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

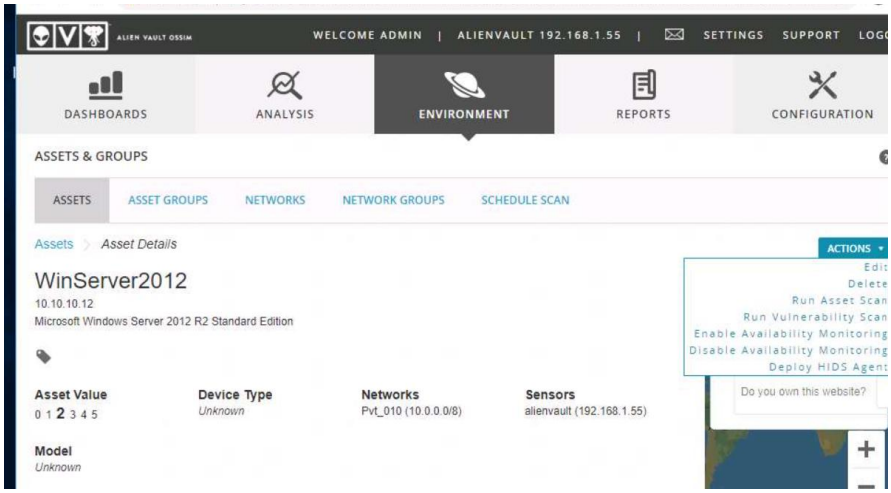
- Access OSSIM web interface and complete initial setup.

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.



Create a Correlation Directive

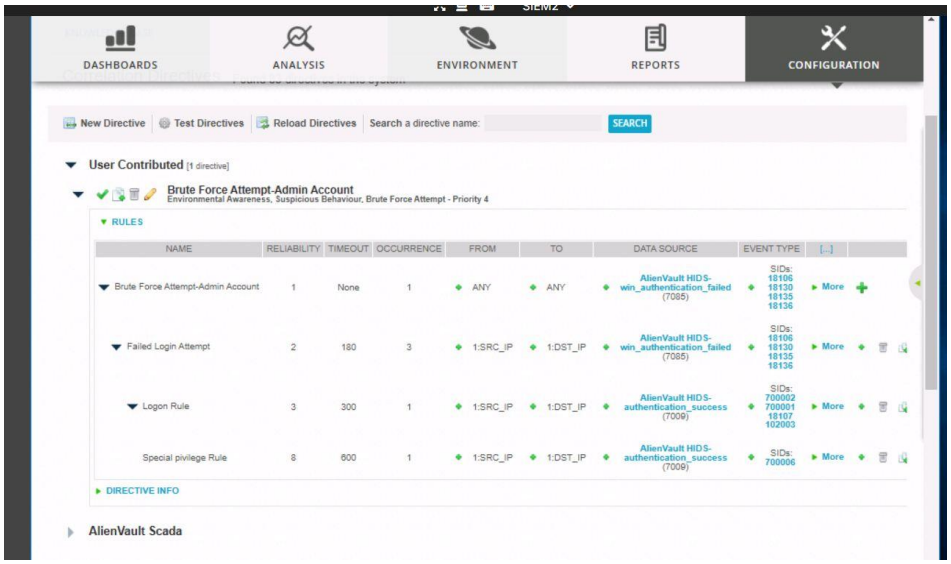
Objective: Detect brute force attacks on admin accounts.

- 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.

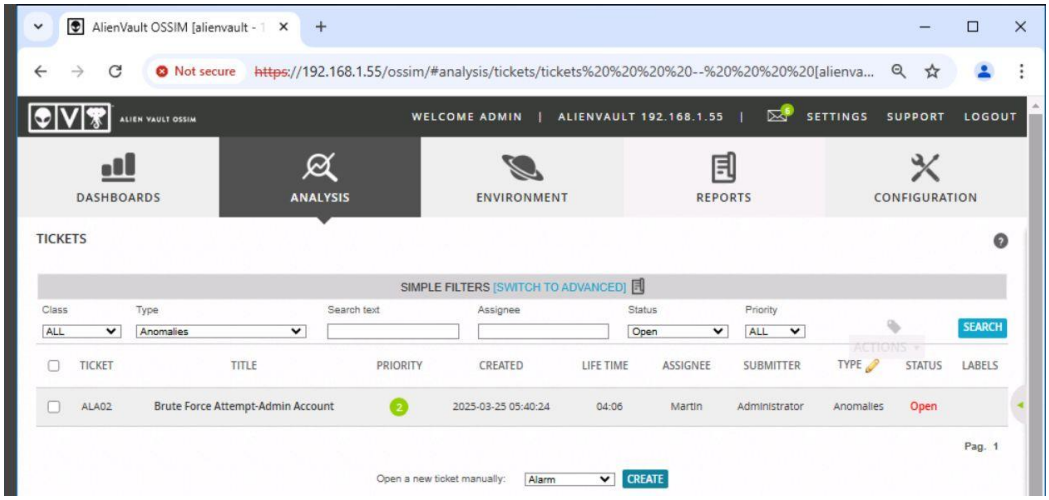


Generate the Alarm

- 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.



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.

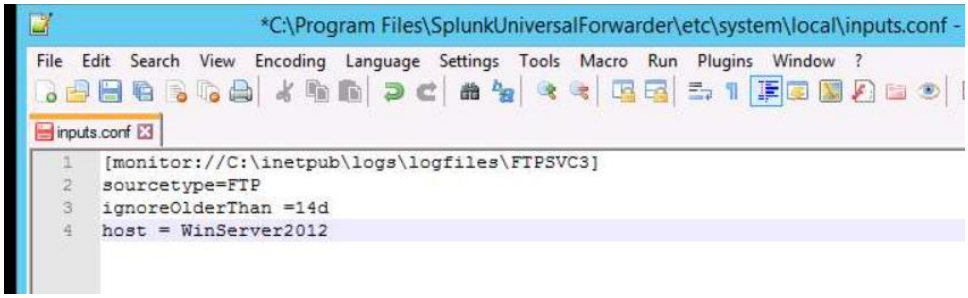
Lab Objectives

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

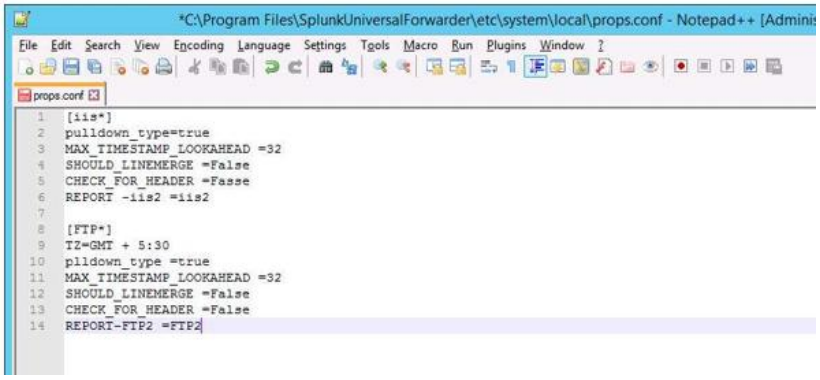
2. Edit inputs.conf

- inputs.conf → Edit it
- Add this lines



Edit props.conf

- Edit it props.conf.
- Add this



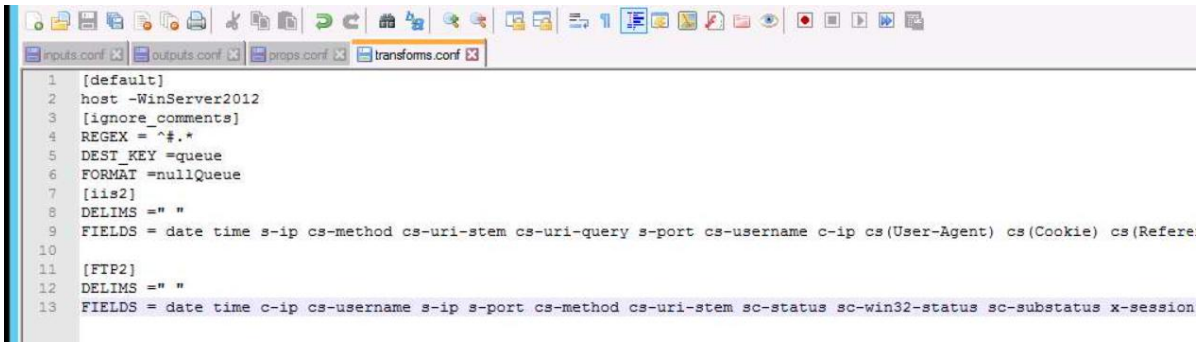
- Save it

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

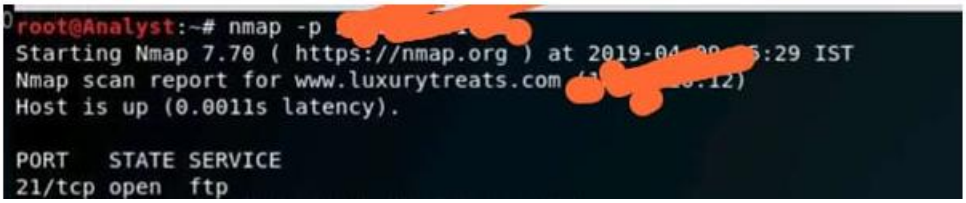


Restart Splunk Forwarder Service

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

2: Simulate Unauthorized FTP Access from Kali Linux

Run Port Scan



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*

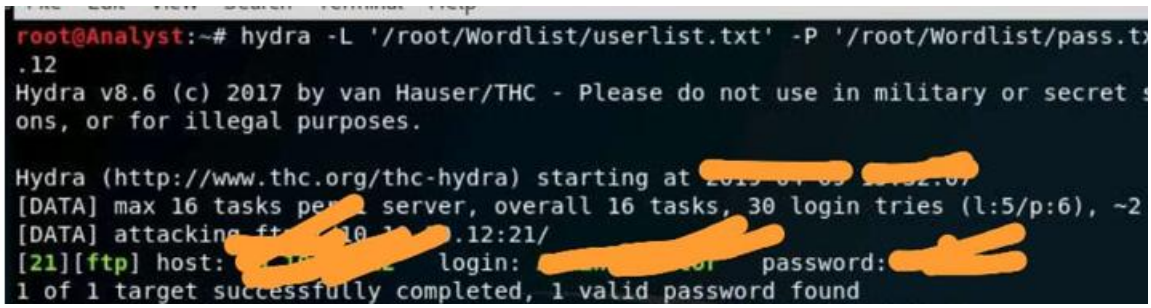
- Wait for credentials to be cracked.

Login Using Cracked Credentials

ftp 192.17*.1*6.9*

Username: ****

Password: ******



3: Simulate Data Theft Using FileZilla on Windows10

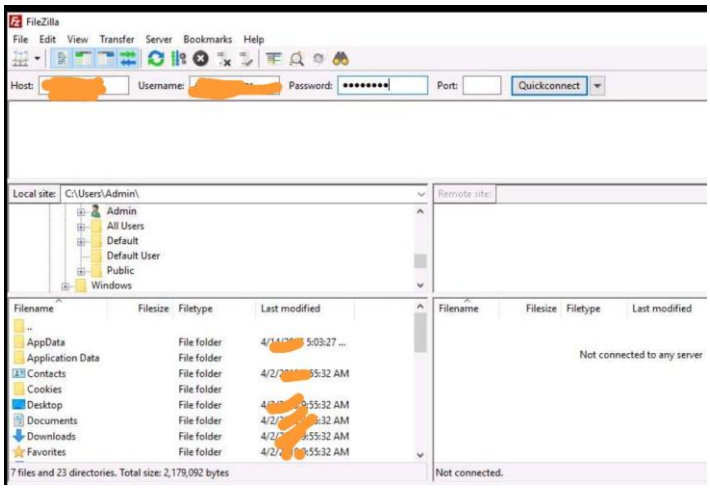
Login to Windows10

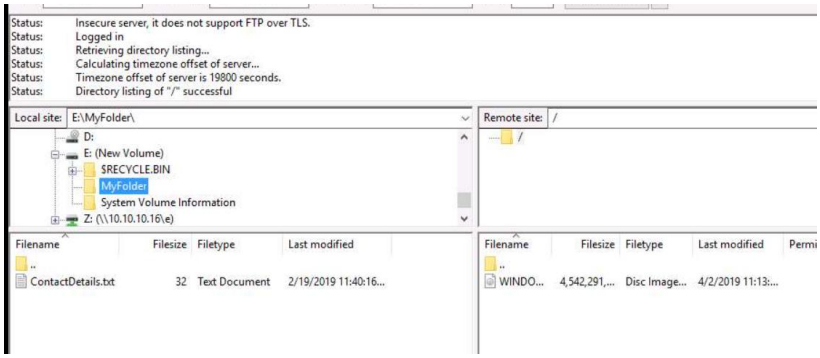
- Username:
- Password:

Prepare for Data Exfiltration

Use FileZilla to Connect to FTP

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



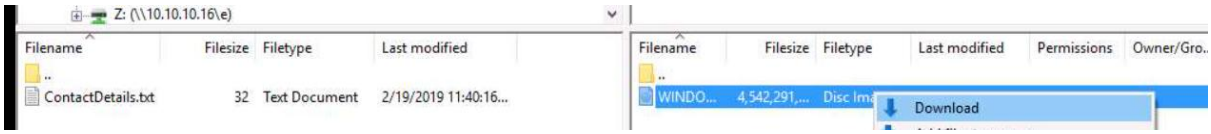


Download Sensitive File (this file content on file manager)

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

Thrishank Reddy koppala

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



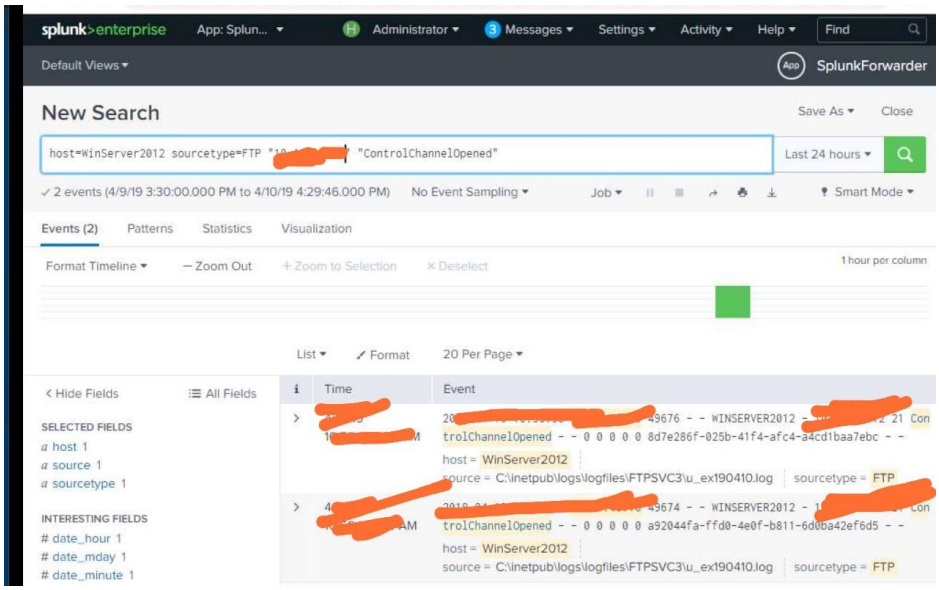
4: Detect & Contain Attack Using Splunk on SIEM1

Open Splunk in Chrome

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

Detect FTP Connection

- Use this search in Splunk



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

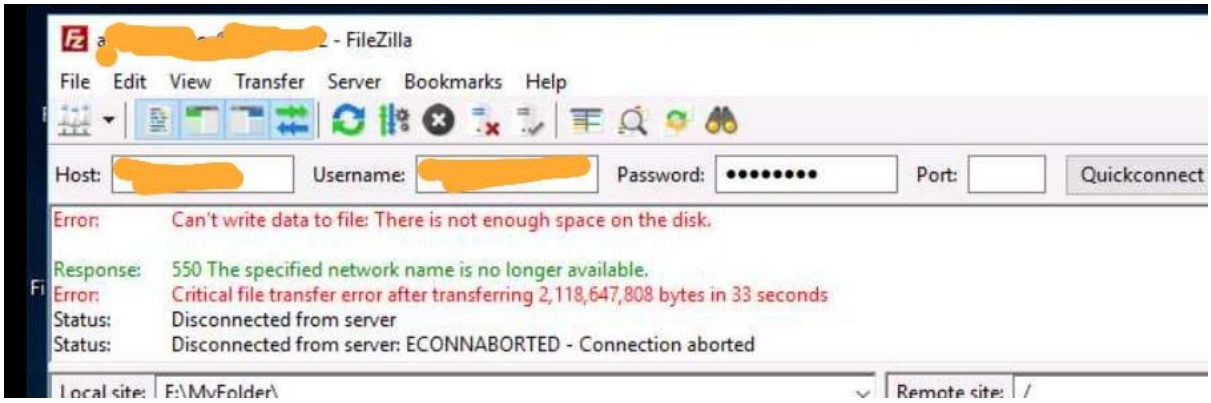
5: Stop Data Loss by Killing FTP Service

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

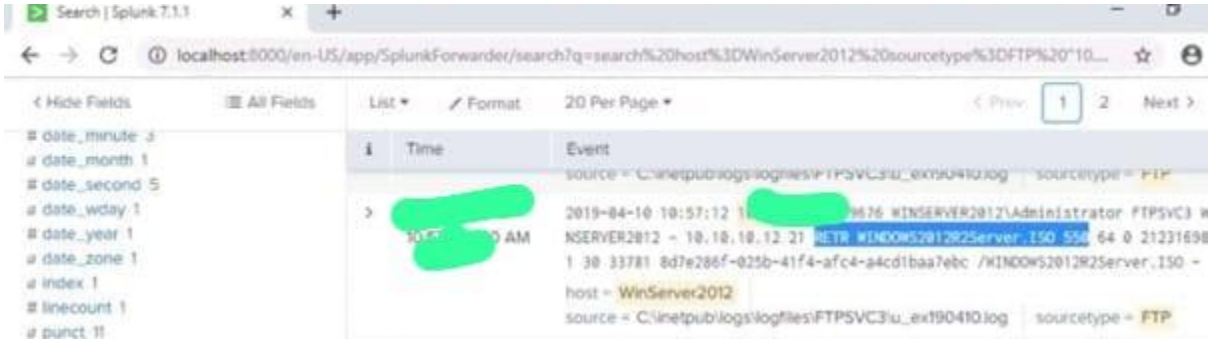
- FileZilla shows an **error**: Connection lost, partial file downloaded.

Check Logs in Splunk

- Back in SIEM → Splunk search:

host=WinServer2012 sourcetype=FTP ""

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



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.

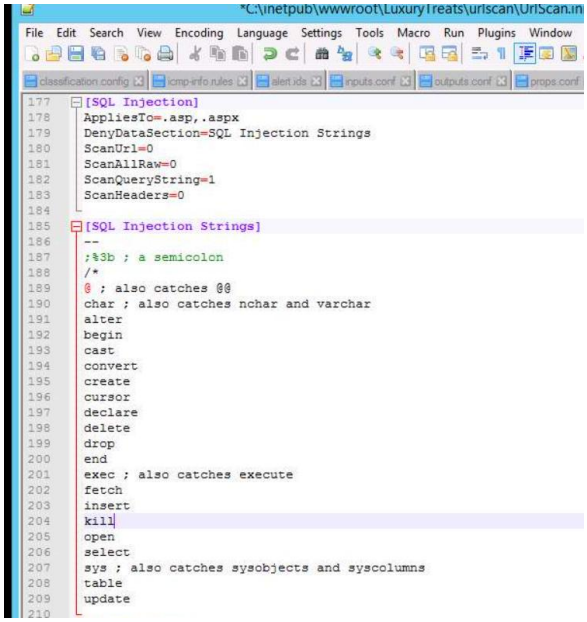
Create SQL Injection Filter Rule

3. Edit UrlScan.ini

Edit it

Add SQL Injection Rule

Add this **after line 175**



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

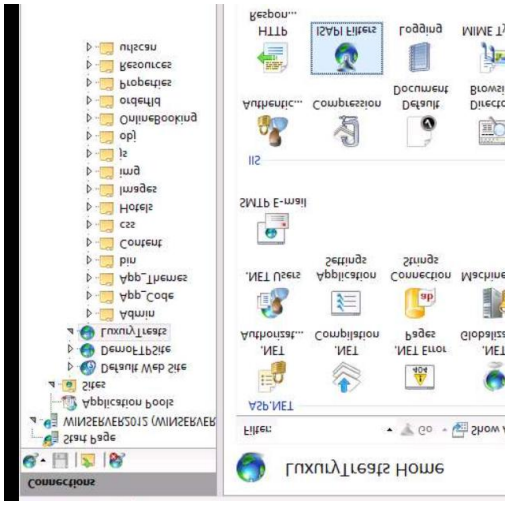
- In the left pane (Connections), expand:
    - Sites → Click LuxuryTreats
- In the middle pane (Home), double-click **ISAPI Filters**

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.

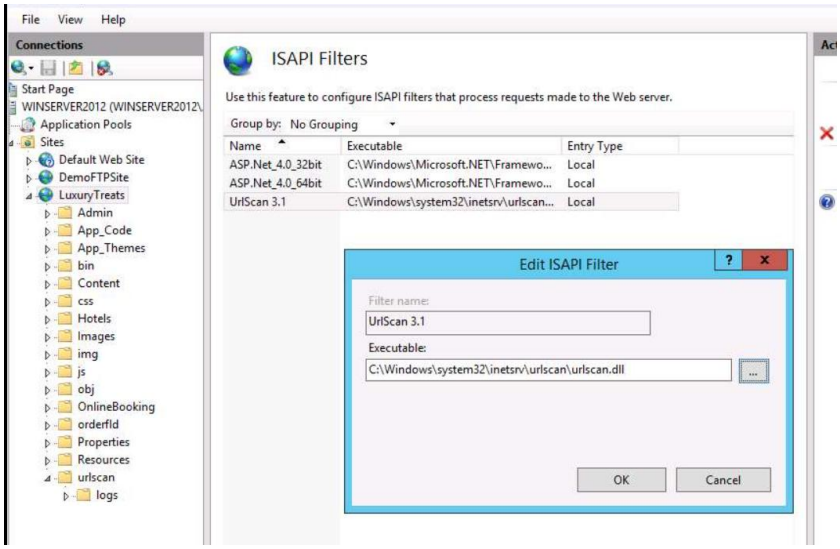


- Click **UrlScan 3.1** → In right pane click **Edit**

Set DLL Path

C:\inetpub\wwwroot\LuxuryTreats\urlscan

- Select: urlscan.dll → Click OK



Restart IIS

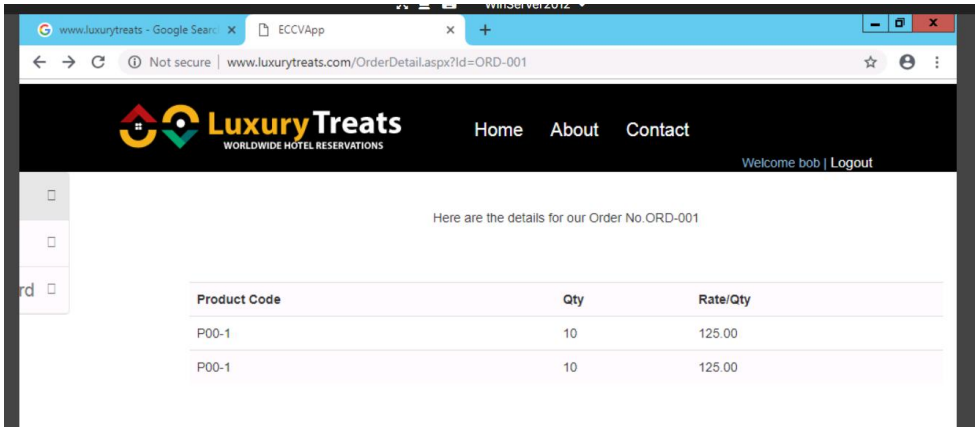
- On the left pane, click the top-level server: WINSERVER2012
- On right pane → click **Restart**

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.

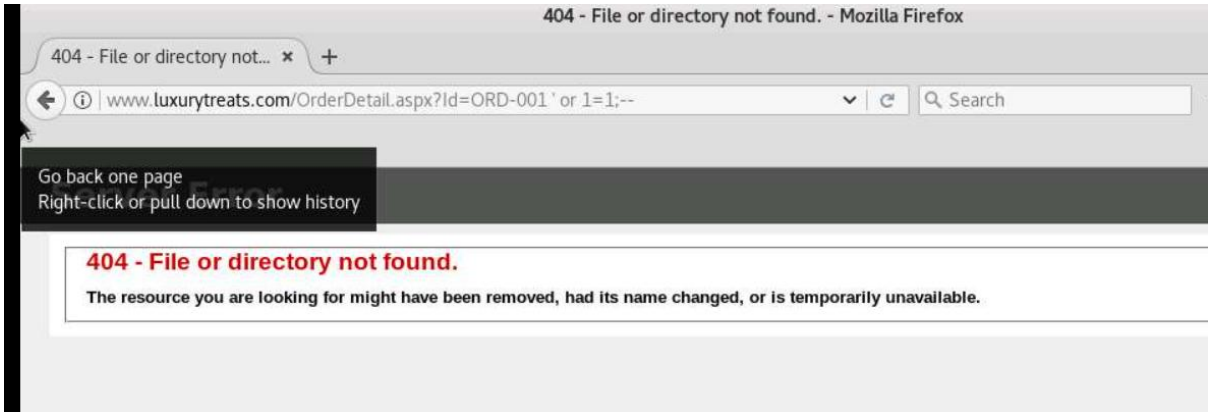


As per standard security practice, only authorized person should see their personal data. If person can see other's order details, then it can be considered as security breach. This can be possible using SQL Injection technique. Attacker use this technique to bypass security measures of other user's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



Thrishank Reddy koppala

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.

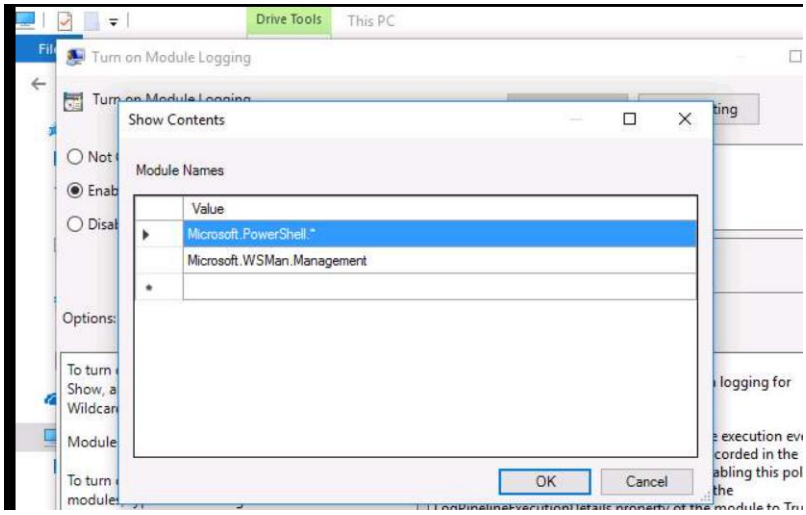
Steps to Configure Logging (on Windows10)

1. Enable PowerShell Logging

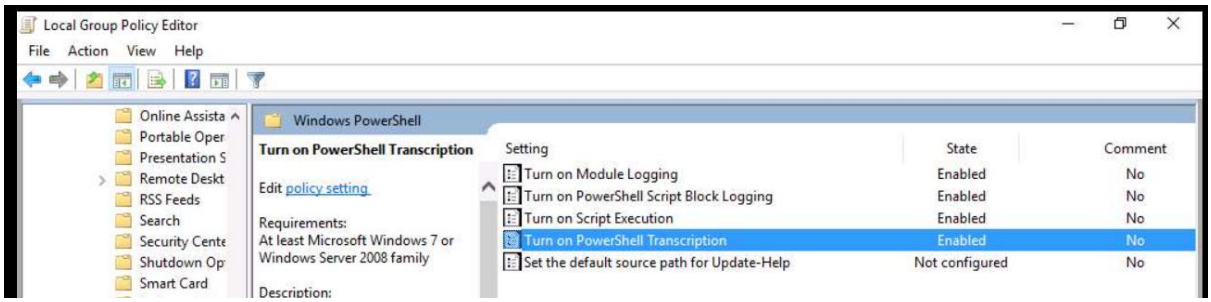
- Open: Edit group policy
- Navigate to:
  Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell

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**



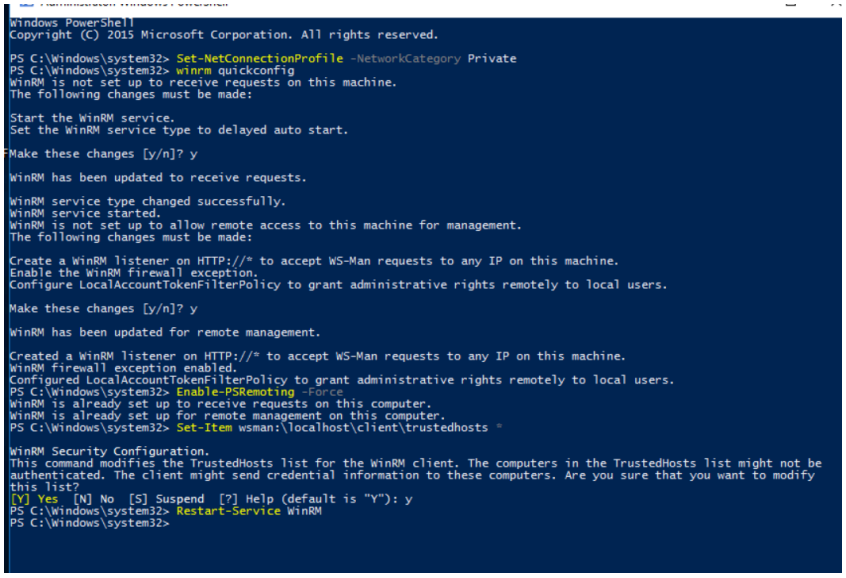
Turn on the enable



Enable PowerShell Remoting on Both Machines

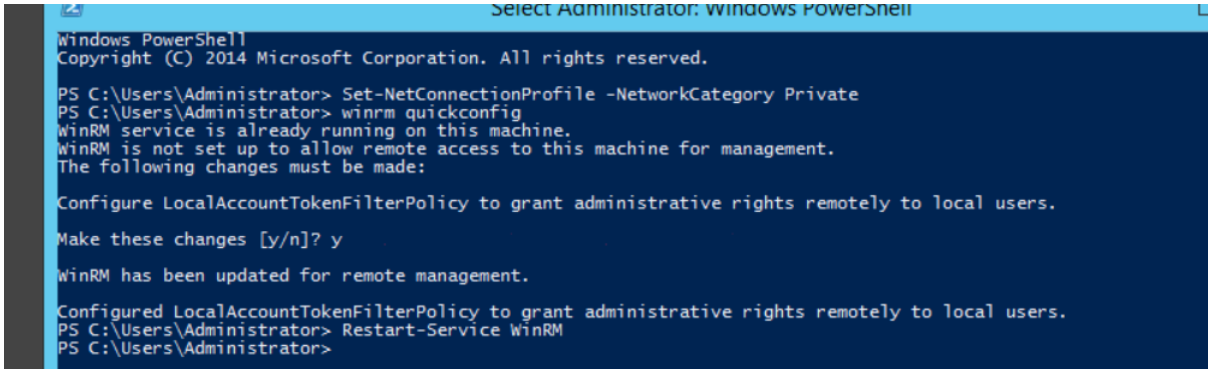
Windows10:

- 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



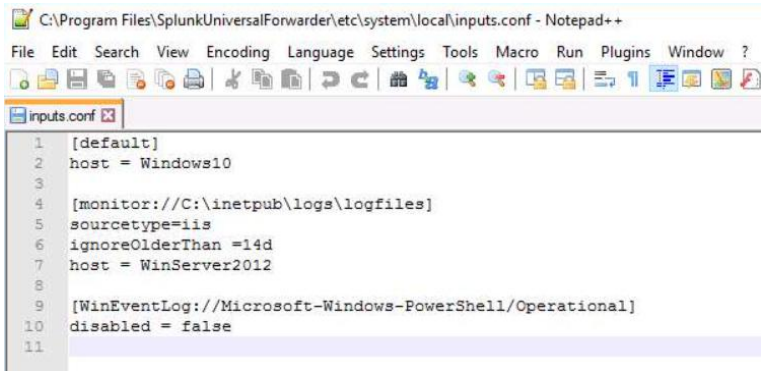
WinServer2012:

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



Configure Splunk Forwarder on Windows10

1. **Edit inputs.conf**



2. Restart SplunkForwarder service

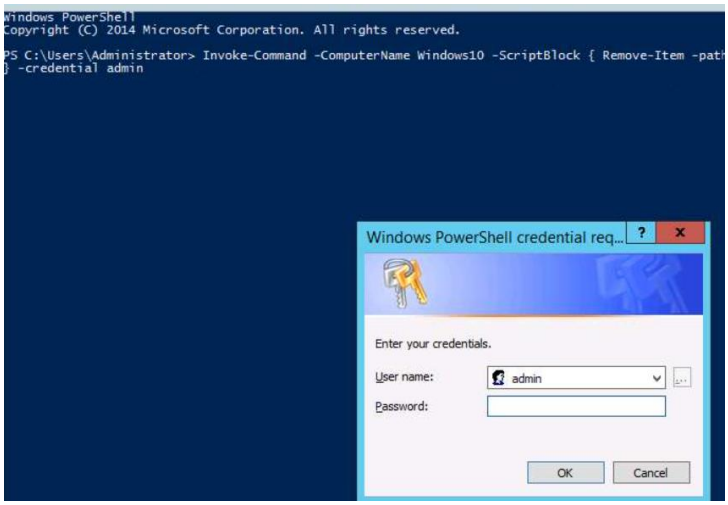
- Search: Services
- Restart: SplunkForwarder

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



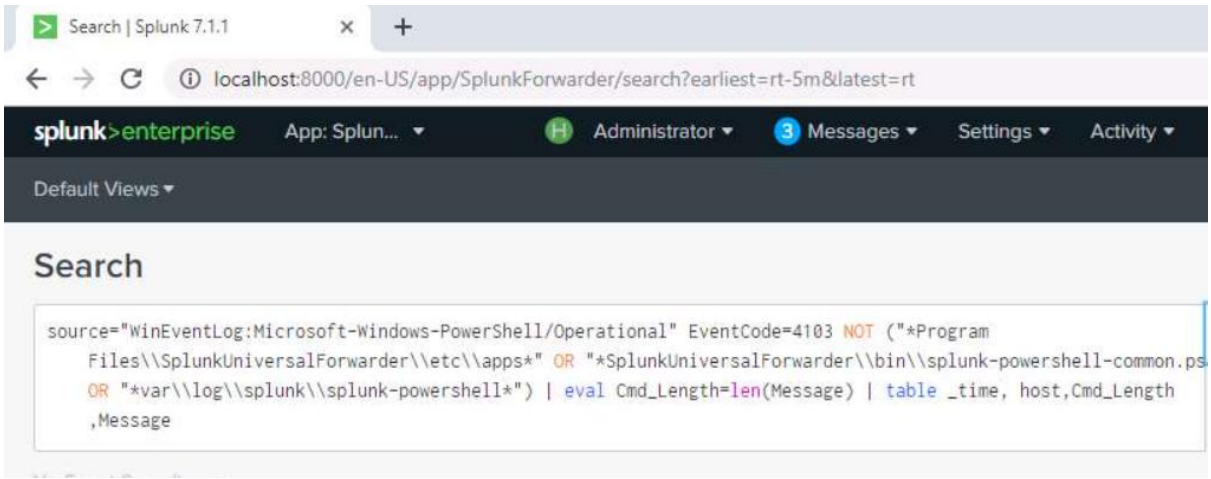
If you Type the password (***)for admin user in the displayed dialog box and click **OK**. On successful execution of the command, **MyFolder** folder will be deleted from **Windows10** system.

- **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



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

ormat

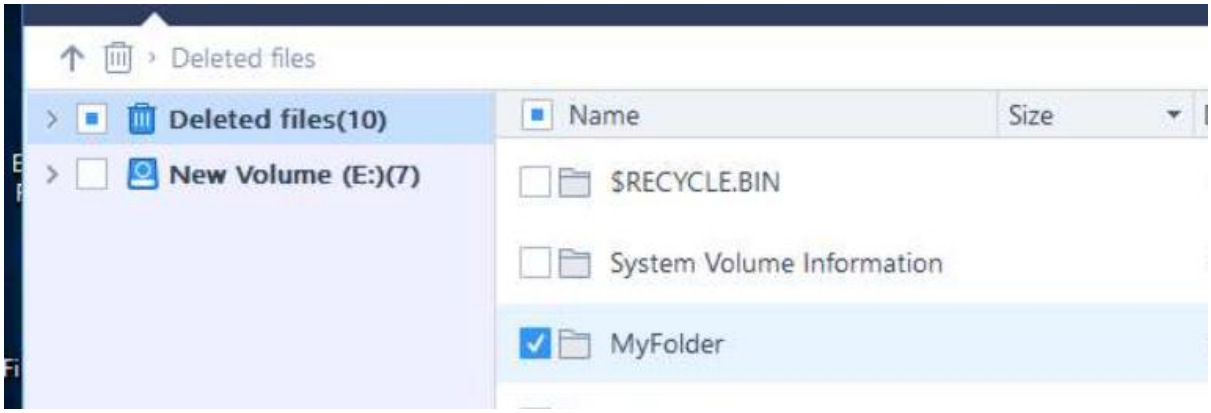
host	Cmd_Length	Message
Windows10	1022	CommandInvocation(Remove-Item): "Remove-Item" ParameterBinding(Remove-Item): name="Path"; value="E:\MyFolder" ParameterBinding(Remove-Item): name="Recurse"; value="True" CommandInvocation(Out-Default): "Out-Default" ParameterBinding(Out-Default): name="Transcript"; 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

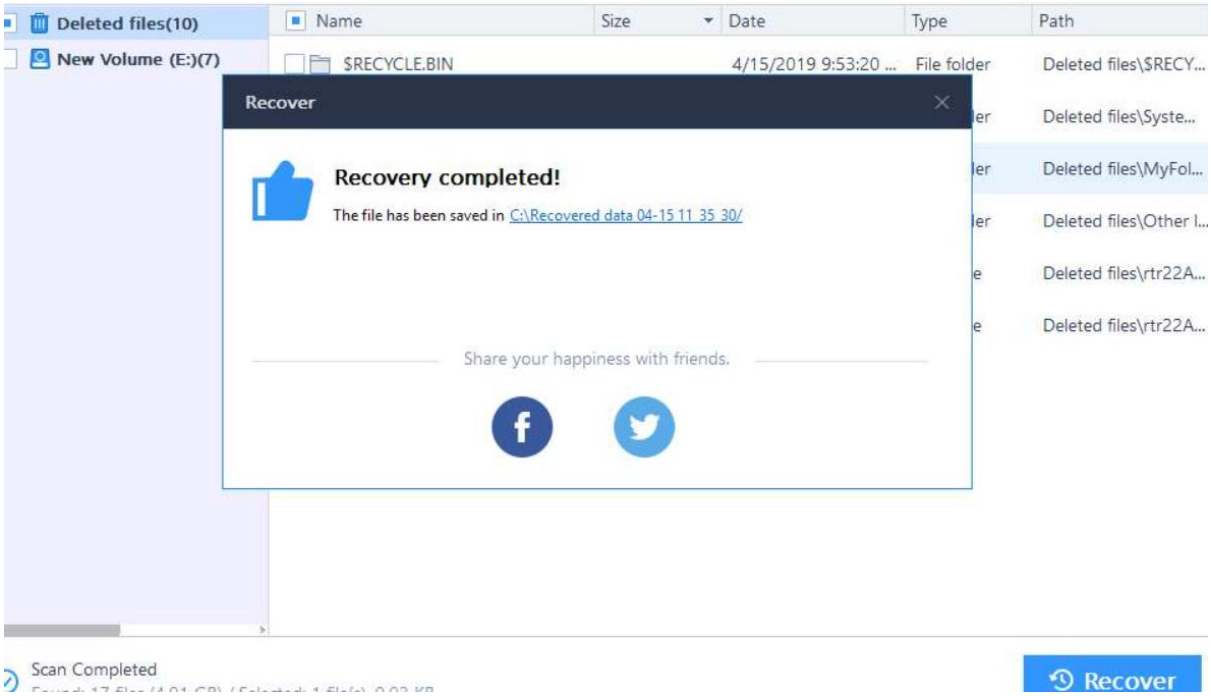
Scan and Recover:

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

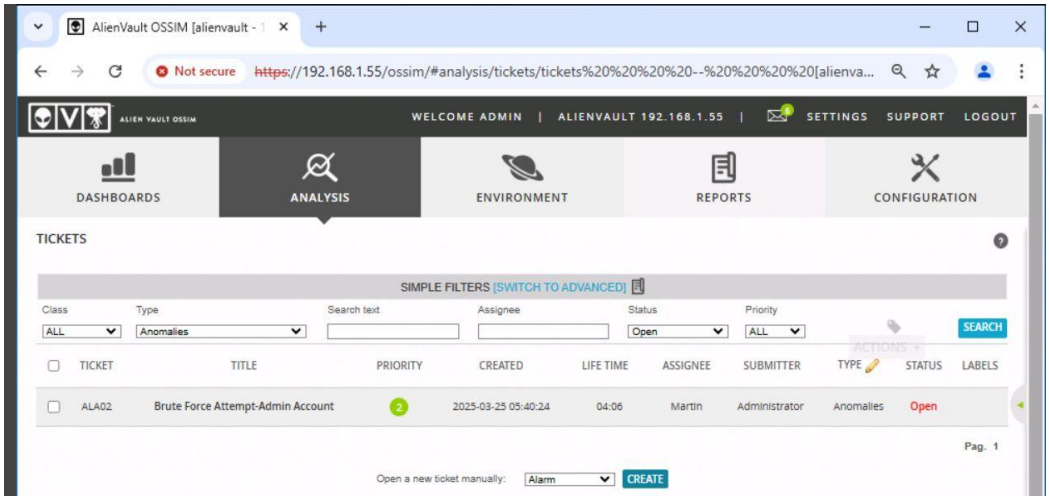


Thrishank Reddy koppala

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.

Thrishank Reddy koppala