windows溯源取证,应急响应案例:tryhackme之 Investigating Windows

原创

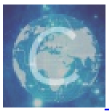
唐仔橙 已于 2022-04-13 20:25:30 修改 2255 收藏

分类专栏： web安全 网络安全入门 tryhackme 文章标签： 安全 web安全 网络安全

于 2022-04-13 19:40:15 首次发布

本文链接：https://blog.csdn.net/qq_43200143/article/details/124155768

版权


web安全 同时被 3 个专栏收录

11 篇文章 1 订阅

订阅专栏

网络安全入门

11 篇文章 0 订阅

订阅专栏

tryhackme

12 篇文章 1 订阅

订阅专栏

文章目录

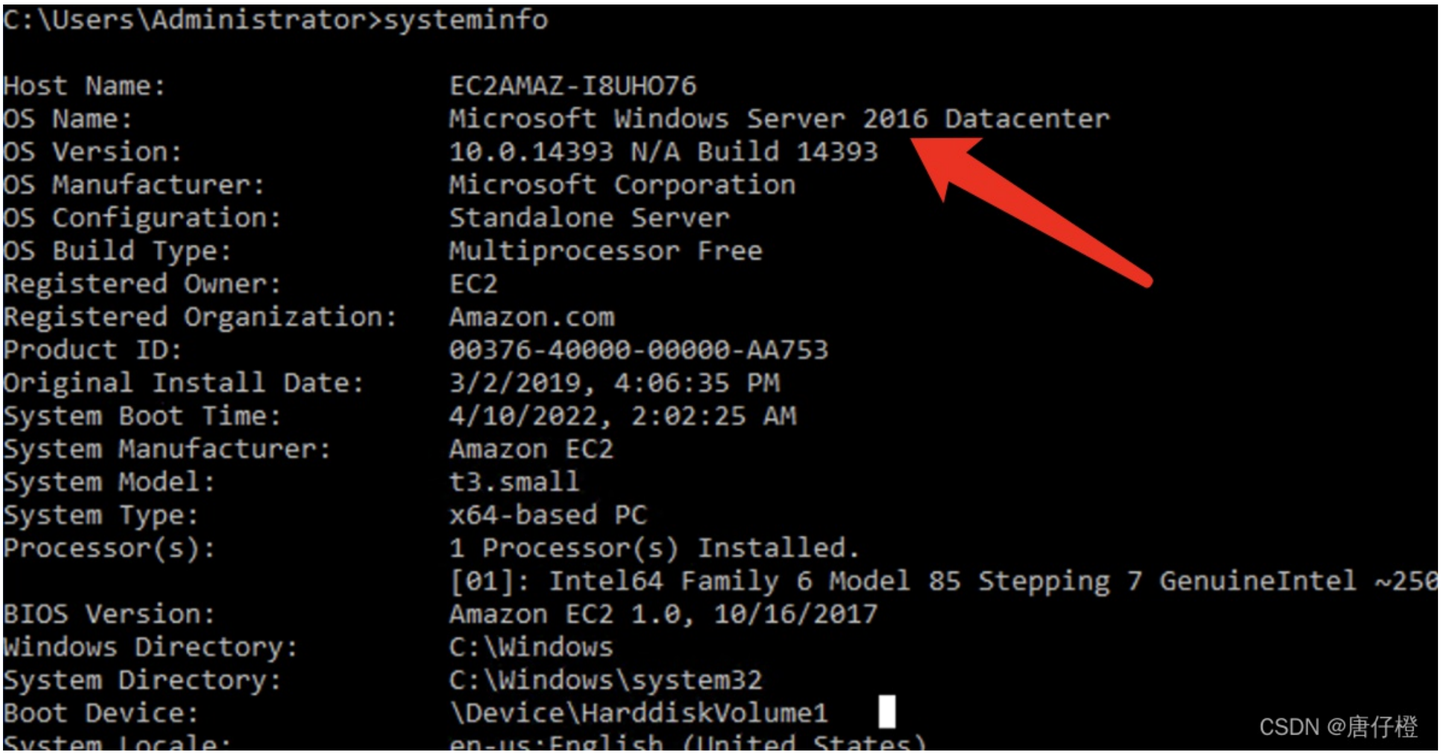
Investigating Windows

tryhackme的一个房间,一个windows应急响应案例.

我们登陆到一台被入侵的windows机器,要对他进行溯源取证.

Whats the version and year of the windows machine?

systeminfo



```
C:\Users\Administrator>systeminfo

Host Name:                 EC2AMAZ-I8UHO76
OS Name:                   Microsoft Windows Server 2016 Datacenter
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          EC2
Registered Organization:   Amazon.com
Product ID:                00376-40000-00000-AA753
Original Install Date:     3/2/2019, 4:06:35 PM
System Boot Time:          4/10/2022, 2:02:25 AM
System Manufacturer:       Amazon EC2
System Model:              t3.small
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~250
BIOS Version:              Amazon EC2 1.0, 10/16/2017
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
```

Which user logged in last?

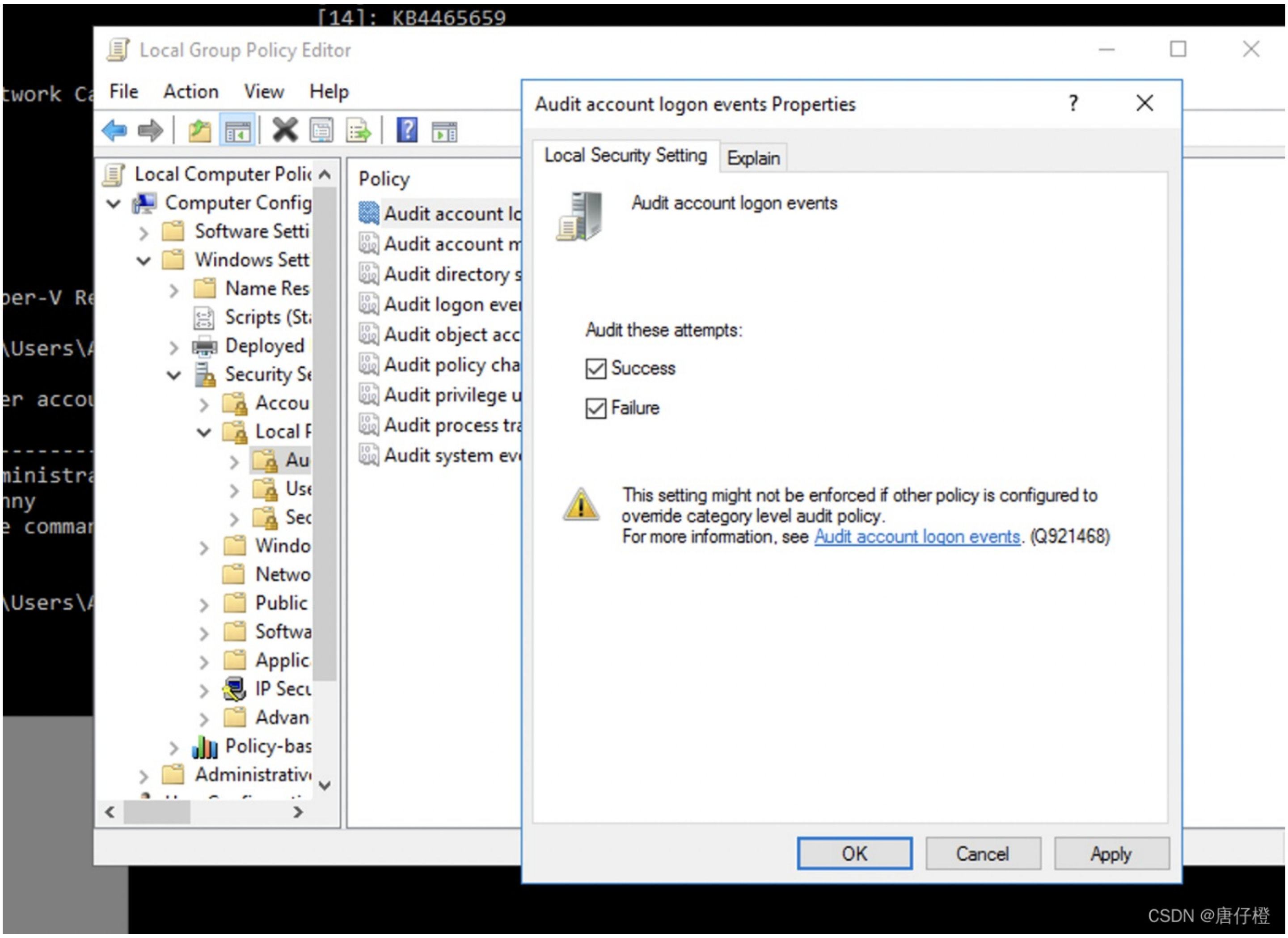
查找用户登陆记录

1.运行,输入: gpedit.msc

2.“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“审核策略”，双击其中的“审核帐户登陆事件”

==>审核登录事件–>勾上成功/失败–>点击应用–>点击确定

3.控制面板–>系统和安全–>查看事件日志–>事件查看器–>windows日志–>安全，便可以看到用户的登录和注销以及账户名等信息



```
[14]: KB4465659
twork Ca
per-V Re
\Users\A
er accou
--------
ministra
nny
e comman
\Users\A
```

Audit account logon events Properties

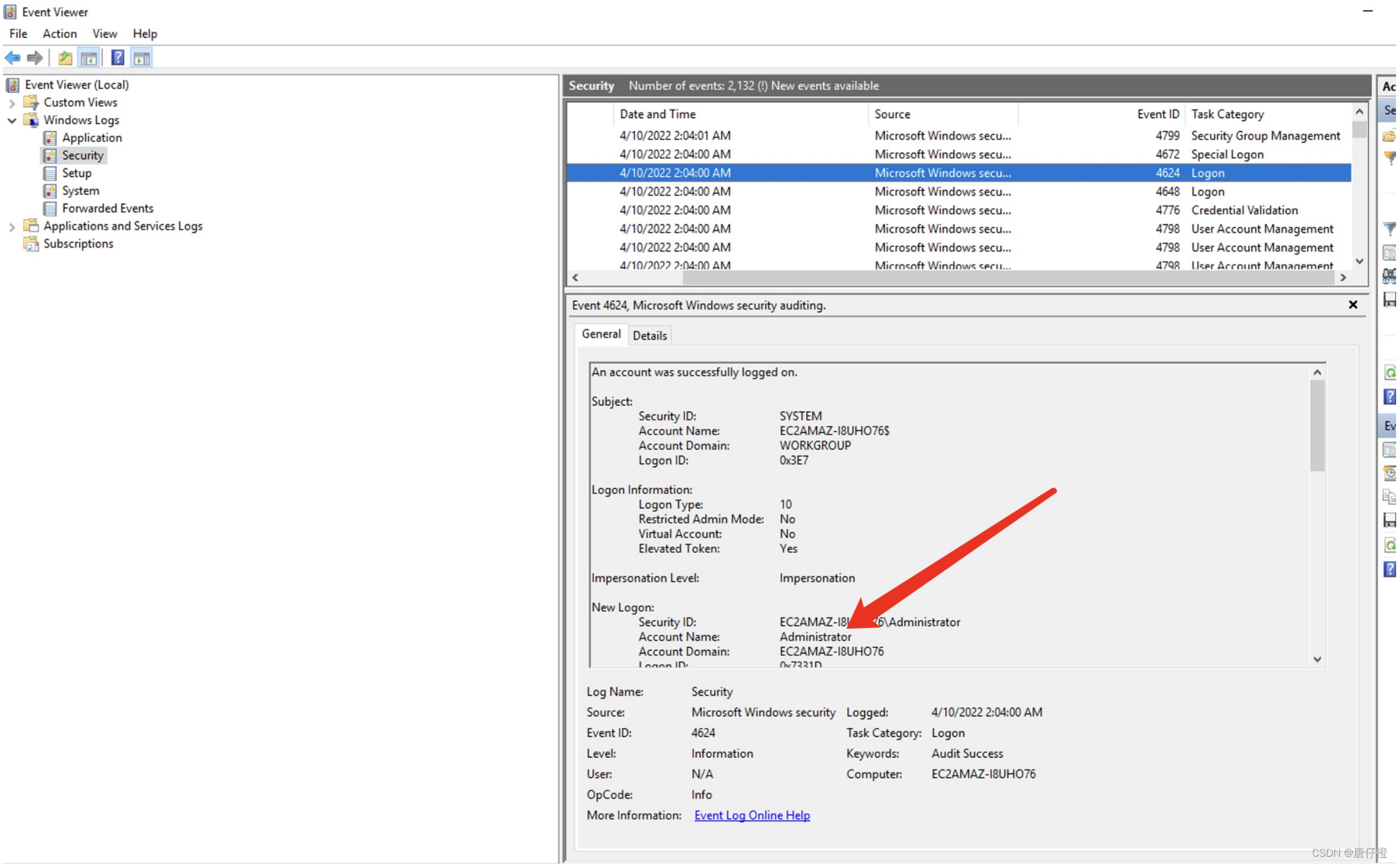
Audit account logon events

Audit these attempts:

☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)



Security Number of events: 2,132 (!) New events available

Date and Time	Source	Event ID	Task Category
4/10/2022 2:04:01 AM	Microsoft Windows secu...	4799	Security Group Management
4/10/2022 2:04:00 AM	Microsoft Windows secu...	4672	Special Logon
4/10/2022 2:04:00 AM	Microsoft Windows secu...	4624	Logon
4/10/2022 2:04:00 AM	Microsoft Windows secu...	4648	Logon
4/10/2022 2:04:00 AM	Microsoft Windows secu...	4776	Credential Validation
4/10/2022 2:04:00 AM	Microsoft Windows secu...	4798	User Account Management
4/10/2022 2:04:00 AM	Microsoft Windows secu...	4798	User Account Management
4/10/2022 2:04:00 AM	Microsoft Windows secu...	4798	User Account Management

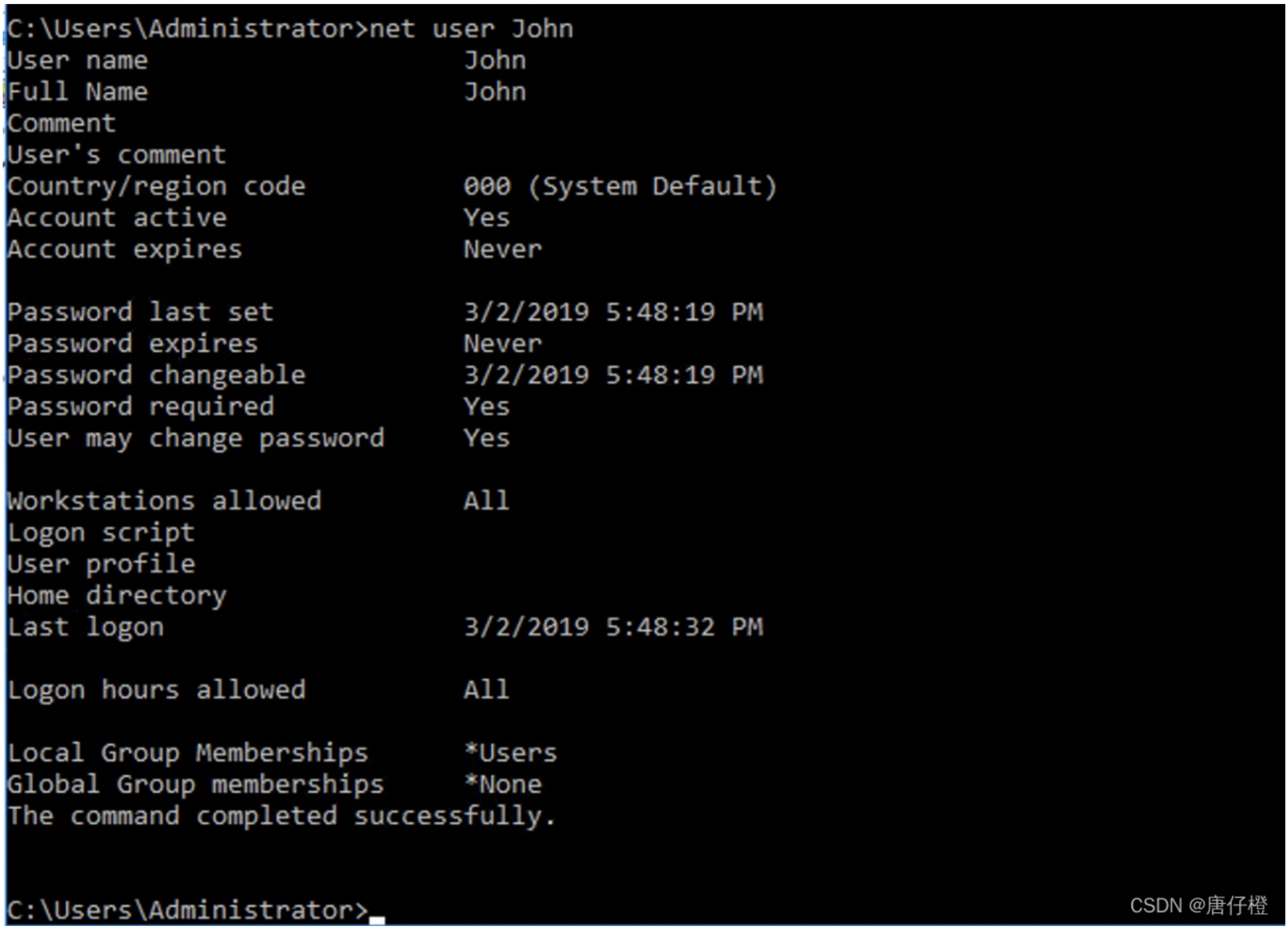
Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           EC2AMAZ-I8UHO76$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             10
        Restricted Admin Mode:  No
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            EC2AMAZ-I8UHO76\Administrator
        Account Name:           Administrator
        Account Domain:         EC2AMAZ-I8UHO76
        Logon ID:               0x7331D
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/10/2022 2:04:00 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EC2AMAZ-I8UHO76
OpCode:	Info		
More Information:	Event Log Online Help		

When did John log onto the system last?

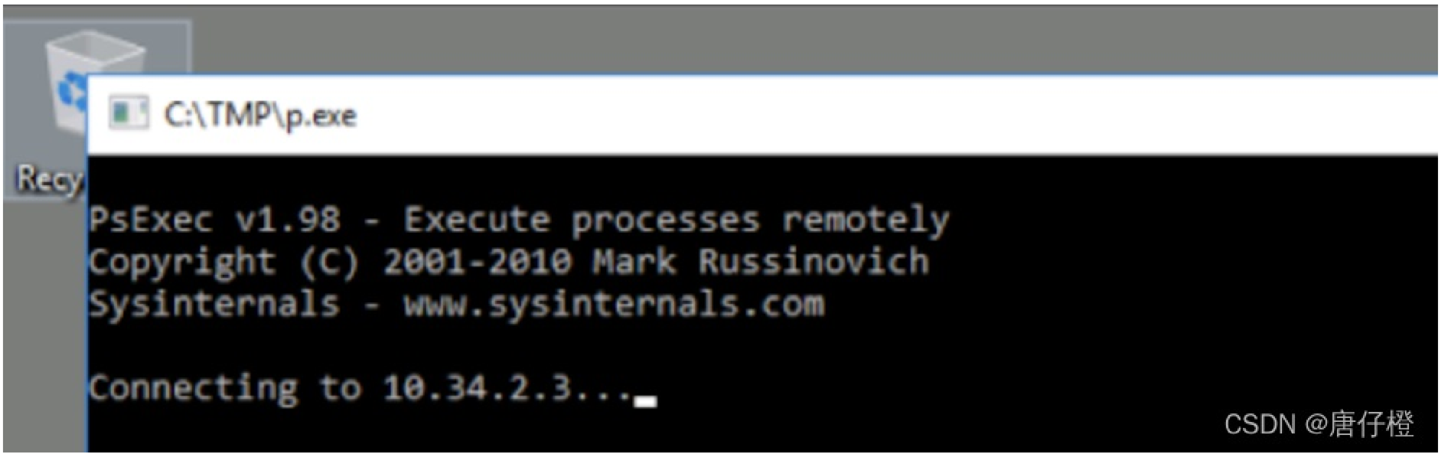
net user John 可以查看这个用户的信息



```
C:\Users\Administrator>net user John
User name                    John
Full Name                    John
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/2/2019 5:48:19 PM
Password expires             Never
Password changeable          3/2/2019 5:48:19 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/2/2019 5:48:32 PM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\Administrator>_
```

What IP does the system connect to when it first starts?

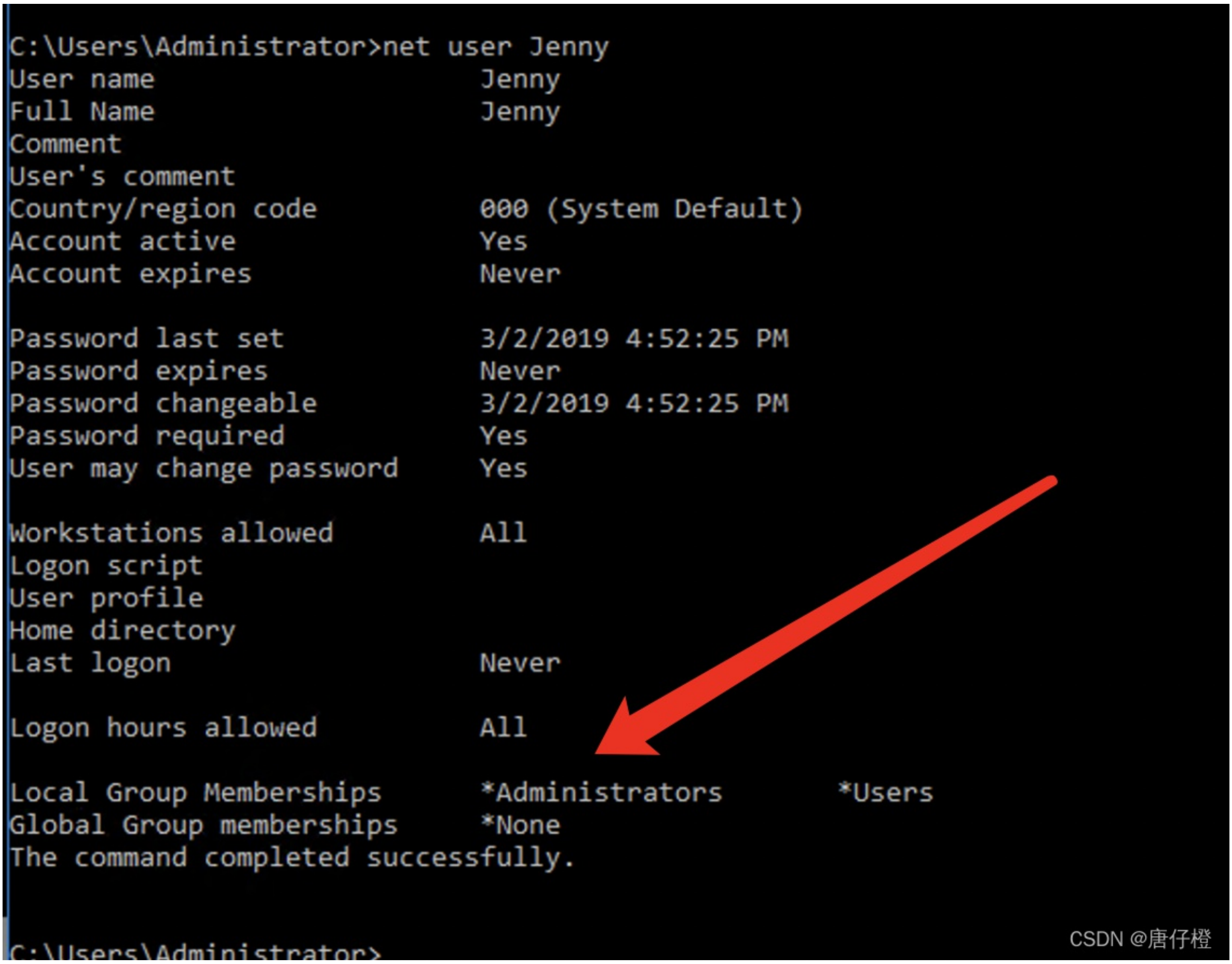
这个容易忽略了,刚开始开机的时候有个窗口,不要轻易关掉



```
PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to 10.34.2.3..._
```

What two accounts had administrative privileges (other than the Administrator user)?

Jenny,Guest

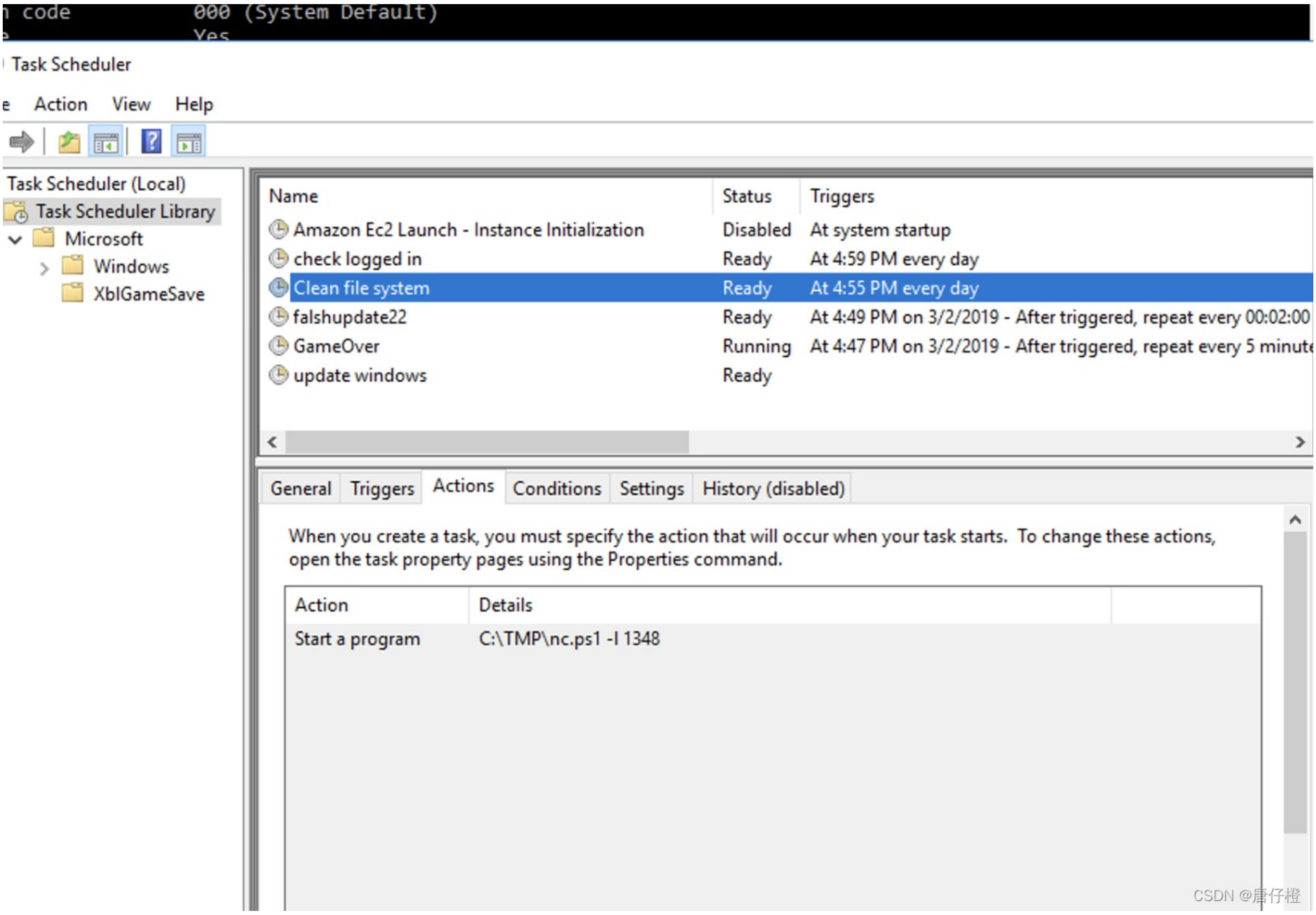


```
C:\Users\Administrator>net user Jenny
User name                    Jenny
Full Name                    Jenny
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/2/2019 4:52:25 PM
Password expires             Never
Password changeable          3/2/2019 4:52:25 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\Administrator>
```

Whats the name of the scheduled task that is malicous.

查看计划任务

命令行:taskschd.msc



```
n code          000 (System Default)
e               Yes
```

Name	Status	Triggers
Amazon Ec2 Launch - Instance Initialization	Disabled	At system startup
check logged in	Ready	At 4:59 PM every day
Clean file system	Ready	At 4:55 PM every day
falshupdate22	Ready	At 4:49 PM on 3/2/2019 - After triggered, repeat every 00:02:00
GameOver	Running	At 4:47 PM on 3/2/2019 - After triggered, repeat every 5 minute
update windows	Ready	

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\TMP\nc.ps1 -l 1348

What file was the task trying to run daily?

nc.ps1

What port did this file listen locally for?

1348 -l参数就是指定本地监听端口

When did Jenny last logon?

net user Jenny查看

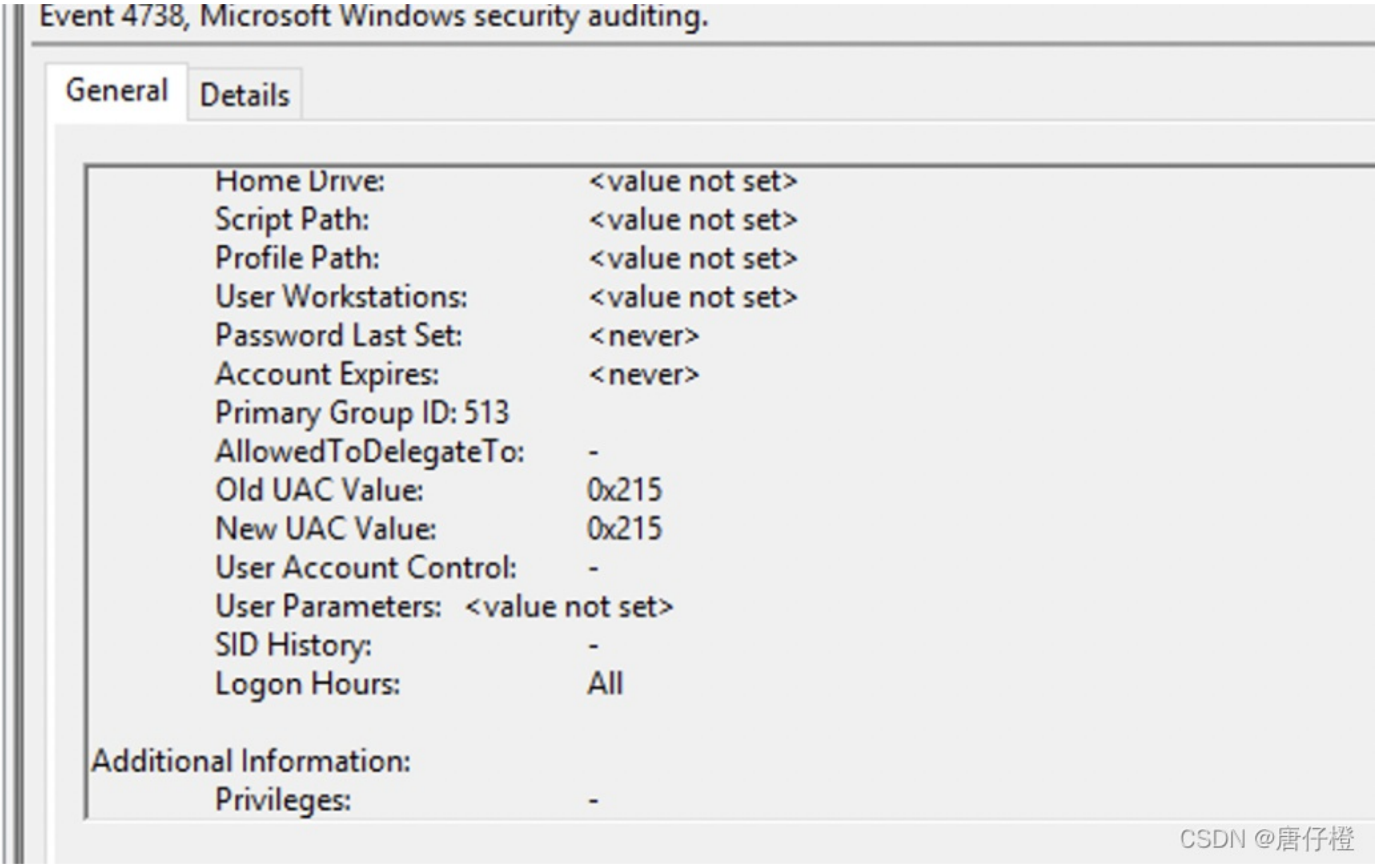
At what date did the compromise take place?

什么时候被入侵的…这个怎么看呀.要看通过什么漏洞打进来的?

根据账号Jenny的创建时间 还有呢?

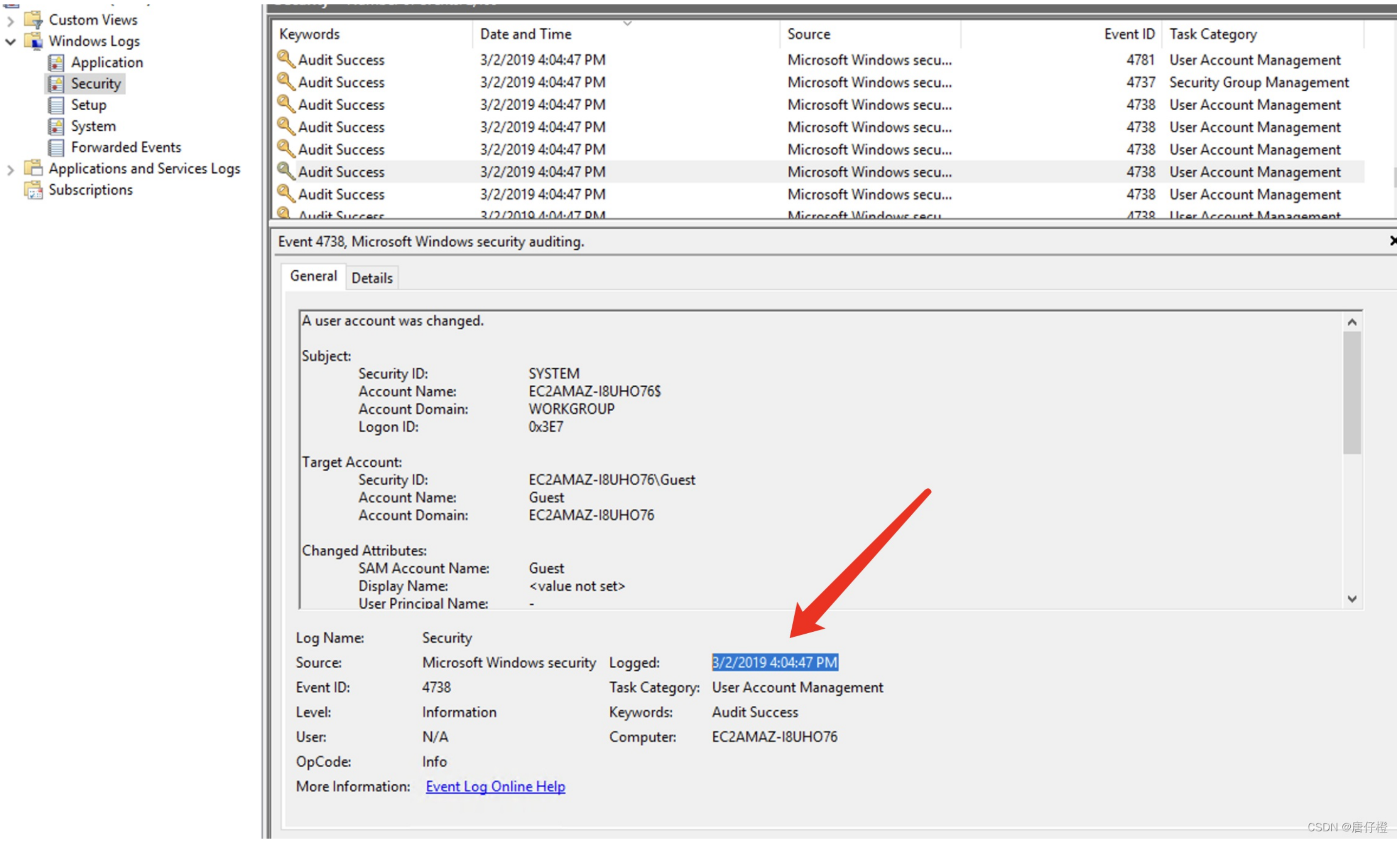
At what time did Windows first assign special privileges to a new logon?

这个意思是什么时候给普通用户 管理员权限的,这个应该可以看日志吧.



Event 4738, Microsoft Windows security auditing.

```
Home Drive:             <value not set>
Script Path:            <value not set>
Profile Path:           <value not set>
User Workstations:      <value not set>
Password Last Set:      <never>
Account Expires:        <never>
Primary Group ID: 513
AllowedToDelegateTo:    -
Old UAC Value:          0x215
New UAC Value:          0x215
User Account Control:   -
User Parameters:   <value not set>
SID History:            -
Logon Hours:            All

Additional Information:
Privileges:             -
```



Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4781	User Account Management
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4737	Security Group Management
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4738	User Account Management
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4738	User Account Management
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4738	User Account Management
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4738	User Account Management
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4738	User Account Management
Audit Success	3/2/2019 4:04:47 PM	Microsoft Windows secu...	4738	User Account Management

Event 4738, Microsoft Windows security auditing.

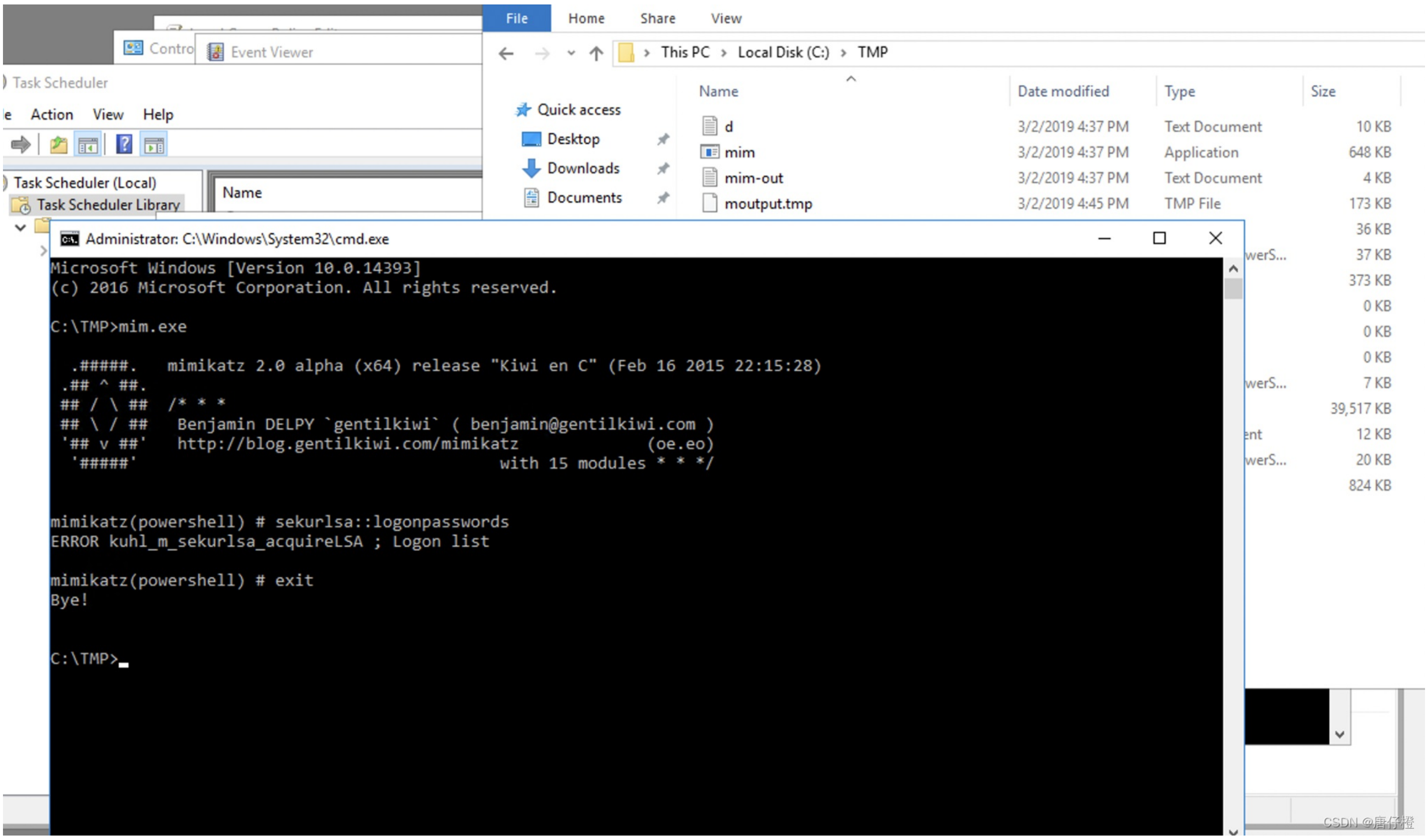
```
A user account was changed.

Subject:
        Security ID:            SYSTEM
        Account Name:           EC2AMAZ-I8UHO76$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Target Account:
        Security ID:            EC2AMAZ-I8UHO76\Guest
        Account Name:           Guest
        Account Domain:         EC2AMAZ-I8UHO76

Changed Attributes:
        SAM Account Name:       Guest
        Display Name:           <value not set>
        User Principal Name:    -
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	3/2/2019 4:04:47 PM
Event ID:	4738	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EC2AMAZ-I8UHO76
OpCode:	Info		
More Information:	Event Log Online Help		

What tool was used to get Windows passwords?

在攻击者留下的目录中寻找

mimikatz



Name	Date modified	Type	Size
d	3/2/2019 4:37 PM	Text Document	10 KB
mim	3/2/2019 4:37 PM	Application	648 KB
mim-out	3/2/2019 4:37 PM	Text Document	4 KB
moutput.tmp	3/2/2019 4:45 PM	TMP File	173 KB
			36 KB
		werS...	37 KB
			373 KB
			0 KB
			0 KB
			0 KB
		werS...	7 KB
			39,517 KB
		ent	12 KB
		werS...	20 KB
			824 KB

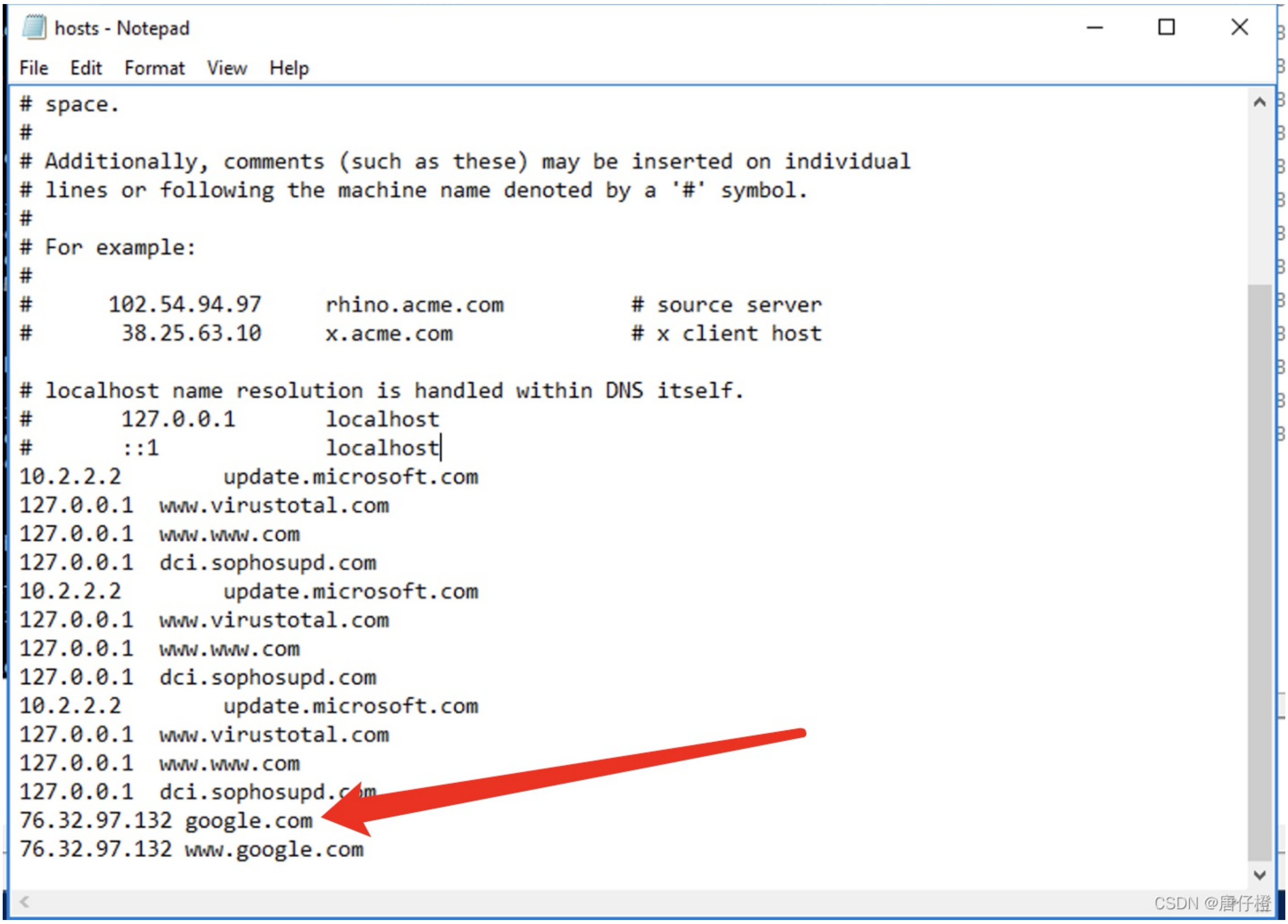
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\TMP>mim.exe

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                 with 15 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Logon list

mimikatz(powershell) # exit
Bye!


C:\TMP>_
```

What was the attackers external control and command servers IP?

找攻击者的c2ip地址

C:\Windows\System32\drivers\etc\hosts

将google的ip替换成了攻击者自己的

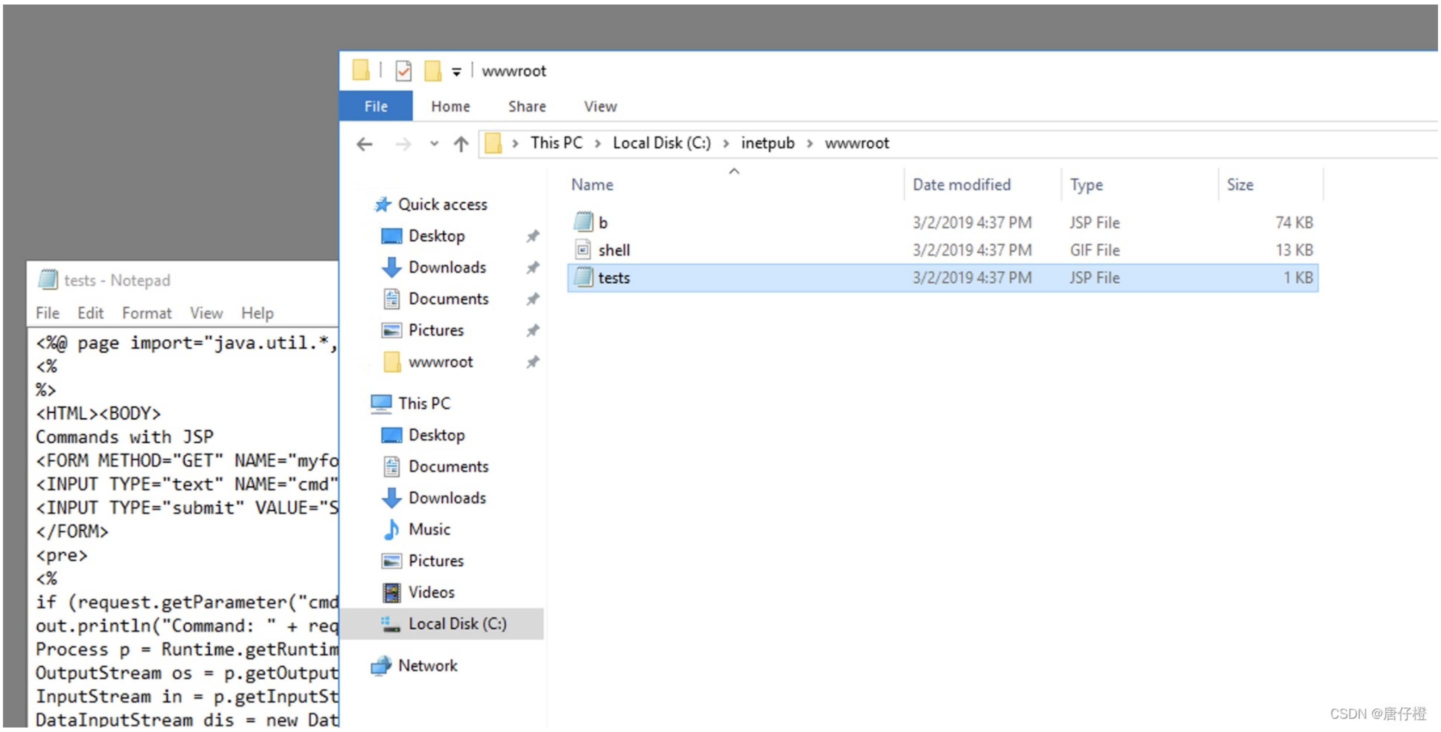


```
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
10.2.2.2        update.microsoft.com
127.0.0.1  www.virustotal.com
127.0.0.1  www.www.com
127.0.0.1  dci.sophosupd.com
10.2.2.2        update.microsoft.com
127.0.0.1  www.virustotal.com
127.0.0.1  www.www.com
127.0.0.1  dci.sophosupd.com
10.2.2.2        update.microsoft.com
127.0.0.1  www.virustotal.com
127.0.0.1  www.www.com
127.0.0.1  dci.sophosupd.com
76.32.97.132 google.com
76.32.97.132 www.google.com
```

What was the extension name of the shell uploaded via the servers website?

上传的webshell的后缀名.

找到web目录就会发现



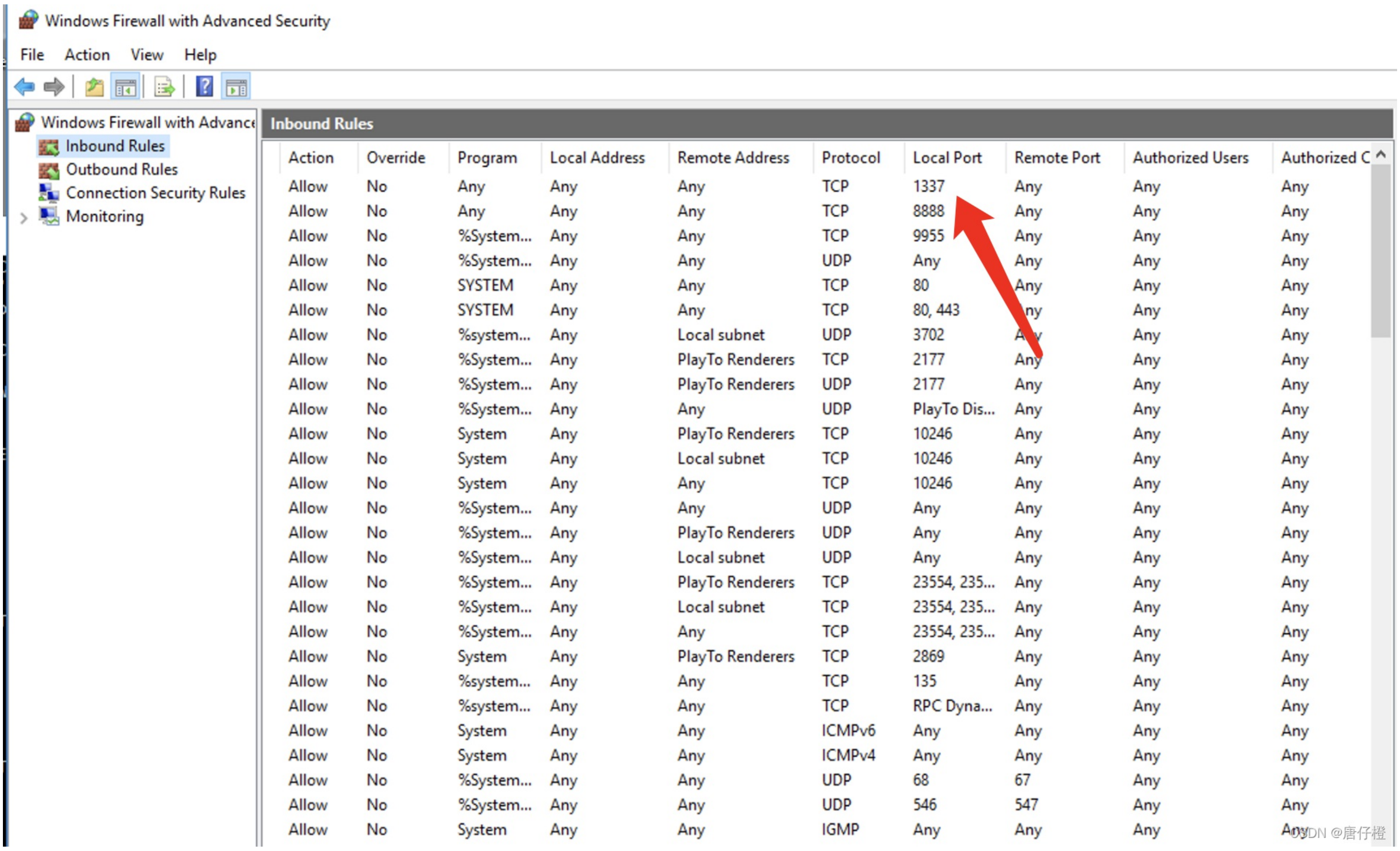
```
<%@ page import="java.util.*,
<%
%>
<HTML><BODY>
Commands with JSP
<FORM METHOD="GET" NAME="myfo
<INPUT TYPE="text" NAME="cmd"
<INPUT TYPE="submit" VALUE="S
</FORM>
<pre>
<%
if (request.getParameter("cmd
out.println("Command: " + req
Process p = Runtime.getRuntim
OutputStream os = p.getOutput
InputStream in = p.getInputSt
DataInputStream dis = new Dat
```

Name	Date modified	Type	Size
b	3/2/2019 4:37 PM	JSP File	74 KB
shell	3/2/2019 4:37 PM	GIF File	13 KB
tests	3/2/2019 4:37 PM	JSP File	1 KB

What was the last port the attacker opened?

查看最后开放的端口

防火墙里可以查看开放的端口,默认按照时间排序吗??



Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authorized C
Allow	No	Any	Any	Any	TCP	1337	Any	Any	Any
Allow	No	Any	Any	Any	TCP	8888	Any	Any	Any
Allow	No	%System...	Any	Any	TCP	9955	Any	Any	Any
Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any
Allow	No	SYSTEM	Any	Any	TCP	80	Any	Any	Any
Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any	Any	Any
Allow	No	%system...	Any	Local subnet	UDP	3702	Any	Any	Any
Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any	Any
Allow	No	%System...	Any	PlayTo Renderers	UDP	2177	Any	Any	Any
Allow	No	%System...	Any	Any	UDP	PlayTo Dis...	Any	Any	Any
Allow	No	System	Any	PlayTo Renderers	TCP	10246	Any	Any	Any
Allow	No	System	Any	Local subnet	TCP	10246	Any	Any	Any
Allow	No	System	Any	Any	TCP	10246	Any	Any	Any
Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any
Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any	Any	Any
Allow	No	%System...	Any	Local subnet	UDP	Any	Any	Any	Any
Allow	No	%System...	Any	PlayTo Renderers	TCP	23554, 235...	Any	Any	Any
Allow	No	%System...	Any	Local subnet	TCP	23554, 235...	Any	Any	Any
Allow	No	%System...	Any	Any	TCP	23554, 235...	Any	Any	Any
Allow	No	System	Any	PlayTo Renderers	TCP	2869	Any	Any	Any
Allow	No	%system...	Any	Any	TCP	135	Any	Any	Any
Allow	No	%system...	Any	Any	TCP	RPC Dyna...	Any	Any	Any
Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Allow	No	System	Any	Any	ICMPv4	Any	Any	Any	Any
Allow	No	%System...	Any	Any	UDP	68	67	Any	Any
Allow	No	%System...	Any	Any	UDP	546	547	Any	Any
Allow	No	System	Any	Any	IGMP	Any	Any	Any	Any

Check for DNS poisoning, what site was targeted?

hosts文件中,google.com被替换了

参考文章

https://blog.csdn.net/CSNDRYL/article/details/77194060

https://shamsher-khan-404.medium.com/investigating-windows-tryhackme-writeup-65d0ceeaca90