Investigating Windows [TryHackMe]

m4rk0ns3cur1ty · Follow
5 min read · Feb 17, 2021

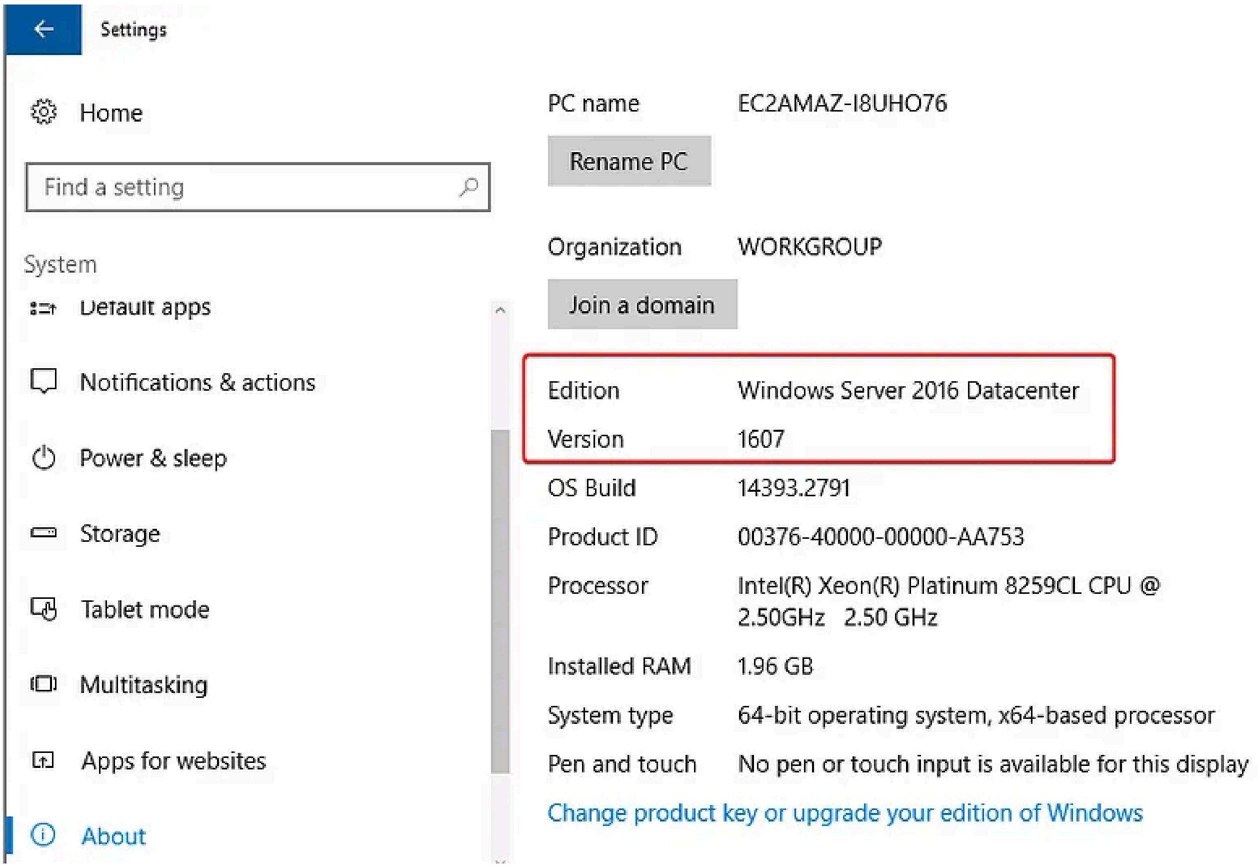
Listen Share More

Lab Link: https://tryhackme.com/room/investigatingwindows
Answer Cheatsheet:
https://github.com/m4rk0ns3cur1ty/Walkthrough/blob/main/TryHackMe/investigating_windows.md

80
Investigating Windows
A windows machine has been hacked, its your job to go investigate this windows machine

Task: Investigating a windows machine that has been previously compromised.

At Windows system, Basic information like **Windows Version, OS Build,** Installed Hardware Information etc. can be found from the **Windows Settings > System > About** or Type “**systeminfo**” on Command Prompt.



PC name EC2AMAZ-I8UHO76

Organization WORKGROUP

Edition Windows Server 2016 Datacenter
Version 1607
OS Build 14393.2791
Product ID 00376-40000-00000-AA753
Processor Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2.50 GHz
Installed RAM 1.96 GB
System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display

Basic Information of Windows OS

Challenge Question: Whats the version and year of the windows machine?
Answer: Windows Server 2016

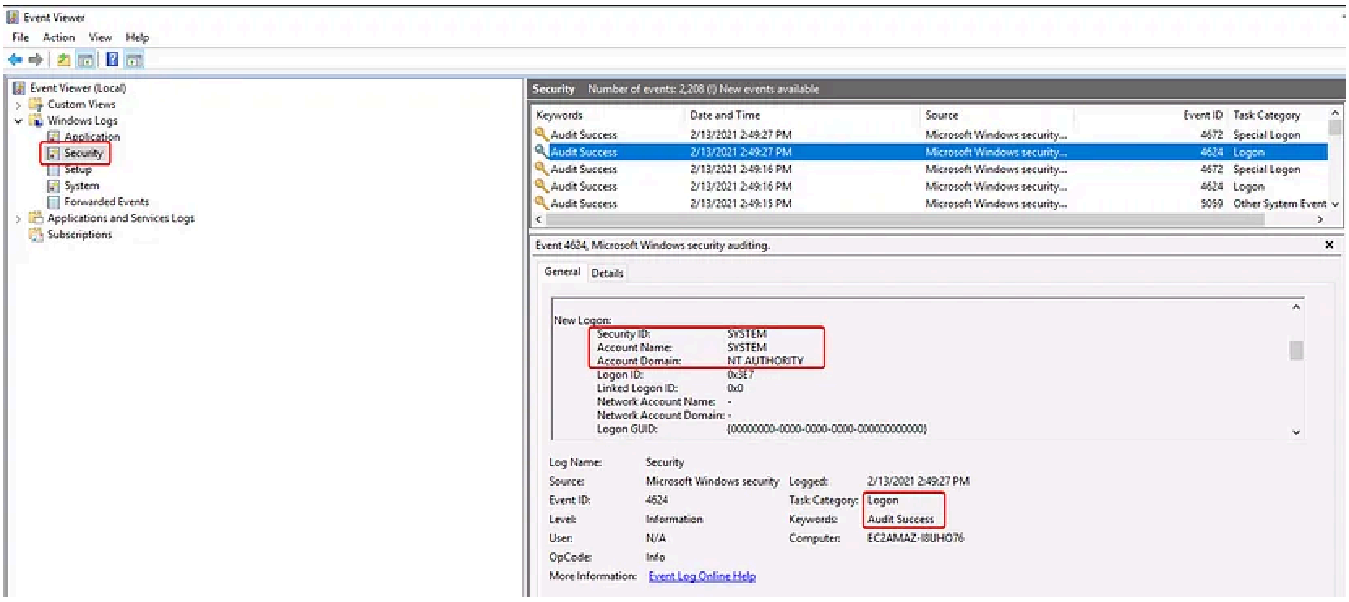
Windows Event Logs is a comprehensive record of the windows system and it's applications. A windows log contains the **source** of the log, **date and time**, **user details**, **Event ID** etc.

Event logs can be viewed by "**Event Viewer**" comes preinstalled with Windows OS.

Event logs are mainly three types -
Application: Contains the logs occurs by an application.
Security: Contains the logs regarding any security events like Login, Logoff etc.
System: Contains the logs generated by Operating system itself. Example: Failure of a driver.

Last logged in user details & timestamp related logged in can be found under the **Event Viewer > Security** section. Then use Event ID:**4624** as a filter to sort the logged in related logs. And use Event ID:**4672** for timestamp related information about Special privileged assigned to a new logon.

> *Event ID 4624: An account was successfully logged in*
>
> *Event ID 4672: Special privileges assigned to new logon*



Security Number of events: 2,208 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/13/2021 2:49:27 PM	Microsoft Windows security...	4672	Special Logon
Audit Success	2/13/2021 2:49:27 PM	Microsoft Windows security...	4624	Logon
Audit Success	2/13/2021 2:49:16 PM	Microsoft Windows security...	4672	Special Logon
Audit Success	2/13/2021 2:49:16 PM	Microsoft Windows security...	4624	Logon
Audit Success	2/13/2021 2:49:15 PM	Microsoft Windows security...	5059	Other System Event

Event 4624, Microsoft Windows security auditing.

```
New Logon:
        Security ID:              SYSTEM
        Account Name:             SYSTEM
        Account Domain:           NT AUTHORITY
        Logon ID:                 0x3E7
        Linked Logon ID:          0x0
        Network Account Name:     -
        Network Account Domain:   -
        Logon GUID:               {00000000-0000-0000-0000-000000000000}
```

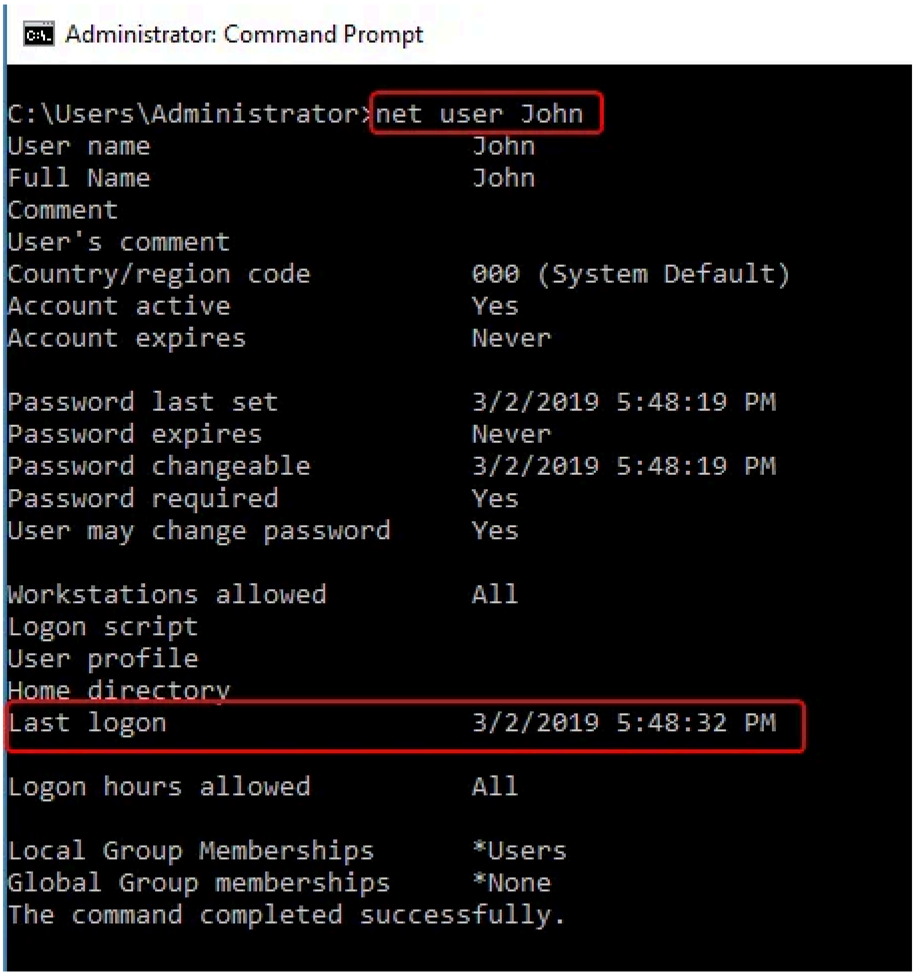
```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          2/13/2021 2:49:27 PM
Event ID:          4624                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        EC2AMAZ-I8UHO76
OpCode:            Info
More Information:  Event Log Online Help
```

Event Logs regarding Successful Logged In.

Challenge Question: Which user logged in last?
Answer: Administrator
Challenge Question: At what time did Windows first assign special privileges to a new logon?
Answer: 03/02/2019 4:04:49 PM

To know about a user information like **Last logged on**, **Local or Global group**, **password related information** etc., we can use "**net user**" command with the username from the command prompt. Only "**net user**" command helps us to know about the available users of the system.

> *net user John*



Administrator: Command Prompt

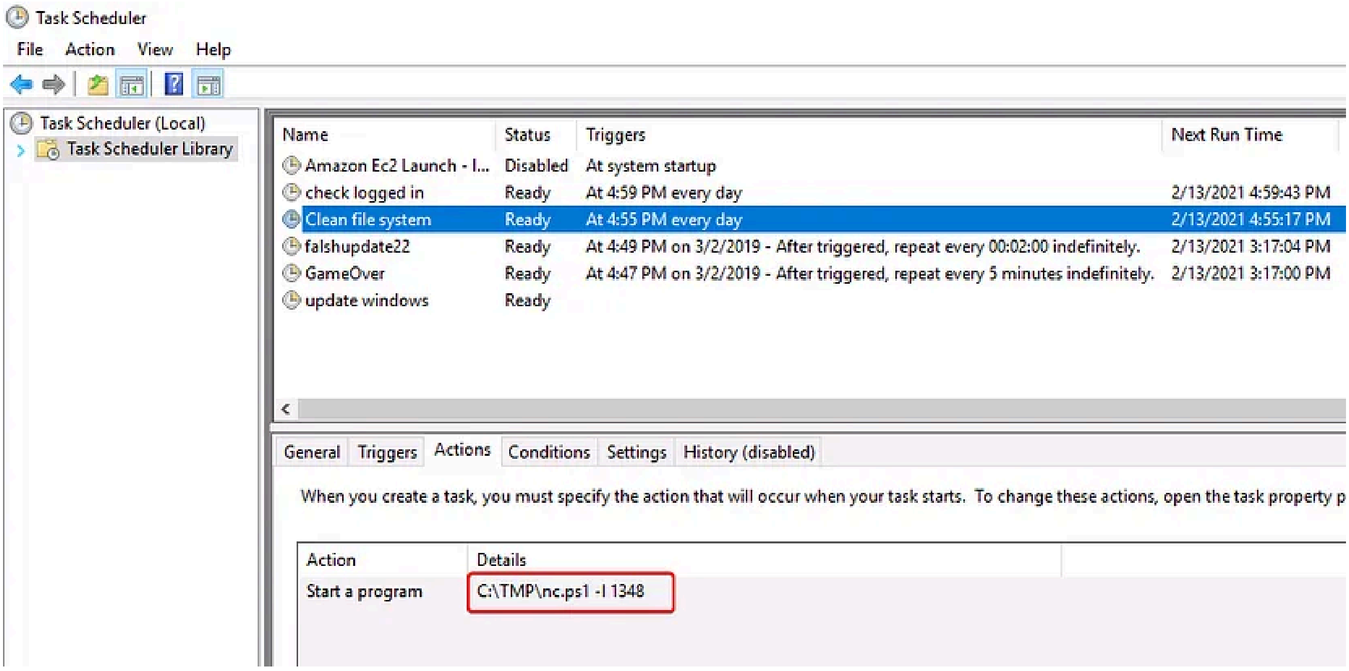
```
C:\Users\Administrator>net user John
User name                    John
Full Name                    John
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

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.
```

Last Logon information of user John

Challenge Question: When did John log onto the system last?
Answer: 03/02/2019 5:48:32 PM
Challenge Question: What two accounts had administrative privileges (other than the Administrator user)?
Answer: Jenny, Guest
Challenge Question: When did Jenny last logon?
Answer: Never

Windows Task Scheduler is a inbuilt tool that enables you to create and execute a automatically schedule any task on your system. Most of the time malware use this features to do it’s bad things on your system.

To know about the active scheduled task on system. Launch **Task Scheduler > Task Scheduler Library**. By clicking on a scheduled task from the list you will able to see more details about the scheduled task like created **timestamp** of the task, **action** or related commands of the task etc.



Name	Status	Triggers	Next Run Time
Amazon Ec2 Launch - I...	Disabled	At system startup	
check logged in	Ready	At 4:59 PM every day	2/13/2021 4:59:43 PM
Clean file system	Ready	At 4:55 PM every day	2/13/2021 4:55:17 PM
falshupdate22	Ready	At 4:49 PM on 3/2/2019 - After triggered, repeat every 00:02:00 indefinitely.	2/13/2021 3:17:04 PM
GameOver	Ready	At 4:47 PM on 3/2/2019 - After triggered, repeat every 5 minutes indefinitely.	2/13/2021 3:17:00 PM
update windows	Ready		

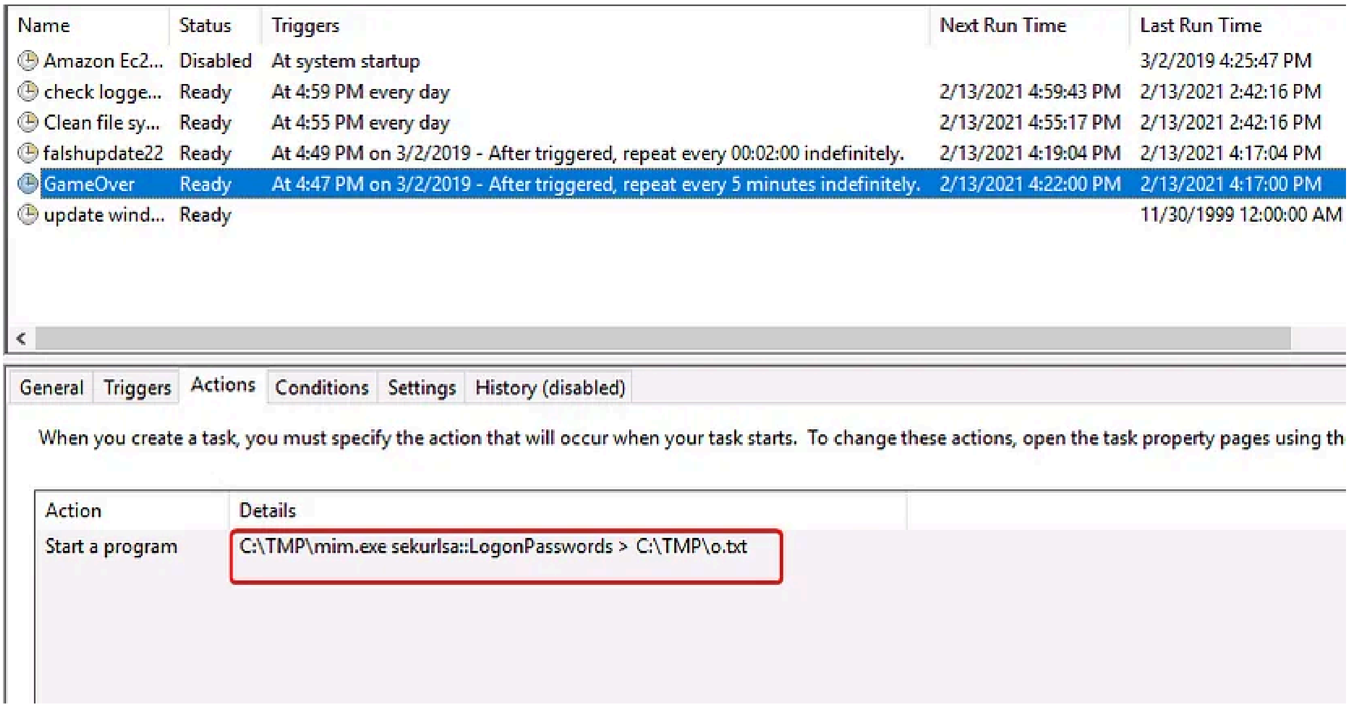
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property p

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

Windows Task Scheduler

Challenge Question: Whats the name of the scheduled task that is malicious.
Answer: Clean file system
Challenge Question: What file was the task trying to run daily?
Answer: nc.ps1
Challenge Question: What port did this file listen locally for?
Answer: 1348
Challenge Question: At what date did the compromise take place?
Answer: 03/02/2019

There is a question on lab i.e. ***What tool was used to get Windows passwords?***. To answer this question, I investigate the automated task from **Task Scheduler**. I noticed there is a task called “**GameOver**” under the action tab I saw there is a executable called “**mim.exe**” located at TMP directory of the system it triggered every **5 min** and save the output at **o.txt** file located at same directory. When I investigate that text file (**o.txt**) I saw “**mimikatz**” tool is used for capturing windows password.



Name	Status	Triggers	Next Run Time	Last Run Time
Amazon Ec2...	Disabled	At system startup		3/2/2019 4:25:47 PM
check logge...	Ready	At 4:59 PM every day	2/13/2021 4:59:43 PM	2/13/2021 2:42:16 PM
Clean file sy...	Ready	At 4:55 PM every day	2/13/2021 4:55:17 PM	2/13/2021 2:42:16 PM
falshupdate22	Ready	At 4:49 PM on 3/2/2019 - After triggered, repeat every 00:02:00 indefinitely.	2/13/2021 4:19:04 PM	2/13/2021 4:17:04 PM
GameOver	Ready	At 4:47 PM on 3/2/2019 - After triggered, repeat every 5 minutes indefinitely.	2/13/2021 4:22:00 PM	2/13/2021 4:17:00 PM
update wind...	Ready			11/30/1999 12:00:00 AM

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 th

Action	Details
Start a program	C:\TMP\mim.exe sekurlsa::LogonPasswords > C:\TMP\o.txt

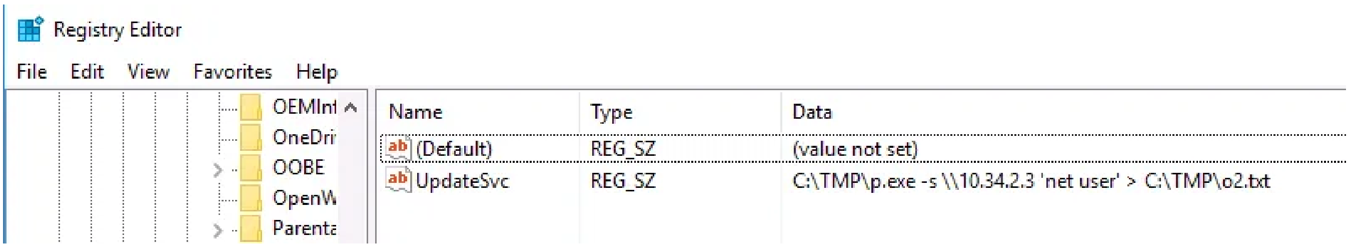
Evidence related to Mimikatz

Challenge Question: What tool was used to get Windows passwords?
Answer: Mimikatz

Windows registry is a type of database that contains information & settings regarding installed software and hardware of a system. “**Registry Editor**” is used to view this registry information from your system.

HKEY_CLASSES_ROOT: Contain the file type, extension etc. related information.
HKEY_CURRENT_USER: Contain settings of a logged in users.
HKEY_LOCAL_MACHINE: Contain information about installed hardware, software and their related settings.
HKEY_USERS: Contain information about the all users present on the system.
HKEY_CURRENT_CONFIG: Contains the Hardware profile

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
This registry key can control the programs to run each time that a user logged on. This key is also used by malware to become persistence on the system.

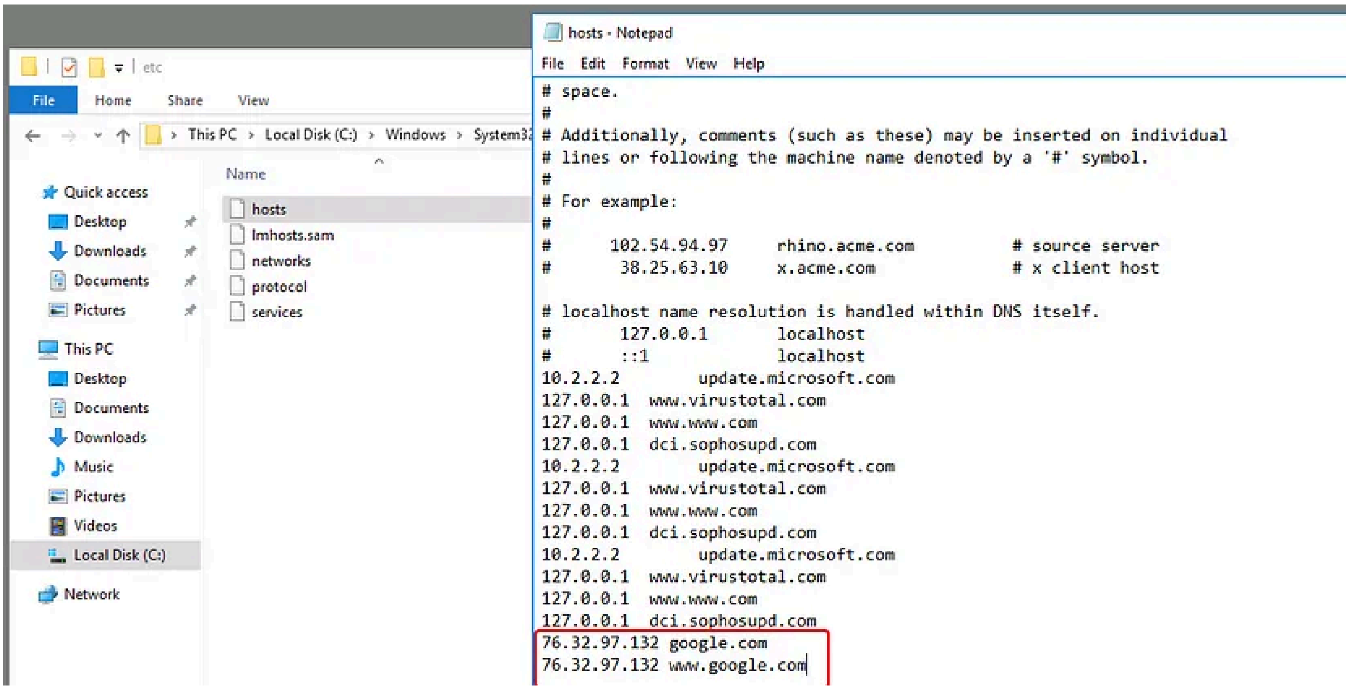


Name	Type	Data
(Default)	REG_SZ	(value not set)
UpdateSvc	REG_SZ	C:\TMP\p.exe -s \\10.34.2.3 'net user' > C:\TMP\o2.txt

Startup Command in Registry Key

Challenge Question: What IP does the system connect to when it first starts?
Answer: 10.34.2.3

Windows **hosts** file is used for maps the server or hostname to IP addresses.
In windows the location of the hosts file is **C:\Windows\System32\drivers\etc\hosts**

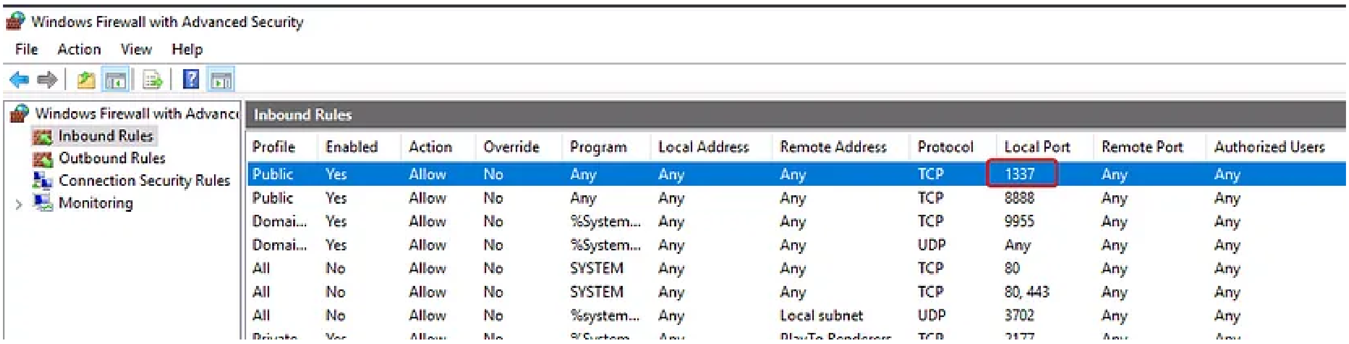


```
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# 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
```

Windows Hosts file

Challenge Question: What was the attackers external control and command servers IP?
Answer: 76.32.97.132
Challenge Question: Check for DNS poisoning, what site was targeted?
Answer: google.com

Windows firewall's **Inbound Rules** defend the network against the incoming traffic. It is always helpful to save your system from malware or DDOS related attacks. It also contains the details of the **port** and **address** of the local and remote server.

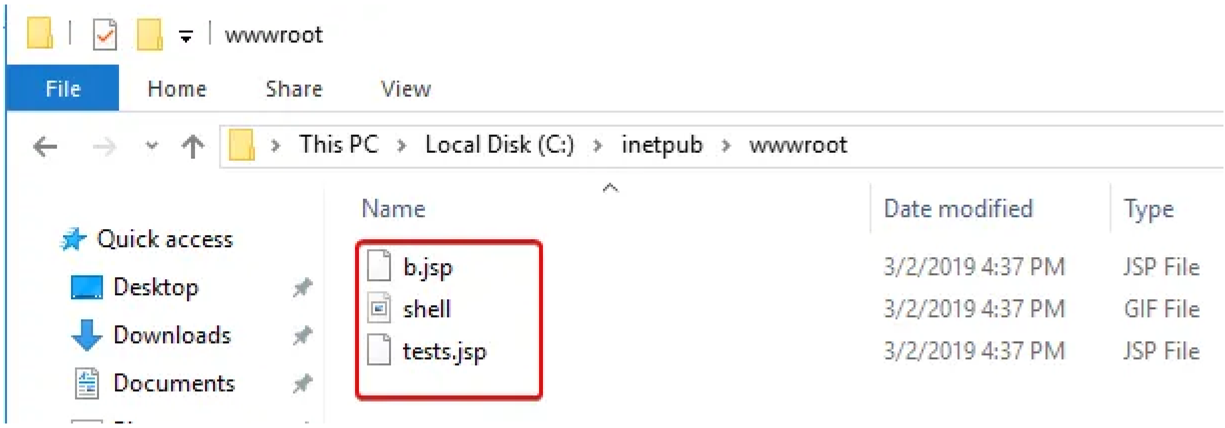


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users
Public	Yes	Allow	No	Any	Any	Any	TCP	1337	Any	Any
Public	Yes	Allow	No	Any	Any	Any	TCP	8888	Any	Any
Domai...	Yes	Allow	No	%System...	Any	Any	TCP	9955	Any	Any
Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any
All	No	Allow	No	SYSTEM	Any	Any	TCP	80	Any	Any
All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any	Any
All	No	Allow	No	%system...	Any	Local subnet	UDP	3702	Any	Any
Private	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any

Windows Firewall Inbound Traffic Rules

Microsoft uses IIS (Internet Informaion Services) as a default web server on the Windows. **inetpub** is the default folder situated under C:\inetpub. It contains the webserver's content. **wwwroot** is a subfolder placed under the inetpub (**C:\inetpub\wwwroot**) holds all the content like of a webpages.



Name	Date modified	Type
b.jsp	3/2/2019 4:37 PM	JSP File
shell	3/2/2019 4:37 PM	GIF File
tests.jsp	3/2/2019 4:37 PM	JSP File

Challenge Question: What was the extension name of the shell uploaded via the servers website?
Answer: .jsp

That's all!!

Forensics Cybersecurity Windows Tryhackme Hacking

Follow

Written by m4rk0ns3cur1ty

60 Followers · 4 Following

Digital Forensics | Malware Researcher

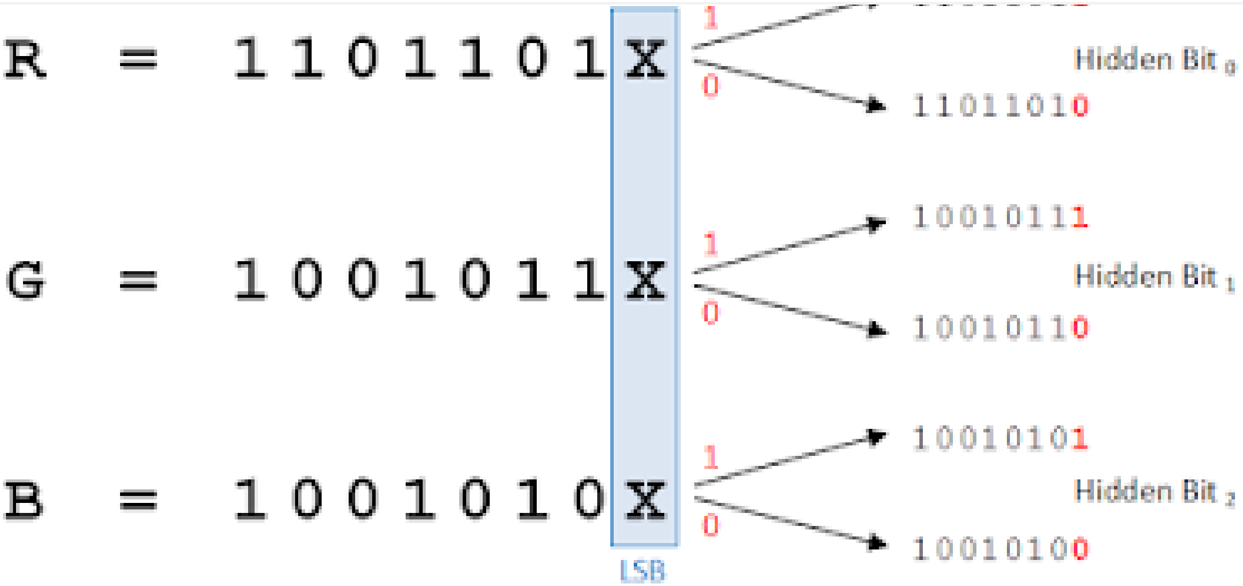
No responses yet

What are your thoughts?

Respond

Open in app ↗

Medium Search



m4rk0ns3cur1ty

Image Challenges -1 [Cats are innocent, right?]

This challenge is taken from Codefest'19 CTF. It is a steganography challenge based on LSB (Least Significant Bit) Steganography.

Aug 29, 2019 8

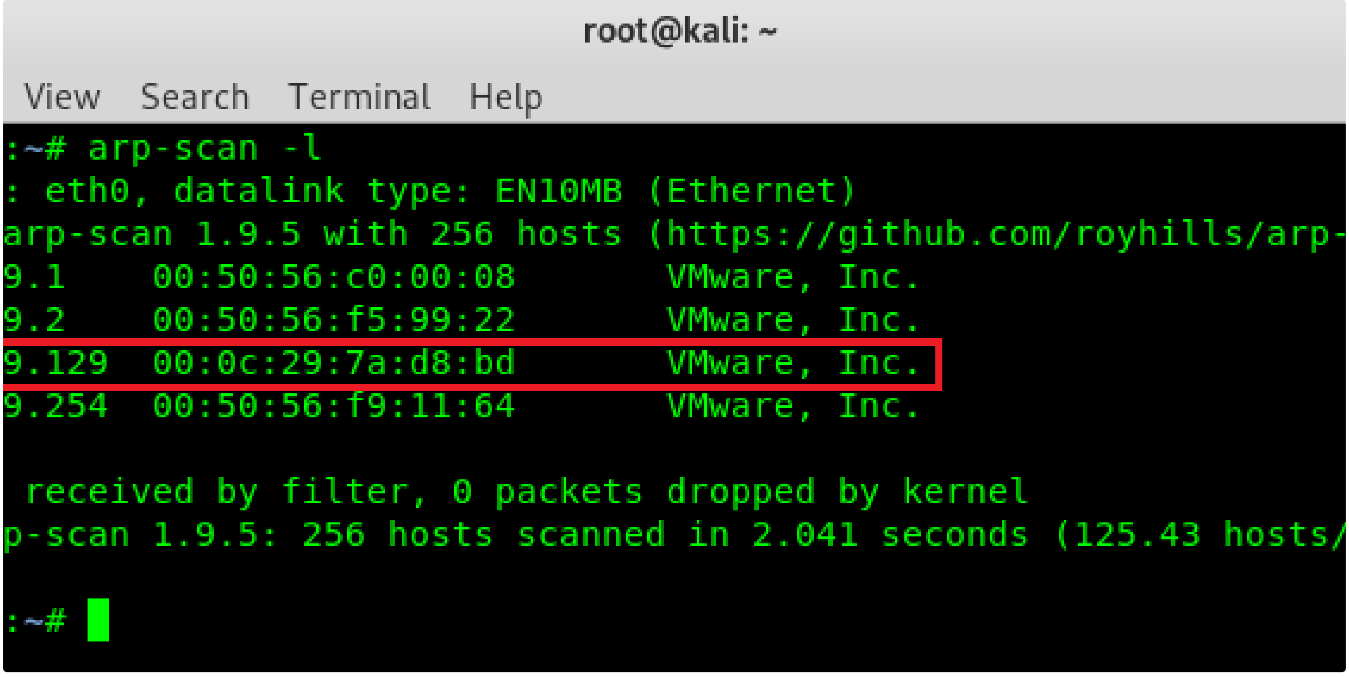
“TSURUGI Linux - the sharpest weapon in your DFIR arsenal...”
TSURUGI
LINUX

m4rk0ns3cur1ty

Tsurugi Linux- A Short Review

Tsurugi Linux- A Open Source Project for Digital Forensics and Incident Response purposes.

Nov 27, 2018 115 1



```
:~# arp-scan -l
: eth0, datalink type: EN10MB (Ethernet)
arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-
9.1    00:50:56:c0:00:08       VMware, Inc.
9.2    00:50:56:f5:99:22       VMware, Inc.
9.129  00:0c:29:7a:d8:bd       VMware, Inc.
9.254  00:50:56:f9:11:64       VMware, Inc.

 received by filter, 0 packets dropped by kernel
p-scan 1.9.5: 256 hosts scanned in 2.041 seconds (125.43 hosts/

:~#
```

m4rk0ns3cur1ty

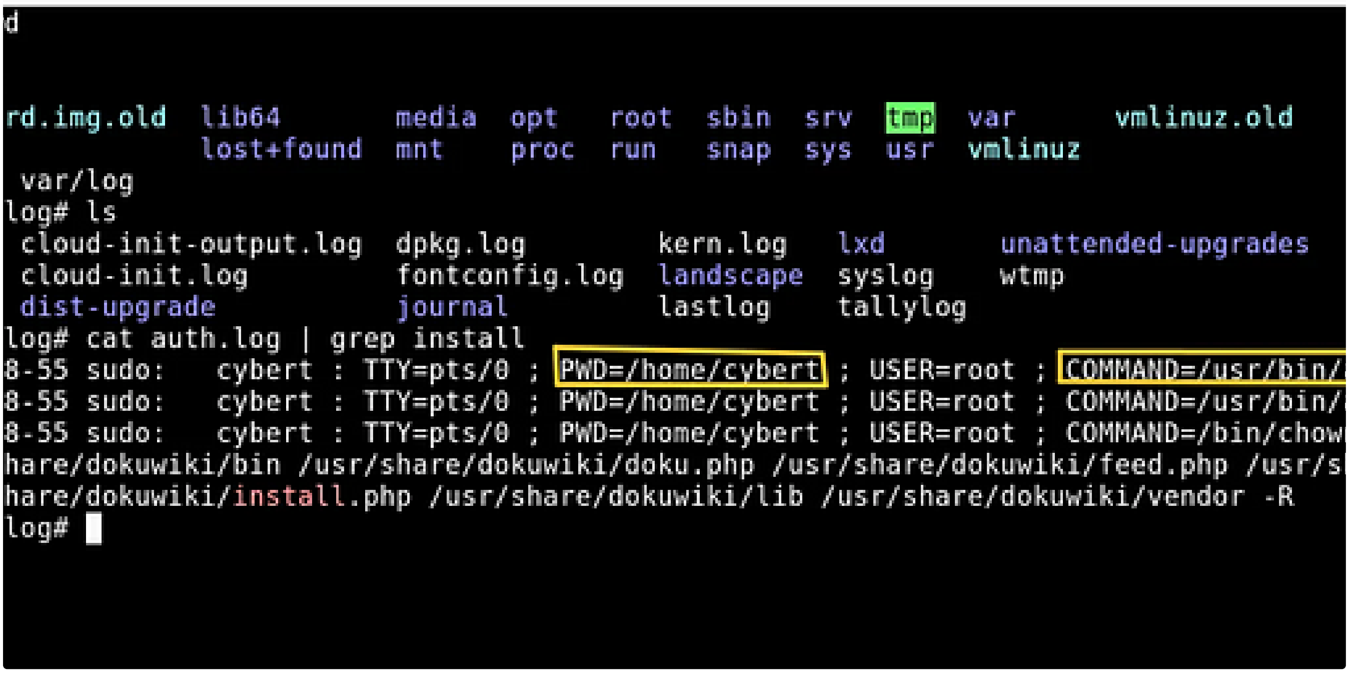
Symfonos: 1 Walkthrough [VulnHub]

Download Link- https://www.vulnhub.com/entry/symfonos-1,322/ Difficulty: Beginner

Jul 25, 2019 26

See all from m4rk0ns3cur1ty

Recommended from Medium



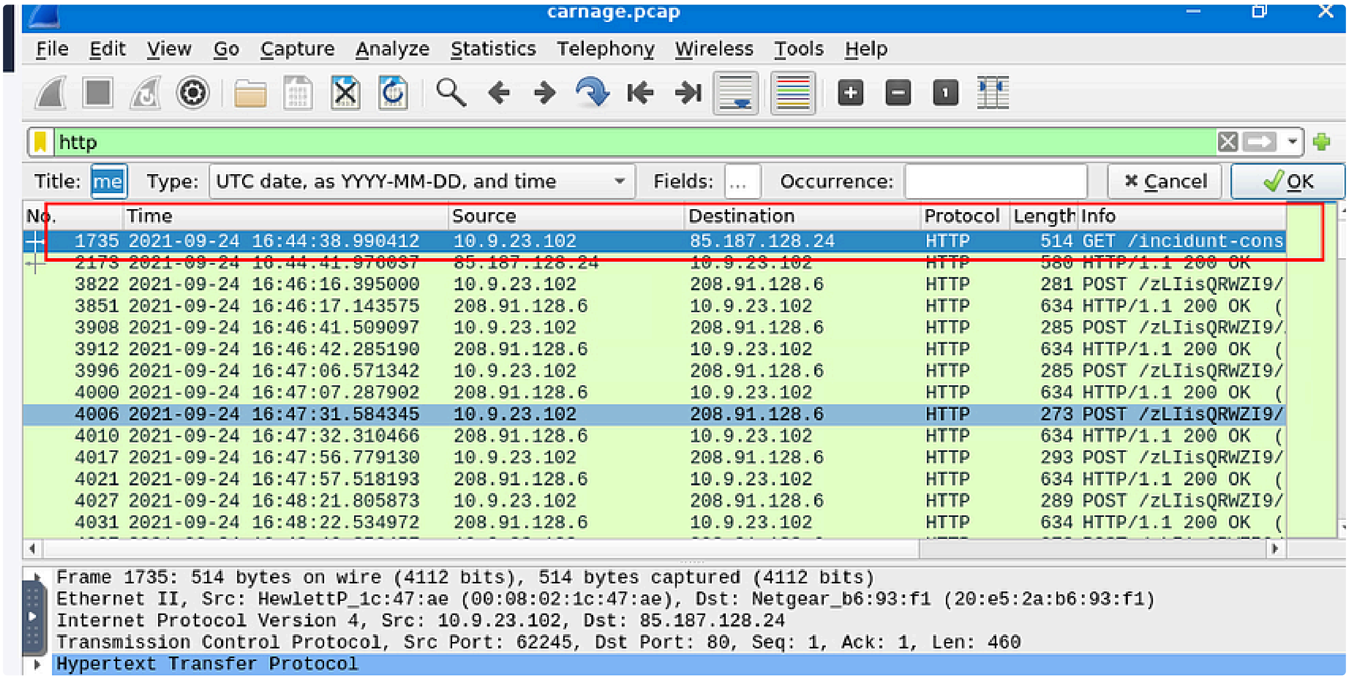
```
d

rd.img.old  lib64       media  opt   root  sbin  srv  tmp  var      vmlinuz.old
            lost+found  mnt    proc  run   snap  sys  usr  vmlinuz
 var/log
log# ls
 cloud-init-output.log  dpkg.log        kern.log   lxd       unattended-upgrades
 cloud-init.log         fontconfig.log  landscape  syslog    wtmp
 dist-upgrade           journal         lastlog    tallylog
log# cat auth.log | grep install
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log# 
```

Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here: https://tryhackme.com/room/disgruntled

Oct 22, 2024



carnage.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
Title: me   Type: UTC date, as YYYY-MM-DD, and time   Fields: ...   Occurrence:        × Cancel   ✓ OK

No.  Time                        Source          Destination     Protocol  Length Info
1735 2021-09-24 16:44:38.990412  10.9.23.102     85.187.128.24   HTTP      514 GET /incidunt-cons
2173 2021-09-24 16:44:41.970037  85.187.128.24   10.9.23.102     HTTP      580 HTTP/1.1 200 OK
3822 2021-09-24 16:46:16.395000  10.9.23.102     208.91.128.6    HTTP      281 POST /zLIisQRWZI9/
3851 2021-09-24 16:46:17.143575  208.91.128.6    10.9.23.102     HTTP      634 HTTP/1.1 200 OK  (
3908 2021-09-24 16:46:41.509097  10.9.23.102     208.91.128.6    HTTP      285 POST /zLIisQRWZI9/
3912 2021-09-24 16:46:42.285190  208.91.128.6    10.9.23.102     HTTP      634 HTTP/1.1 200 OK  (
3996 2021-09-24 16:47:06.571342  10.9.23.102     208.91.128.6    HTTP      285 POST /zLIisQRWZI9/
4000 2021-09-24 16:47:07.287902  208.91.128.6    10.9.23.102     HTTP      634 HTTP/1.1 200 OK  (
4006 2021-09-24 16:47:31.584345  10.9.23.102     208.91.128.6    HTTP      273 POST /zLIisQRWZI9/
4010 2021-09-24 16:47:32.310466  208.91.128.6    10.9.23.102     HTTP      634 HTTP/1.1 200 OK  (
4017 2021-09-24 16:47:56.779130  10.9.23.102     208.91.128.6    HTTP      293 POST /zLIisQRWZI9/
4021 2021-09-24 16:47:57.518193  208.91.128.6    10.9.23.102     HTTP      634 HTTP/1.1 200 OK  (
4027 2021-09-24 16:48:21.805873  10.9.23.102     208.91.128.6    HTTP      289 POST /zLIisQRWZI9/
4031 2021-09-24 16:48:22.534972  208.91.128.6    10.9.23.102     HTTP      634 HTTP/1.1 200 OK  (

Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24
Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
Hypertext Transfer Protocol
```

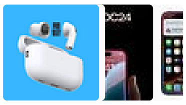
Chicken0248

[TryHackMe Write-up] Carnage

Apply your analytical skills to analyze the malicious network traffic using Wireshark.

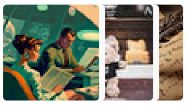
Aug 17, 2024 👏 50

Lists



Tech & Tools

22 stories · 380 saves

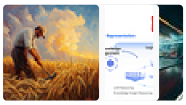


Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves

Staff picks

796 stories · 1561 saves



Natural Language Processing

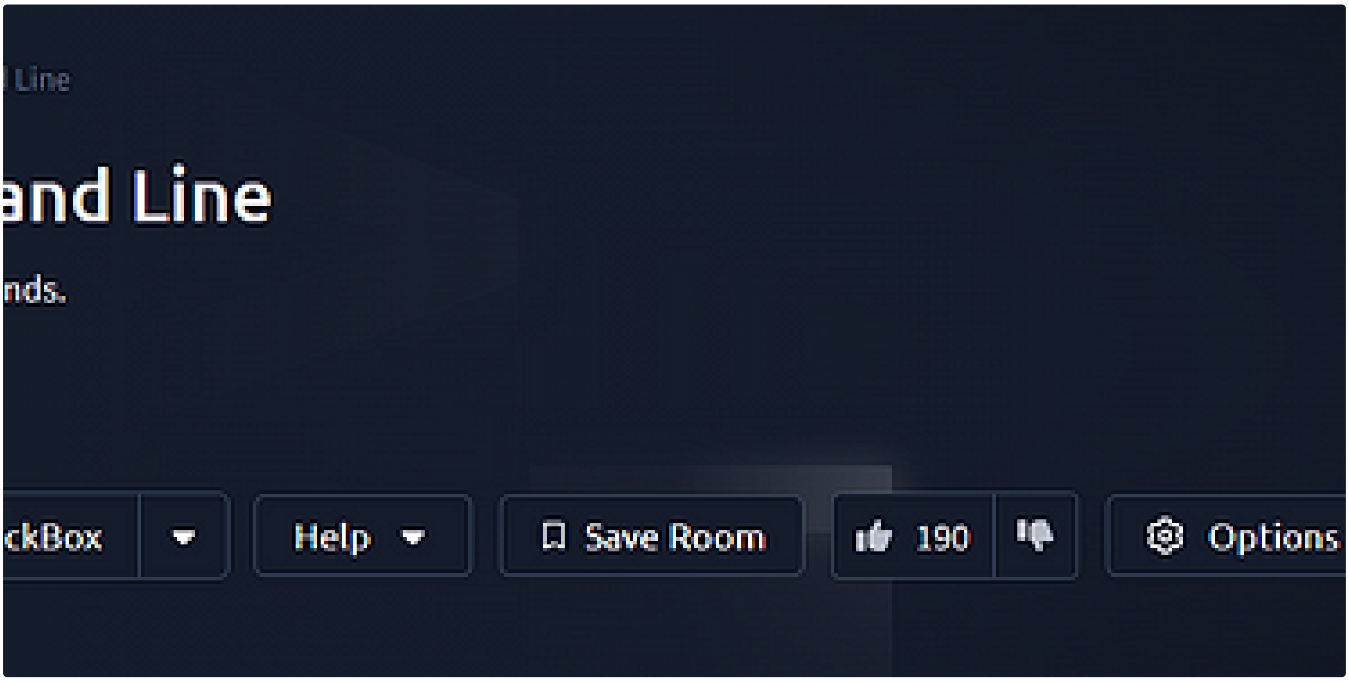
1884 stories · 1529 saves

IritT

Windows Fundamentals 1—Complete Beginner—Windows Exploitation Basics—TryHackMe Walkthrough

In part 1 of the Windows Fundamentals module, we'll start our journey learning about the Windows desktop, the NTFS file system, UAC, the...

Oct 23, 2024

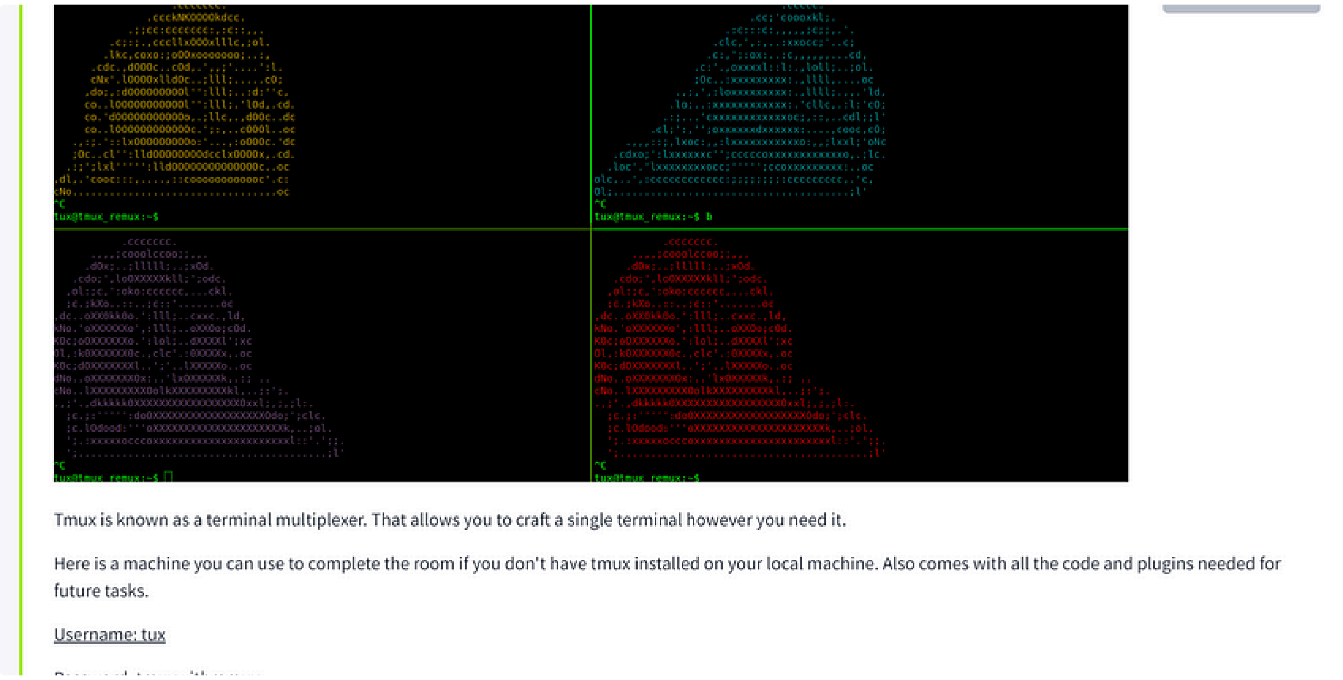


TRedEye

Windows Command Line

Windows Command Line

Oct 27, 2024 30



```
tux@tmux_remux:~$
tux@tmux_remux:~$ b
tux@tmux_remux:~$
tux@tmux_remux:~$
```

Tmux is known as a terminal multiplexer. That allows you to craft a single terminal however you need it.

Here is a machine you can use to complete the room if you don't have tmux installed on your local machine. Also comes with all the code and plugins needed for future tasks.

Username: tux

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: REmux The Tmux

Tryhackme Free Walk-through Room: REmux The Tmux

Nov 10, 2024 1

Praj Shete

Writeup > LetsDefend: Adobe ColdFusion RCE

Scenario: Our ERD software was triggered, alerted, and isolated a web server for suspicious use of the “nltest.exe” command. Investigate...

Nov 14, 2024

See more recommendations