Failed Login Attempt	2	180	3	1:SRC_IP	1:DST_IP	AlienVault HIDS- win_authentication_failed (7085)	SIDs: 18106 18130 18132 18136	
Logon Rule	3	300	1	1:SRC_IP	1:DST_IP	AlienVault HIDS- authentication_success (7009)	SIDs: 700002 700001 18107 102003	
Special privilege Rule	8	600	1	1:SRC_IP	1:DST_IP	AlienVault HIDS- authentication_success (7009)	SIDs: 700006	

DIRECTIVE INFO

AlienVault Scada

Generate the Alarm

- Simulate multiple failed login attempts on WinServer2012.
- Perform a successful login afterward.
- OSSIM should detect the activity and raise a **Brute Force Attempt** alarm.

Create and Assign the Ticket

- Go to ANALYSIS > ALARMS.
- Select the newly raised alarm.
- Create a ticket from the alarm.
- Assign it to the IRT user created earlier.

The screenshot shows the AlienVault OSSIM web interface. At the top, there's a header with the logo, 'ALIEN VAULT OSSIM', and navigation links for 'WELCOME ADMIN', 'ALIENVault 192.168.1.55', 'SETTINGS', 'SUPPORT', and 'LOGOUT'. Below the header, there are five main menu items: 'DASHBOARDS' (with a bar chart icon), 'ANALYSIS' (with a magnifying glass icon, currently selected), 'ENVIRONMENT' (with a planet icon), 'REPORTS' (with a document icon), and 'CONFIGURATION' (with a wrench icon). The main content area is titled 'TICKETS' and features a 'SIMPLE FILTERS' section with dropdowns for 'Class' (set to 'ALL'), 'Type' (set to 'Anomalies'), 'Search text' (empty), 'Assignee' (empty), 'Status' (set to 'Open'), and 'Priority' (set to 'ALL'). There's also a 'SEARCH' button. Below the filters is a table of tickets. The first and only ticket listed is 'ALA02', with the title 'Brute Force Attempt-Admin Account'. It has a green circular badge with the number '2' next to it. The ticket details show it was created on '2025-03-25 05:40:24' by 'Martin' (Administrator) and is an 'Anomalies' type with a status of 'Open'. At the bottom of the table, there's a note 'Open a new ticket manually:' followed by a dropdown set to 'Alarm' and a 'CREATE' button.

2: Containing Data Loss Incidents

IRT along with technical, management, and legal team prepare a containment strategy to control the effect of incident.

Lab Scenario

Containment of incident is very crucial phase, and this has to be performed in order to immediately stop the live attack to reduce the further damages and losses. FTP servers are used to transfer files between computers on a network. These servers are easily targeted by hackers to get sensitive information stored. If such servers are accessed by unauthorized users of malicious intent, they can delete or copy sensitive data of the organization. In this lab, we are monitoring such unauthorized access to FTP server and stop the data download activity initiated by unauthorized user immediately so that the users cannot download all of the data that was intended.

Lab Objectives

The objective of this lab is to explain how the incidents are contained in containment phase of in incident response process. In this lab, we are containing data loss incident.

1. Configure Splunk Universal Forwarder on WinServer2012

2. Edit inputs.conf

- inputs.conf → Edit it
- Add this lines

```
*C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf -
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
inputs.conf [3]
1 [monitor://C:\inetpub\logs\LogFiles\FTPSVC3]
2 sourcetype=FTP
3 ignoreOlderThan =14d
4 host = WinServer2012
```

Edit props.conf

- Edit it props.conf.
- Add this

```
*C:\Program Files\SplunkUniversalForwarder\etc\system\local\props.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
props.conf [3]
1 [iis*]
2 pulldown_type=true
3 MAX_TIMESTAMP_LOOKAHEAD =32
4 SHOULD_LINEMERGE =False
5 CHECK_FOR_HEADER =False
6 REPORT_iis2 =iis2
7
8 [FTP*]
9 TZ=GMT + 5:30
10 pulldown_type =true
11 MAX_TIMESTAMP_LOOKAHEAD =32
12 SHOULD_LINEMERGE =False
13 CHECK_FOR_HEADER =False
14 REPORT-FTP2 =FTP2
```

- Save it

Edit/create transforms.conf

- Same folder → If transforms.conf doesn't exist, create it.
 - Add this
- [FTP2] DELIMS=" "
- FIELDS=date time c-ip cs-username s-ip s-port cs-method cs-uri-stem sc-status sc-win32-status sc-substatus x-session x-fullpath

```
*C:\Program Files\SplunkUniversalForwarder\etc\system\local\transforms.conf -
inputs.conf outputs.conf props.conf transforms.conf
[default]
host -WinServer2012
[ignore_comments]
REGEX =^#.*
DEST_KEY =queue
FORMAT =nullQueue
[iis2]
DELIMS =" "
FIELDS = date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Cookie) cs(Refere
[FTP2]
DELIMS =" "
FIELDS = date time c-ip cs-username s-ip s-port cs-method cs-uri-stem sc-status sc-win32-status sc-substatus x-session
```

Restart Splunk Forwarder Service

- Start menu → Administrative Tools → Services.
- Restart the SplunkForwarder service.

2: Simulate Unauthorized FTP Access from Kali Linux

Run Port Scan

```
root@Analyst:~# nmap -p [REDACTED] Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-29 16:29 IST Nmap scan report for www.luxurytreats.com ([REDACTED]) Host is up (0.0011s latency). PORT      STATE SERVICE 21/tcp      open  ftp
```

Try to Access FTP

```
ftp 1*2.17*.1*6.9*
```

- Try random usernames/passwords.

Brute Force with Hydra

```
hydra -L '/root/Wordlist/userlist.txt' -P '/root/Wordlist/pass.txt' ftp://192.17*.1*6.9*
```

- Wait for credentials to be cracked.

Login Using Cracked Credentials

```
ftp 192.17*.1*6.9*
```

Username: ****

Password: *****

```
root@Analyst:~# hydra -L '/root/Wordlist/userlist.txt' -P '/root/Wordlist/pass.txt' .12 Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret operations, or for illegal purposes. Hydra (http://www.thc.org/thc-hydra) starting at 2019-04-29 16:32:07 [DATA] max 16 tasks per server, overall 16 tasks, 30 login tries (l:5/p:6), ~2 [DATA] attacking ftp://[REDACTED].10.10.10.12:21/ [21][ftp] host: [REDACTED] login: [REDACTED] password: [REDACTED] 1 of 1 target successfully completed, 1 valid password found
```

3: Simulate Data Theft Using FileZilla on Windows10

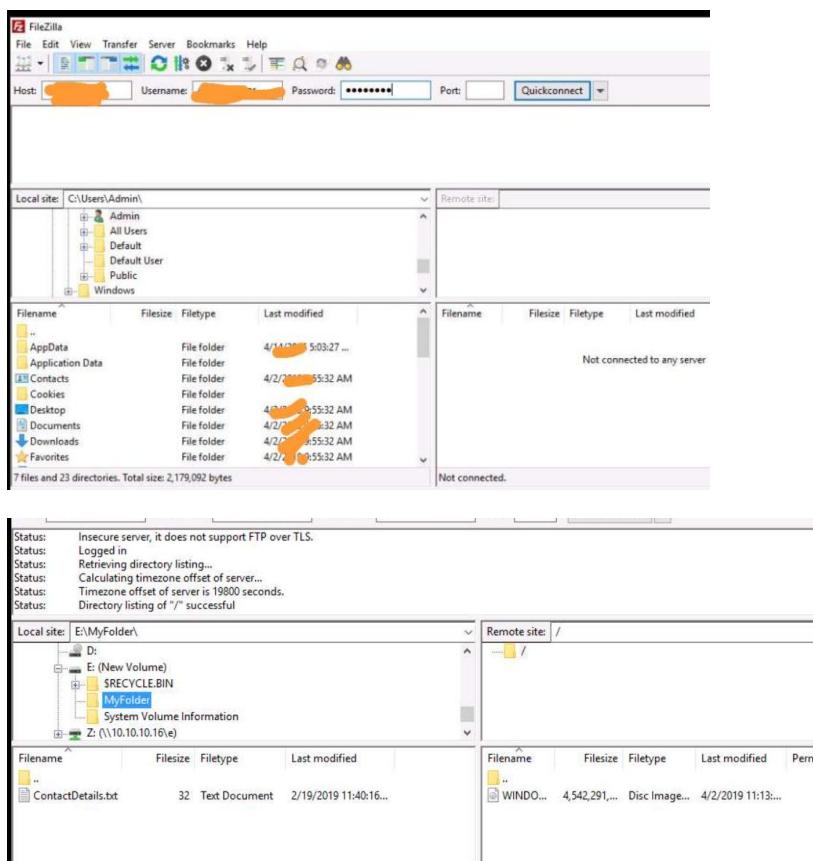
Login to Windows10

- Username:
- Password:

Prepare for Data Exfiltration

Use FileZilla to Connect to FTP

- Open FileZilla
- Fill:
 - Host:
 - Username:
 - Password:
 - Click Quickconnect



Download Sensitive File (this file content on file manager)

To download WINDOWS2012R2Server.ISO file of 4.22 GB size from FTP site, right-click WINDOWS2012R2Server.ISO file from the Remote site pane and click Download
Do NOT wait for it to finish! Go to next step immediately

Here we are assuming that download activity is in process and we must stop this as soon as download of file is identified



4: Detect & Contain Attack Using Splunk on SIEM1

Open Splunk in Chrome

- Go to: <http://localhost:8000>
- Username: admin
- Password: *****

Detect FTP Connection

- Use this search in Splunk

A screenshot of a Splunk search interface. The search bar contains the query 'host=WinServer2012 sourcetype=FTP *10.***.* "ControlChannelOpened"'. The results show two events from 'WinServer2012' over the last 24 hours. The first event is timestamped '2019-09-10 10:21:21' and the second is '2019-09-10 10:21:21'. Both events mention 'ControlChannelOpened' and 'source = C:\inetpub\logs\LogFiles\FTPSVC3\...'. The interface includes a sidebar with selected fields like 'host', 'source', and 'sourcetype', and interesting fields like '#date_hour', '#date_mday', and '#date_minute'.

- You'll see a log showing connection from **Windows10**

5: Stop Data Loss by Killing FTP Service

Go to WinServer2012 → Open Task Manager

- Right-click Taskbar → Task Manager → Services tab
- Find **ftpsvc** → Right-click → Click Stop.

This stops the FTP server, ending the file transfer.

After stopping the server, it will show like this



6: Confirm Block on Windows10 and Log the Event

Switch to Windows10

- FileZilla shows an **error**: Connection lost, partial file downloaded.

Check Logs in Splunk

- Back in SIEM → Splunk search:

```
host=WinServer2012 sourcetype=FTP ""
```

- You'll find logs showing partial download and error 550.

A screenshot of a Splunk search interface. The search bar shows "localhost:8000/en-US/app/SplunkForwarder/search?q=search%20host%3DWinServer2012%20sourcetype%3DFTP%20%10...". The results table has columns: #, Hide Fields, All Fields, List, Format, 20 Per Page, < Prev, 1, 2, Next >. One result is highlighted:

#	Time	Event
1	2019-04-10 10:57:12	source = C:\inetpub\logs\LogFiles\FTPSVC3\IIS_ex190410.log sourcetype = FTP 2019-04-10 10:57:12 10.10.10.10 59676 WINSERVER2012\Administrator FTSPVC3 R NSERVER2012 - 10.10.10.10.12.21 RETR WINDOWS2012R2Server.ISO 550 64 0 21231698 1 30 33781 8d7e286f-025b-41f4-afc4-a4cd1baa7ebc /WINDOWS2012R2Server.ISO - host = WinServer2012 source = C:\inetpub\logs\LogFiles\FTPSVC3\IIS_ex190410.log sourcetype = FTP

Eradicating SQL Injection and XSS Incidents

Eradication involves removing or eliminating the root cause of the incident and closing all the attack vectors to prevent similar incidents in future.

Lab Scenario

If the target website is www.LuxuryTreats undergoing SQL and XSS attacks, the ideal eradication strategy would be to identify the root cause of such attacks. These attacks are possible when attacker poises normal web requests with malicious parameters and sends it to the webservers. Web filters, if configured properly, can help you eradicate such SQL and XSS injection vulnerabilities as they filter requests based on allowed or denied characters in the web requests

Lab Objectives

The objective of this lab is to explain how the incidents are eradicated in eradication phase of incident response process. In this lab, we are eradicating SQL Injection and XSS incidents.

www.LuxuryTreats, it is a vulnerable website,

1: Install UrlScan Tool on WinServer2012

Log in to WinServer2012

Install UrlScan

Path C:\Windows\system32\inetsrv\urlscan

2.Copy UrlScan Config to Website Folder

- Go to C:\Windows\system32\inetsrv\ folder, copy urlscan folder.
- Paste into C:\inetpub\wwwroot\LuxuryTreats folder.

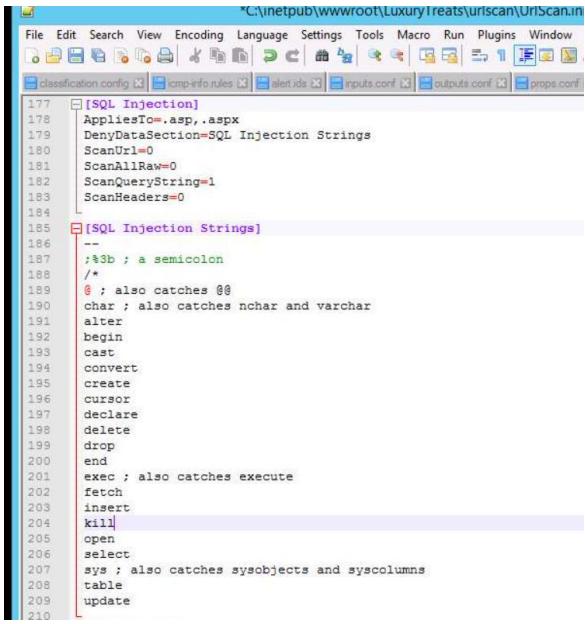
Create SQL Injection Filter Rule

3. Edit UrlScan.ini

Edit it

Add SQL Injection Rule

Add this **after line 175**



The screenshot shows a Notepad window with the file path "C:\inetpub\wwwroot\LuxuryTreats\UrlScan\UrlScan.ini". The content of the file is a configuration for UrlScan, specifically for SQL Injection detection. It includes sections for [SQL Injection] and [SQL Injection Strings], listing various keywords and symbols that trigger the detection process.

```
*C:\inetpub\wwwroot\LuxuryTreats\UrlScan\UrlScan.ini
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window
classification.config icmp-info.rules alert.ids inputs.conf outputs.conf props.conf
[SQL Injection]
AppliesTo=.asp,.aspx
DenyDataSection=SQL Injection Strings
ScanUrl=0
ScanAllRaw=0
ScanQueryString=1
ScanHeaders=0
[SQL Injection Strings]
--%3b : a semicolon
/*
@ ; also catches @@ char ; also catches nchar and varchar
alter
begin
cast
convert
create
cursor
declare
delete
drop
end
exec ; also catches execute
fetch
insert
kill
open
select
sys ; also catches sysobjects and syscolumns
table
update
209
210
```

4: Apply UrlScan to Website (via IIS)

Open IIS Manager

- Start Menu → Windows Administrative Tools → **Internet Information Services (IIS) Manager**
- In IIS, only administrators have permission to configure settings and view detailed web server logs. These logs record all website activities, including attempts of SQL Injection (SQLi) and Cross-Site Scripting (XSS) attacks. Administrators use IIS logs and Event Viewer to monitor and analyze security events. This helps in early detection and response to malicious activities.

Assign Filter to Website

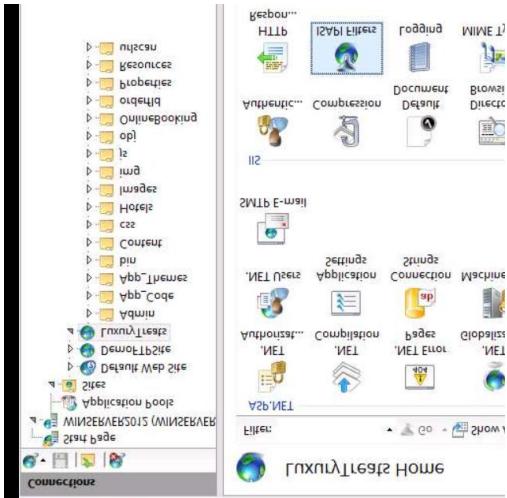
- In the left pane (Connections), expand:
 - Sites → Click LuxuryTreats
- In the middle pane (Home), double-click **ISAPI Filters**

Why use ISAPI Filters (like UrlScan)

ISAPI filters in IIS allow you to modify or extend the behavior of the web server. By using an ISAPI filter like **UrlScan 3.1**, you can:

- **Monitor and block malicious HTTP requests** such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and other common attacks.
- **Limit the size or type of files** that can be uploaded, preventing large files that could lead to a DoS (Denial of Service) attack.

- **Control URL patterns**, restricting access to sensitive or unnecessary parts of your web server.

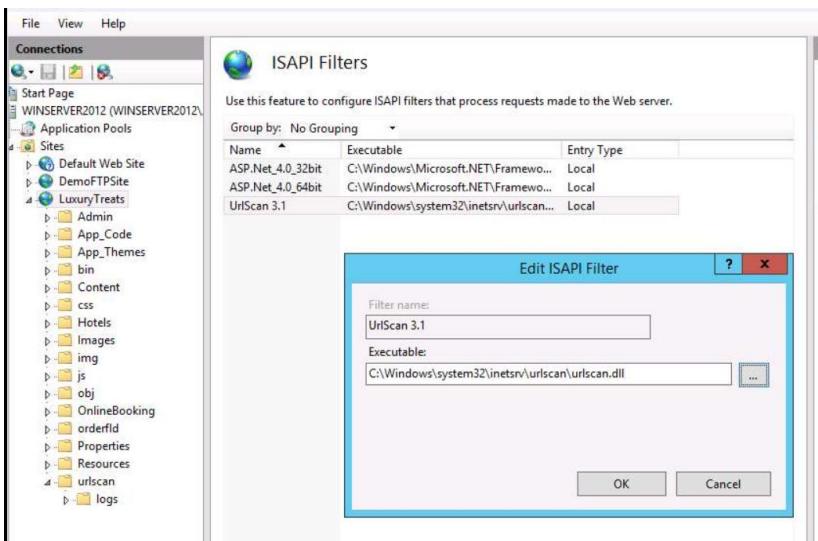


- Click **UrlScan 3.1** → In right pane click **Edit**

Set DLL Path

C:\inetpub\wwwroot\LuxuryTreats\urlscan

- Select: **urlscan.dll** → Click **OK**



Restart IIS

- On the left pane, click the top-level server: **WINSERVER2012**
- On right pane → click **Restart**

Test Protection from Attacks

Test as Legit User windowserver

- Open Chrome → go to <http://www.luxurytreats.com>
- Login with:
 - Username: ** Password: **
- Click **My Orders** → Select ORD-001 → View order details.

This works normally.

The screenshot shows a web browser window with the URL <http://www.luxurytreats.com/OrderDetail.aspx?Id=ORD-001>. The page title is "Order Detail". The main content area displays the following table:

Product Code	Qty	Rate/Qty
P00-1	10	125.00
P00-1	10	125.00

As per standard security practice, only authorized person should see their personal data. If person can see other's order details, then it can be considered as security breach. This can be possible using SQL Injection technique. Attacker use this technique to bypass security measures of other user's data.

Try SQL Injection Attack (Kali Linux)

- Login:
 - Username: ***Password: **
- Open Firefox → go to:

<http://www.luxurytreats.com/OrderDetail.aspx?Id=ORD-001' or 1=1;-->

The screenshot shows a Mozilla Firefox browser window with the following details:

- Address bar: <http://www.luxurytreats.com/OrderDetail.aspx?Id=ORD-001' or 1=1;-->
- Status bar: 404 - File or directory not found. - Mozilla Firefox
- Error message: 404 - File or directory not found.
- Description: The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

UrlScan should block all incoming SQL Injection, no matter **which machine** (Windows, Kali, Linux) or **which browser** (Chrome, Firefox) sends it.

-  **UrlScan will first inspect the HTTP request** before allowing it to reach the web application.

If the request contains:

- ' or 1=1;-- (SQL injection pattern) .<script> (XSS attack pattern)

Recovering from Data Loss Incidents

In recovery phase, IRT has to perform recover actions in order to maintain business continuity.

Lab Scenario

Malicious insiders, with the privileged rights or through the elevated privileges, can delete sensitive data intentionally to disrupt the business continuity of the organization. Such type of data loss incidents, if detected, can be recovered using data recovery tools.

Lab Objectives

The objective of this lab is to explain how the recovery is done from the incident losses in the recovery phase of incident response process. In this lab, we are recovering deleted data.

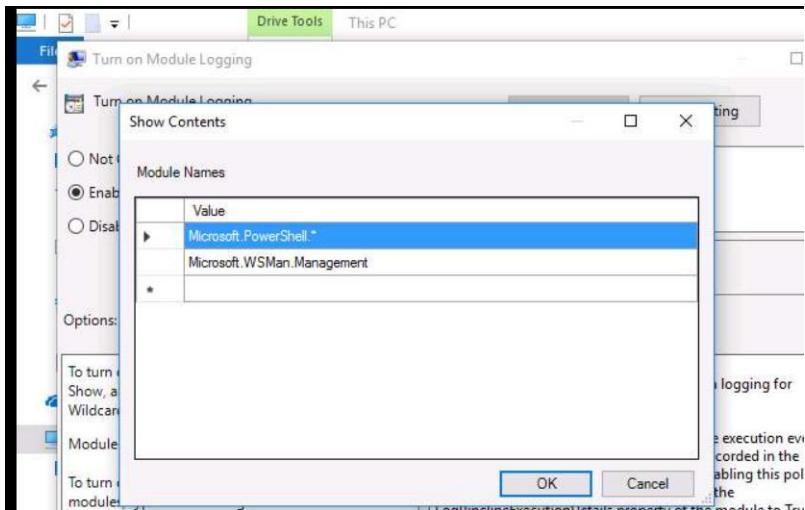
Steps to Configure Logging (on Windows10)

1. Enable PowerShell Logging

- Open: Edit group policy
- Navigate to:
Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell

a. Turn on Module Logging

In the **Turn on Module Logging** window, click **Enabled**. Click **Show..** button. In the **Show Contents** dialogbox type **Microsoft.PowerShell.*** and **Microsoft.WSMan.Management** in the **Module Names** table. Click **OK**



Turn on the enable

Setting	State	Comment
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on Script Execution	Enabled	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configured	No

Enable PowerShell Remoting on Both Machines

Windows10:

- Open PowerShell (as admin):
 - Set-NetConnectionProfile -NetworkCategory Private
 - winrm quickconfig → Type y
 - Enable-PSRemoting -Force
 - Set-Item wsman:\localhost\client\trustedhosts * → Type y
 - Restart-Service WinRM

```

Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Set-NetConnectionProfile -NetworkCategory Private
PS C:\Windows\system32> winrm quickconfig
WinRM is not set up to receive requests on this machine.
The following changes must be made:

Start the WinRM service.
Set the WinRM service type to delayed auto start.
Make these changes [y/n]? y
WinRM has been updated to receive requests.

WinRM service type changed successfully.
WinRM service started.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP:///* to accept WS-Man requests to any IP on this machine.
Enable the WinRM firewall exception.
Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
Make these changes [y/n]? y
WinRM has been updated for remote management.

Created a WinRM listener on HTTP:///* to accept WS-Man requests to any IP on this machine.
WinRM Firewall exception enabled.
Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
PS C:\Windows\system32> Enable-PSSession -Force
WinRM is already set up to receive requests on this computer.
WinRM is already set up for remote management on this computer.
PS C:\Windows\system32> Set-Item wsman:\localhost\client\trustedhosts

WinRM Security Configuration.
This command modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts list might not be authenticated. The client might send credential information to these computers. Are you sure that you want to modify this list?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32> Restart-Service WinRM
PS C:\Windows\system32>

```

WinServer2012:

- Open PowerShell (as admin):
 - Set-NetConnectionProfile -NetworkCategory Private
 - winrm quickconfig → Type y
 - Restart-Service WinRM

```

Select Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Set-NetConnectionProfile -NetworkCategory Private
PS C:\Users\Administrator> winrm quickconfig
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

Make these changes [y/n]? y
WinRM has been updated for remote management.

Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
PS C:\Users\Administrator> Restart-Service WinRM
PS C:\Users\Administrator>

```

Configure Splunk Forwarder on Windows10

1. Edit inputs.conf

```

C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
inputs.conf

1 [default]
2 host = Windows10
3
4 [monitor://C:\inetpub\logs\LogFiles]
5 sourcetype=iis
6 ignoreOlderThan =1d
7 host = WinServer2012
8
9 [WinEventLog://Microsoft-Windows-PowerShell/Operational]
10 disabled = false
11

```

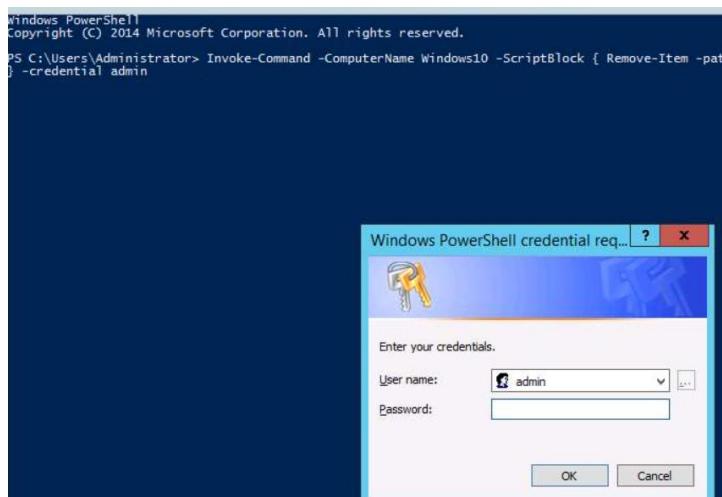
2. Restart SplunkForwarder service

- Search: Services
- Restart: SplunkForwarder

Data Deletion Attack Simulation

- **Setup Target Folder:**
- Here, we have supposed that malicious insider on Winserver2012 machine will delete the sensitive data (**MyFolder**) on **Windows10** machine. We have also assumed that this malicious insider has somehow succeeded in gaining the credential of user (**Username: and Password:**) on Windows10 machine either through brute force or social engineering techniques.
 - Copy MyFolder from Z:\SOC-Tools to E:\ drive on Windows10 machine.
 - Click the E:\ drive then Edit the properties and Grant **Full Control** permissions to the folder.
- **On WinServer2012 (Attacker):**
 - Configure trusted hosts to Windows10 machine.
 - Use Invoke-Command with PowerShell to **delete** E:\MyFolder remotely:

```
Invoke-Command -ComputerName Windows10 -ScriptBlock { Remove-Item -path E:\MyFolder -recurse } -Credential admin
```



If you Type the password (***)for admin user in the displayed dialog box and click **OK**. On successful execution of the command, **MyFolder** folder will be deleted from **Windows10** system.

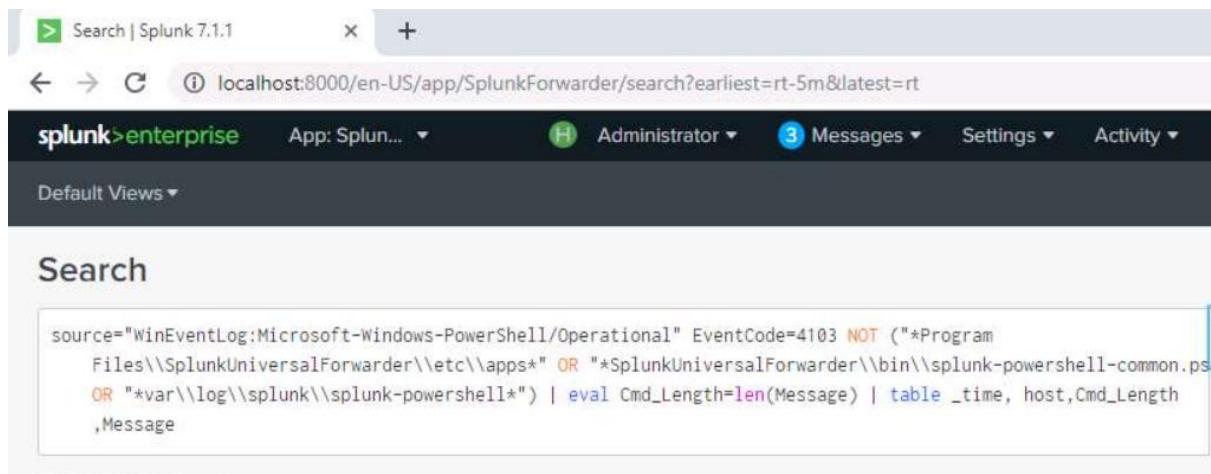
- **Result:**

- MyFolder is deleted on Windows10.
- Deletion detected via **Splunk SIEM** using PowerShell event code **4103**.

Detection in Splunk SIEM

- **On SIEM1 (Splunk Search):**

Click **SplunkForwarder**. In the **New Search** textbox, type the following command to detect the remotely executed PowerShell commands used to delete folder. Select **30 minute window** and click **search** icon



```
source="WinEventLog:Microsoft-Windows-PowerShell/Operational" EventCode=4103 NOT ("*Program Files\\SplunkUniversalForwarder\\etc\\apps*" OR "*SplunkUniversalForwarder\\bin\\splunk-powershell-common.ps OR "*var\\log\\splunk\\splunk-powershell*") | eval Cmd_Length=len(Message) | table _time, host,Cmd_Length ,Message
```

You will view the captured **PowerShell logs** displaying **remote script execution** details, which indicate execution of a delete command on **E:\\MyFolder**.

Statistics (2) Visualization

Format

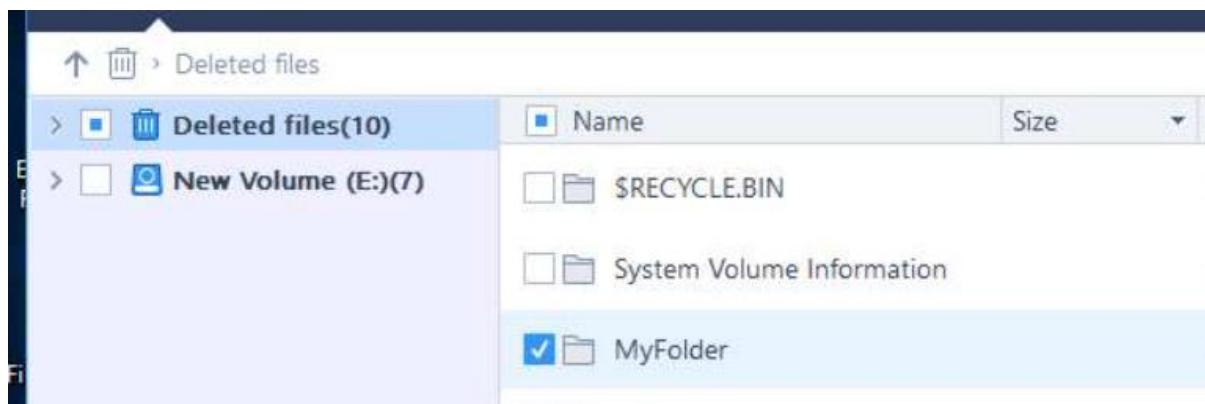
host	Cmd_Length	Message
Windows10	1022	CommandInvocation(Remove-Item): "Remove-Item" ParameterBinding(Remove-Item): name="Path"; value="E:\MyFolder" ParameterBinding(Remove-Item): name="Recurse"; value="True" CommandInvocation(Out-Default): "Out-Default" ParameterBinding(Out-Default): name="Transcript"; value="True" ParameterBinding(Out-Default): name="OutVariable"; value="" Context: Severity = Informational Host Name = ServerRemoteHost Host Version = 1.0.0.0 Host ID = 55f62fff-54c8-4f28-938e-c06547edd25a Host Application = C:\Windows\system32\wsmprovhost.exe -Embedding Engine Version = 5.0.10586.1417 Runspace ID = af0e4a4b-f062-42bb-99e9-9acf4f22712a Pipeline ID = 1 Command Name = Remove-Item Command Type = Cmdlet Script Name = Command Path = Sequence Number = 16 User = WINDOWS10\Admin Connected User = WINDOWS10\admin Shell ID = Microsoft.PowerShell User Data:
Windows10	1022	CommandInvocation(Remove-Item): "Remove-Item" ParameterBinding(Remove-Item): name="Path"; value="E:\MyFolder" ParameterBinding(Remove-Item): name="Recurse"; value="True" CommandInvocation(Out-Default): "Out-Default" ParameterBinding(Out-Default): name="Transcript"; value="True" ParameterBinding(Out-Default): name="OutVariable"; value="" Context: Severity = Informational Host Name = ServerRemoteHost Host Version = 1.0.0.0 Host ID = 762d2656-c902-4479-ad78-5a7f4fe659f2 Host Application = C:\Windows\system32\wsmprovhost.exe -Embedding Engine Version = 5.0.10586.1417 Runspace ID = cbad4a2b-ad51-4732-afdc-669023e5397e Pipeline ID = 1 Command Name = Remove-Item Command Type = Cmdlet Script Name = Command Path = Sequence Number = 16 User = WINDOWS10\Admin Connected User = WINDOWS10\admin Shell ID = Microsoft.PowerShell User Data:

Recover the Deleted Folder using EaseUS Tool

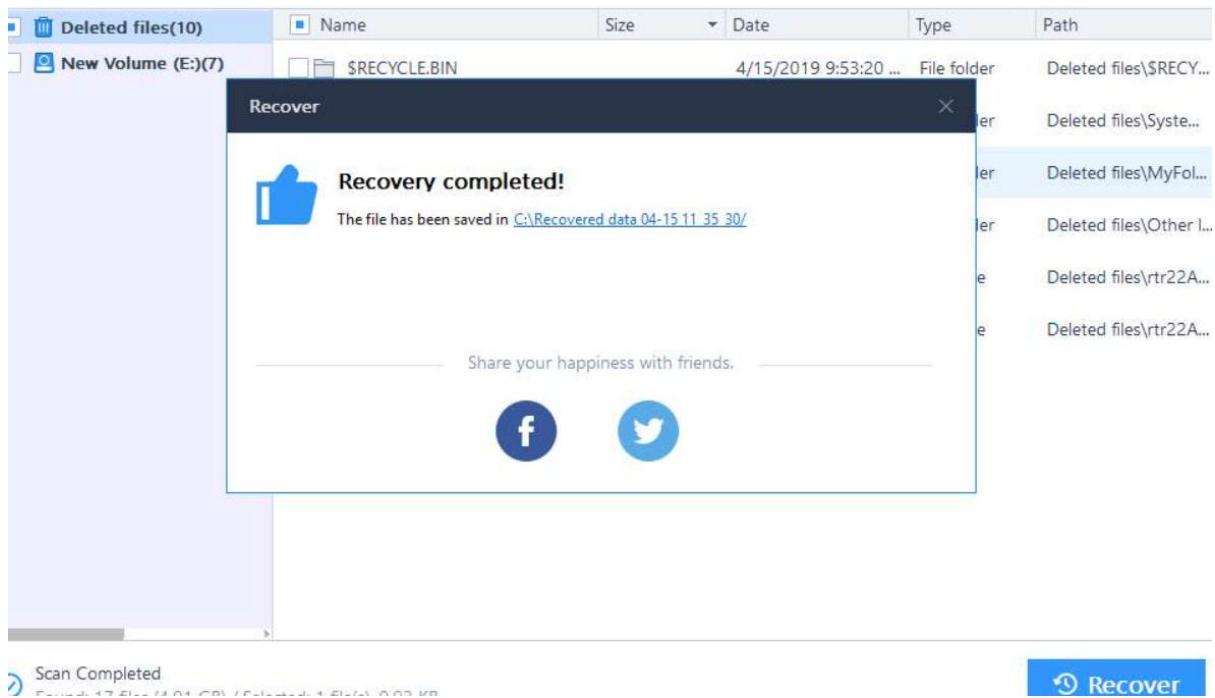
Install EaseUS Data Recovery Tool on Windows10

Scan and Recover:

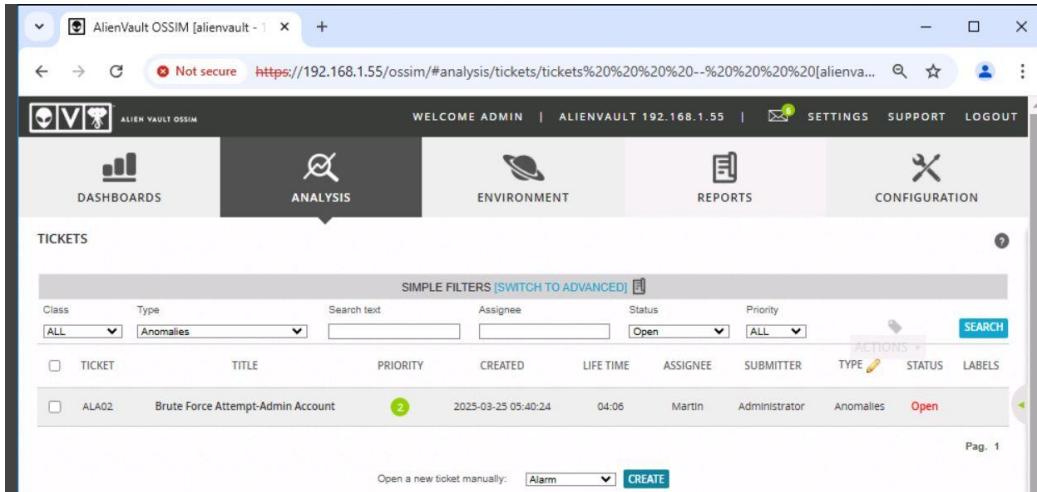
- Select **New Volume (E:)** to scan.
- Locate and recover deleted MyFolder.
- Save recovered files to **C:\ Drive**.
- As you can see deleted files



EaseUS Data Recovery will display a list of deleted files. Select the deleted folder **MyFolder** and click **Recover**.



Creating Incident Reports using OSSIM



1. To generate an Alarm Report, navigate to **REPORTS-> OVERVIEW** from the menu.
2. In the **REPORTS OPTIONS - Alarms Report**, select from the list of report you want by checking the checkbox next to it. The default date range for alarm report is 30 days. You can change the date range as per your requirements for generating the report.
3. In the **REPORTS OPTIONS - SIEM EVENTS**, select from the list of reports you want by checking the checkbox next to it. The default date range is for SIEM Events report is 30 days.
4. Click **Download PDF** to download the selected report as PDF.
5. You can send this report to the concerned person in IRT. Click **Send by e-mail**, provide email address of the concerned person, and click **SEND** to send the report.