

Log analysis report

Image 1

```
Sample Request:
GET /sample.aspx?country=United+States'+or+!/**/cOnVeRt(int,(!+~+!+(!/**/cAsT(@@version+as+char))+!+~+!))+and+'1'='1 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Referer: http://www.samplepayload.com/sample.aspx?country=United+States'+or+!/**/cOnVeRt(int,(!+~+!+(!/**/cAsT(@@version+as+char))+!+~+!))+a
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pt-PT; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2 (.NET CLR 3.5.30729)
Host: www.samplepayload.com
Connection: Keep-Alive

Sample Response:
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 874
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Thu, 09 Mar 2017 14:53:46 GMT

<h3>Can't load Web page. <br>Error:
Conversion failed when converting the varchar value '!'~!Microsoft SQL Server 2008 R2 (!~! to data type int.</h3><br><br>
```

- **Sample request:**

Here host makes a request to

<http://www.samplepayload.com/sample.aspx?country=United+states>

Actually here make a SQL query for knowing the server version.

In this case, the parameter is 'country' and the value is 'United+states'.

Operating system: Windows NT 5.1 = Windows XP

- **Sample response:**

Here status code is 200, so this is a successful status.

And we can see that on the response page there has a piece of important information and that is the server version.

Server name: Microsoft SQL Server 2008 R2

This server has many CVEs. Such as-

[2017-0148](#)

[2017-0147](#)

[2017-0146](#)

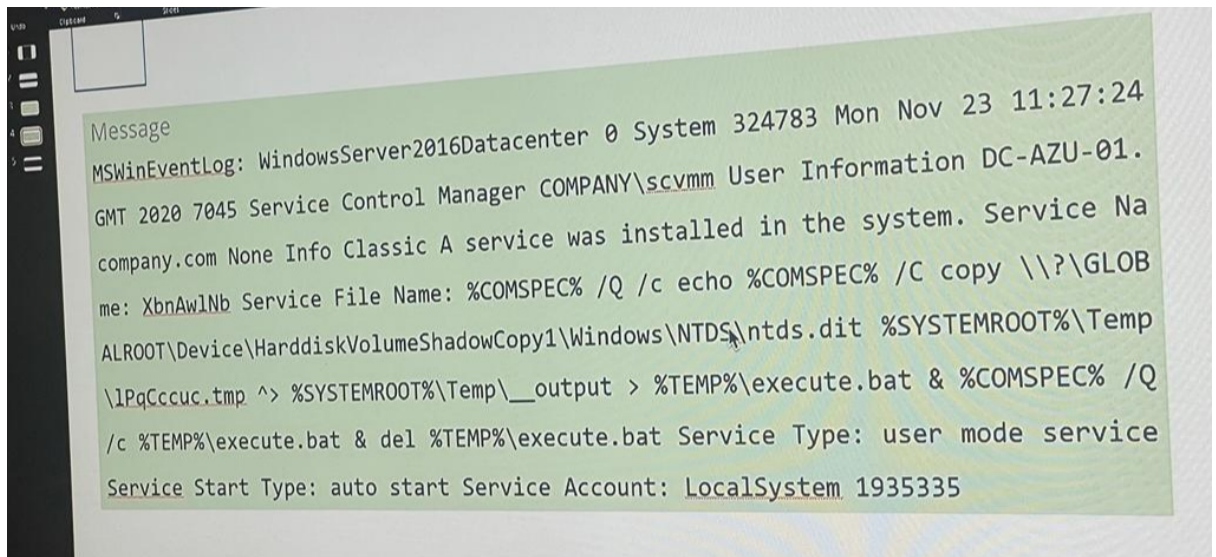
[2017-0145](#)

[2017-0144](#)

[2017-0143](#)

Ref: <https://www.exploit-db.com/exploits/41987>

□ Image 2



MSWinEventLog:

This is the windows event log. Here a service was installed by the DC-AZU-01.company.com

Service control manager: COMPANY\scvmm

Service name: XbnAwlNb

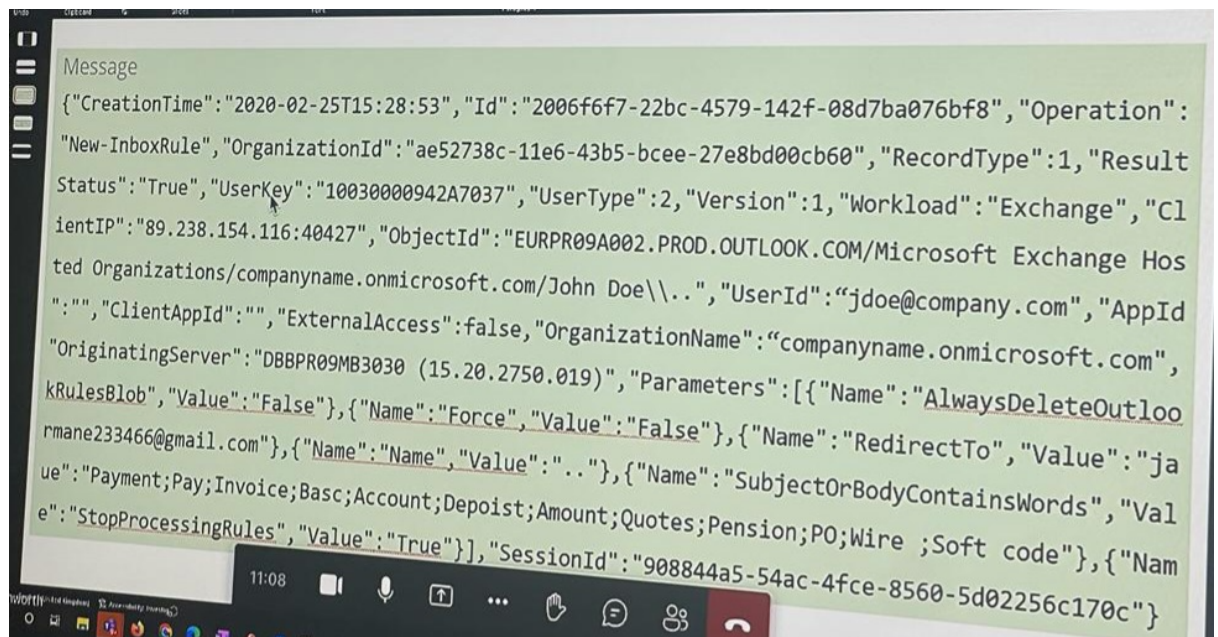
Service account: LocalSystem 1935335

OS: Windows server 2016

Which is executed from the administrator cmd prompt or /windows/system32

This service has not matched any service of windows. So this is totally anonymous service. So, this is malicious.

Image 3



This is also an event log content.

ClientIP: 89.238.158.116

- IP address: **89.238.158.116**
- City: **Burnley**
- Region name: Lancashire
- Country name: United Kingdom
- Life Expectancy: 77.7
- Avg income: **23,117** EUR
- Timezone: Europe/London
- Sub continent: British Islands
- Country code: GB
- Geo-targeting: **true**
- Latitude: 53.8055
- Longitude: -2.2927

Port: 40427

UserID: jdoe@company.com

OS: Windows

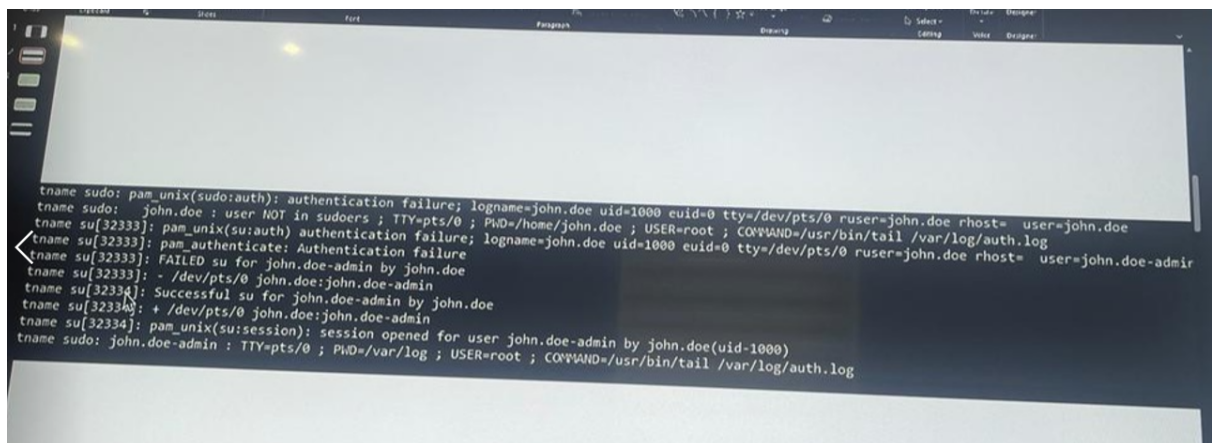
Here just create a session. And the important session parameter is:

Name: SubjectOrBodyContainsWords

Value: Payment; pay etc

And here also have a session ID.

Image 4:



This is auth or authentication log.

Operating System: Linux

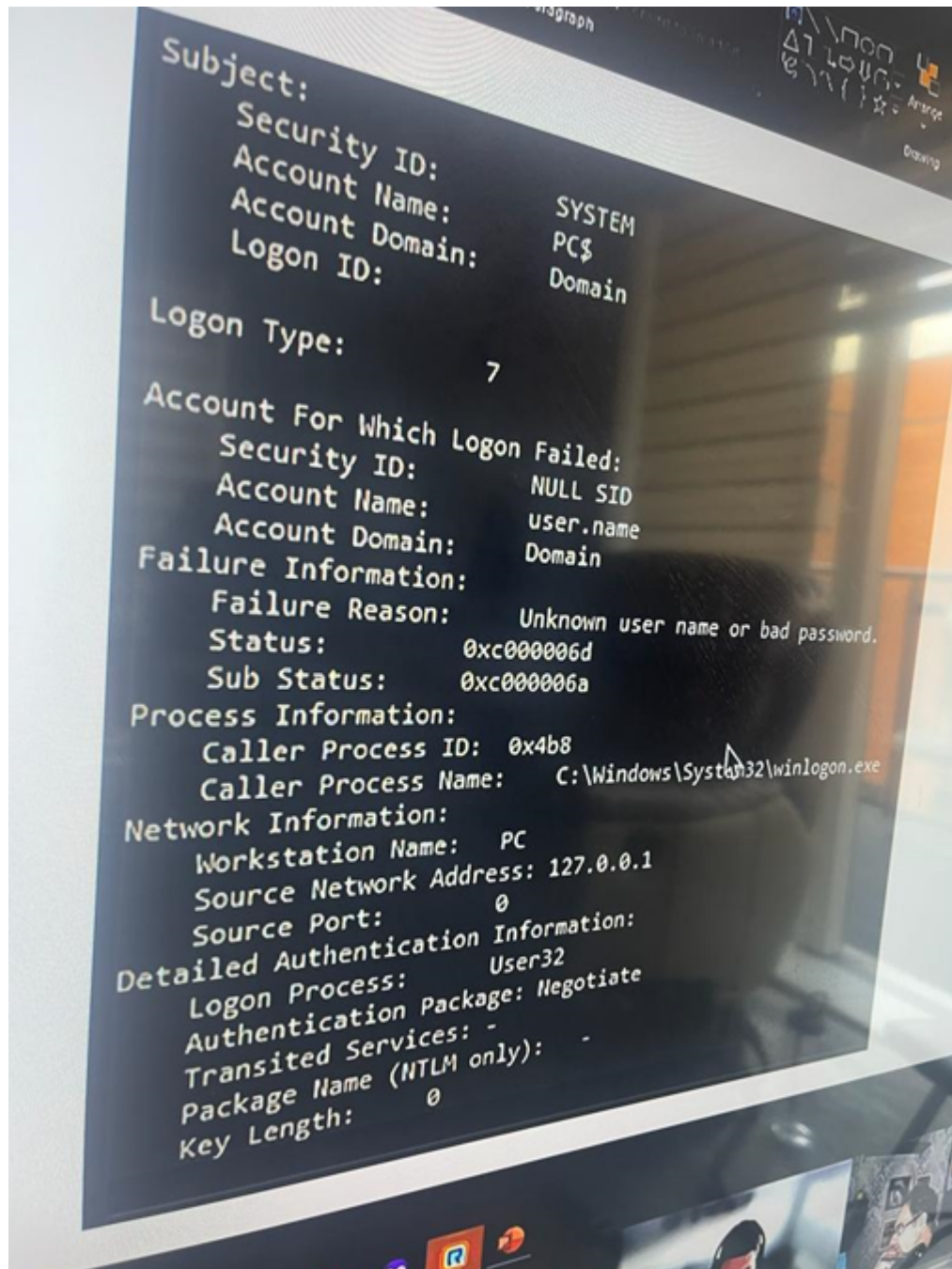
Here we see two users.

1/ john.doe => who is not su or superuser or administrator user

2/ john.doe-admin => who is su or superuser or administrator user.

And we know super user can access the /var/log/auth.log file.

Image 5:



Here we can see the winlogon.exe processing activity. And this is a Syslog.

Operating System: Windows

responsible for handling the secure attention sequence, and loading the user profile on logon.

winlogon.exe is associated with Windows Operating System developed by Microsoft Corporation. It is located in C:\Windows\System32 by default. Malware programmers create files with virus scripts and name them after the winlogon.exe virus with the intention to spread the virus on the internet.

- But here we can see that there has to happen a failed authentication.