

System Hacking

Module 6 (Lab Assignment)

Name: Sachin Saj T K

Roll No: CB.EN.P2CEN18012

Date of Submission: 5/06/2019

Hiding Files Using NTFS Streams

1. Creating readme.txt, and hiding the file in calc.exe

```
C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is BAE7-1A72

Directory of C:\magic

05-06-2019  13:15    <DIR>          .
05-06-2019  13:15    <DIR>          ..
10-07-2015  16:31             26,112 calc.exe
05-06-2019  13:16             11 readme.txt
               2 File(s)                26,123 bytes
               2 Dir(s)  96,174,612,480 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is BAE7-1A72

Directory of C:\magic

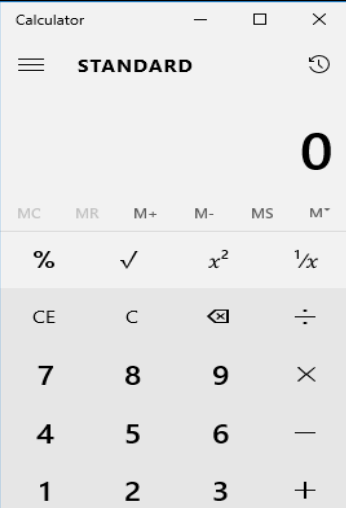
05-06-2019  13:15    <DIR>          .
05-06-2019  13:15    <DIR>          ..
10-07-2015  16:31             26,112 calc.exe
05-06-2019  13:17             11 readme.txt
               2 File(s)                26,123 bytes
               2 Dir(s)  96,174,329,856 bytes free
```

2. Creating backdoor

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ...
C:\Windows\system32>cd ..
C:\Windows>cd..
C:\>cd magic
C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<<

C:\magic>backdoor
C:\magic>
```



Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
NTFS Streams	Output: Calculator (Calc.exe) file executed

Extracting SAM Hashes Using PWdump7 Tool

1. Finding the hashes for the passwords in the local system.

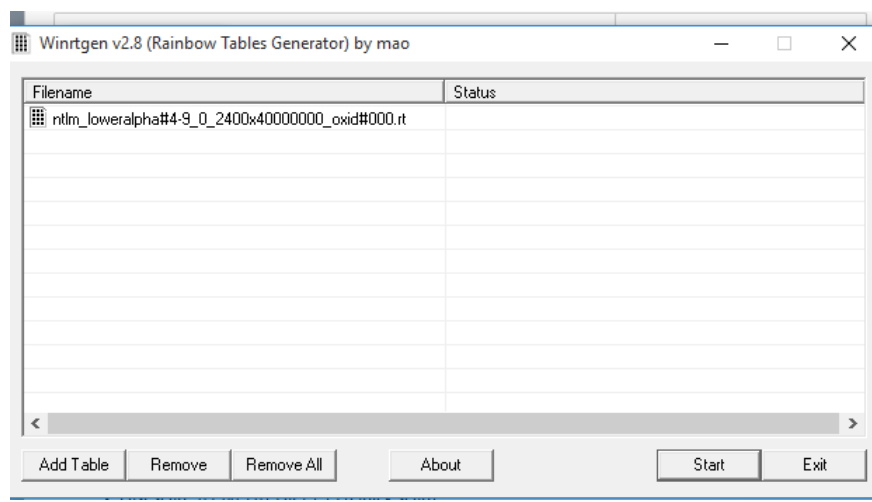
```
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::  
[]:503:NO PASSWORD*****:NO PASSWORD*****:::  
Sachin:1001:NO PASSWORD*****:988DD8F9B4A2E2676CAA683606862990:::
```

Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
PWdump7	Output: List of User and Password Hashes Administrator: 31D6CFE0D16AE931B73C59D7E0C089C0:: Sachin: 988DD8F9B4A2E2676CAA683606862990:::

Creating the Rainbow Tables Using Winrtgen

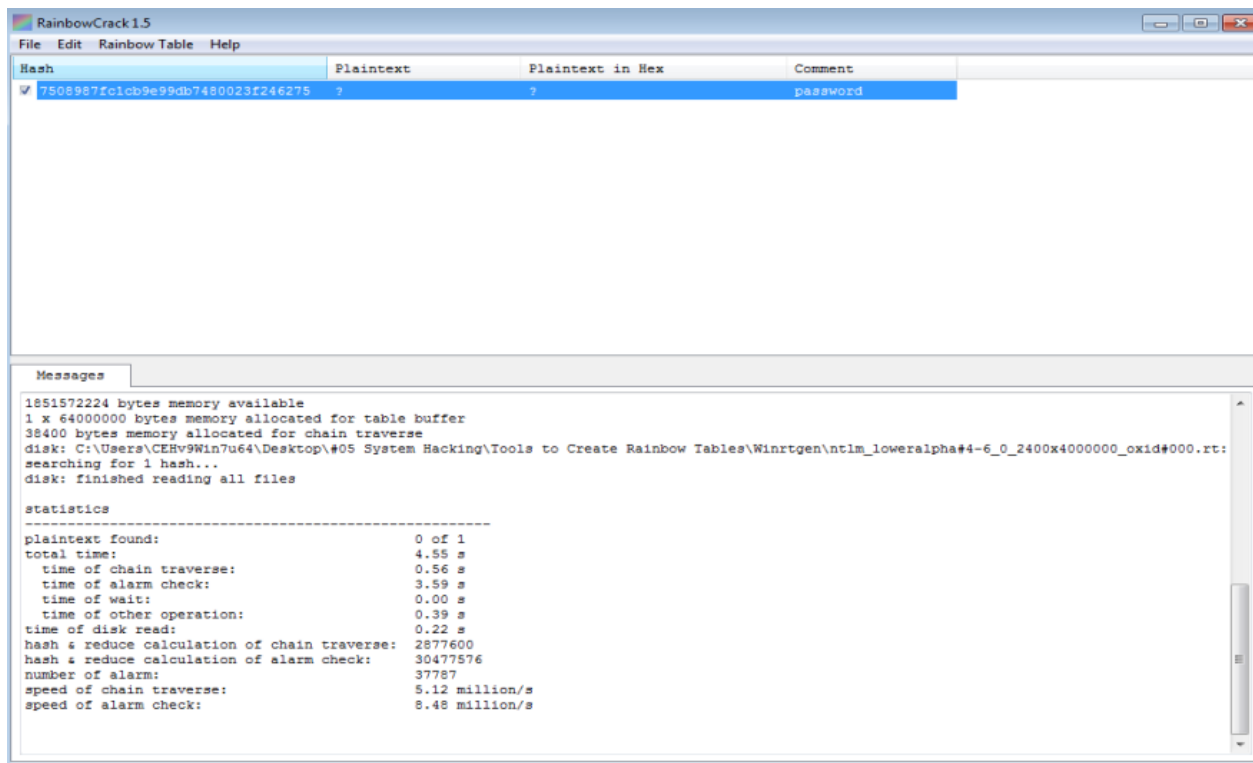
1. Creating lower alpha RainbowCrack table



Lab Analysis

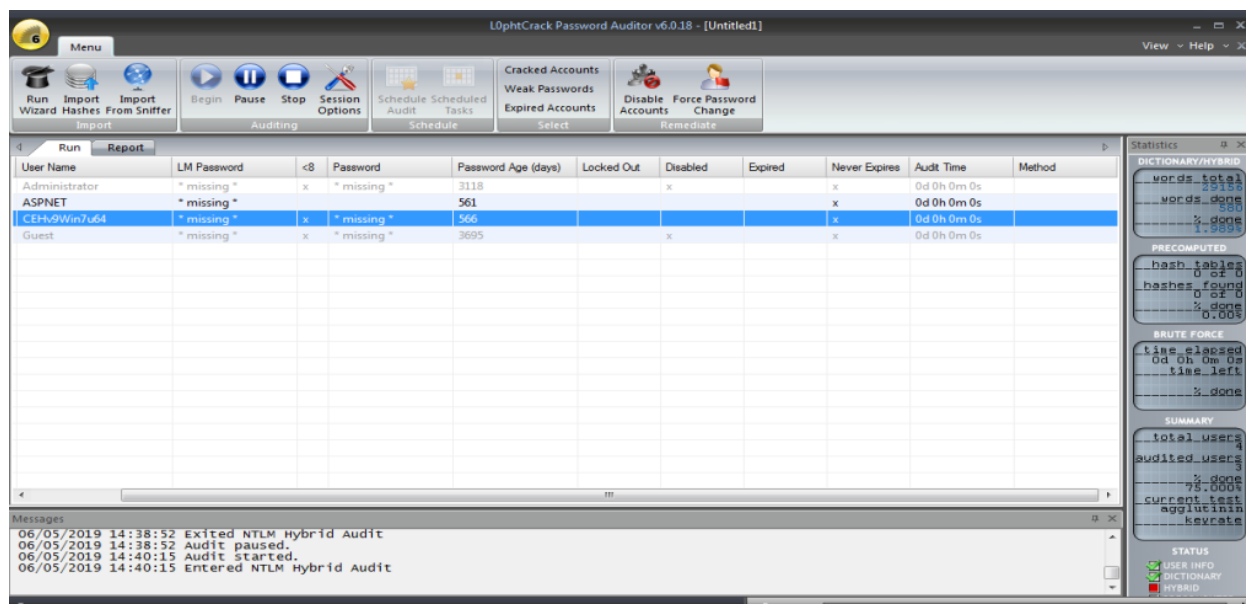
Tool/Utility	Information Collected/Objective Achieved
Winrtge	Purpose: Creating Rainbow table with lower alpha
	Output: Created Rainbow table: ntlm_loweralpha#4.6_0_02400X400000_ox..

Password Cracking Using RainbowCrack



Tool/Utility	Information Collected/Objective Achieved
RainbowCrack	Hashes: 7508987FC1CB9E99DB8580023F246275
	Password Cracked: Could not be cracked

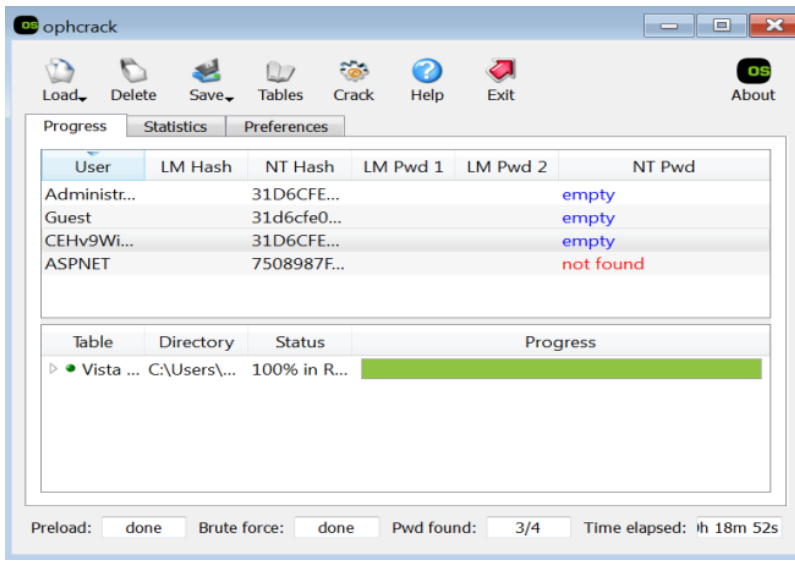
Extracting Administrator passwords Using L0phtCrack



Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
L0phtCrack	User Names:CEHv9Win7u64
	Password Found: asuna

Password Cracking Using Ophcrack



Tool/Utility	Information Collected/Objective Achieved
OphCrack	User Names: CEHv9Win
	Rainbow Table Used : Vista free
	Password Found: Not Found

Hiding Data Using Snow Steganography

1. Using snow steganography, hiding important content inside the text file. Which is can't be seen by third person.

```
C:\Users\CEHv9Win7u64\Desktop\#05 System Hacking\Steganography Tools\Whitespace
Steganography Tools\Snow>snw -C -m "my swiss bank account number is 45656684542
256" -p "magic" readme.txt readme2.txt
Compressed by 23.64%
Message exceeded available space by approximately 524.44%.
An extra 9 lines were added.

C:\Users\CEHv9Win7u64\Desktop\#05 System Hacking\Steganography Tools\Whitespace
Steganography Tools\Snow>snw -C -p "magic" readme2.txt
my swiss bank account number is 45656684542256
C:\Users\CEHv9Win7u64\Desktop\#05 System Hacking\Steganography Tools\Whitespace
Steganography Tools\Snow>
```

Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
Snow Steganography	Output : You will see the hidden data inside Notepad

Viewing, Enabling, and Clearing the Audit Policies Using Auditpol

1. To view Auditpol

```
Security Group Management          Success
Distribution Group Management      No Auditing
Application Group Management        No Auditing
Other Account Management Events     No Auditing
DS Access
Directory Service Changes          No Auditing
Directory Service Replication       No Auditing
Detailed Directory Service Replication No Auditing
Directory Service Access            No Auditing
Account Logon
Kerberos Service Ticket Operations  No Auditing
Other Account Logon Events          No Auditing
Kerberos Authentication Service     No Auditing
Credential Validation                No Auditing

C:\Windows\system32>auditpol /set /category:"system","account logon" /success:en
able /failure:enable
The command was successfully executed.
```

2. Enabling the Auditpol

```
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System Events          Success and Failure
  Security State Change        Success and Failure
Logon/Logoff
```

3. Clearing the Audit policy

```
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    No Auditing
  System Integrity             No Auditing
  IPsec Driver                 No Auditing
  Other System Events          No Auditing
  Security State Change        No Auditing
Logon/Logoff
```

Tool/Utility	Information Collected/Objective Achieved
AuditPol	Result open Auditpol category: <ul style="list-style-type: none">• System<ul style="list-style-type: none">Security System Extension – No AuditingSystem Integrity -- No AuditingIPsec Driver -- No Auditing• Account Logon<ul style="list-style-type: none">Logon -- No AuditingLogoff -- No AuditingAccount Lockout -- No Auditing

Web Activity Monitoring and Recording Using Power Spy 2013

1. PowerSpy started monitoring the victim



2. Website details, which the victim searched.

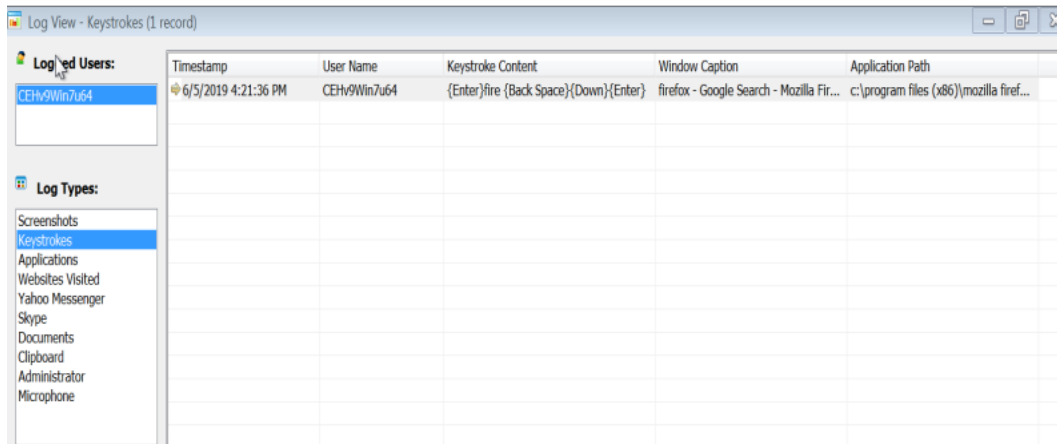
Log View - Websites Visited (2 records)

Logged Users:	Timestamp	User Name	Website URL
CEHV9Win7u64	6/5/2019 4:15:44 PM	CEHV9Win7u64	https://www.google.com/tgws_rd=ssl
	6/5/2019 4:15:31 PM	CEHV9Win7u64	https://www.spytech-web.com/spyagent-buy.shtml

Log Types:

- Screenshots
- Keystrokes
- Applications
- Websites Visited
- Yahoo Messenger
- Skype
- Documents
- Clipboard
- Administrator
- Microphone

3. All the keystrokes that victim did during the monitoring period is noted.



Timestamp	User Name	Keystroke Content	Window Caption	Application Path
6/5/2019 4:21:36 PM	CEHy9Win7u64	{Enter}fire {Back Space}{Down}{Enter}	firefox - Google Search - Mozilla Fir...	c:\program files (x86)\mozilla firef...

Tool/Utility	Information Collected/Objective Achieved
PoweSpy 2013	Output: <ul style="list-style-type: none">Monitoring Keystrokes typed (given above)Website log entries (given above)