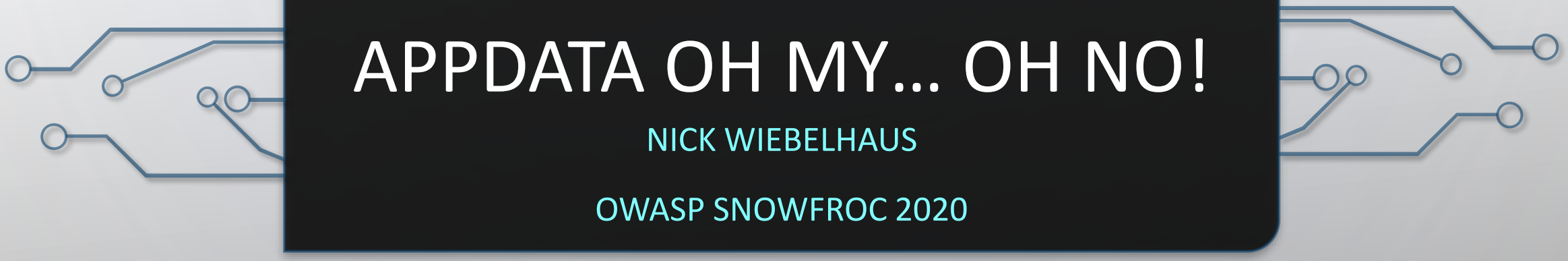


APPDATA OH MY… OH NO!

NICK WIEBELHAUS

OWASP SNOWFROC 2020

ABOUT ME

- Offensive Operations Team Lead – Nelnet
- Offensive Security Consultant
- SANS Community Instructor
  - SEC460 – Enterprise Threat Vulnerability Assessment
  - SEC560 – Network Penetration Testing
- Adjunct Instructor Community College of Aurora
- Certifications: GXPN, GPEN, GWAPT, GCIH, and GEVA

OVERVIEW

- What is AppData
- How to browse AppData
- Where to find sensitive information
  - Browser Application (Web Data)
  - OS Applications
- What we can do about it

WHAT IS THE APPDATA DIRECTORY?

- Contains application settings, files, and data specific to an application on your Windows PC
  - Can include data from Web Applications if cached within the browser
- Hidden folder unique to each user on a system
- Located per users under the users directory
  - C:\Users\<username>\AppData

WINDOWS APPDATA SUBDIRECTORIES

- Local:
  - Specific data to a single computer. Never synced from computer to computer. Data here is generally specific to a computer, or contains files that are too large
- LocalLow:
  - Same as the Local directory but is designed for "low integrity" applications that run with more restricted security settings
- Roaming:
  - Contains data that would "roam" with a user account from computer to computer if your PC was connected to a domain with a roaming profile. Browsers might store user profiles here allowing bookmarks and other browsing data to be access on different PC’s

VIEW AND NAVIGATE APPDATA DIRECTORIES

- Command Line access with PowerShell and cmd.exe
- Windows Explorer (GUI)
  - Local
    - %localappdata%
  - LocalLow
    - %appdata%\..\locallow
  - Roaming
    - %appdata%
  - Manual path navigation
    - Need to enable view Hidden Items in explorer

SENSITIVE DATA IN APPDATA

- Credentials
- Potential PII and PCI
- Documents
- Chat Logs
- API Keys
- Configuration Files
- Internal Network Information

CHROME APPDATA ARTIFACT LOCATIONS

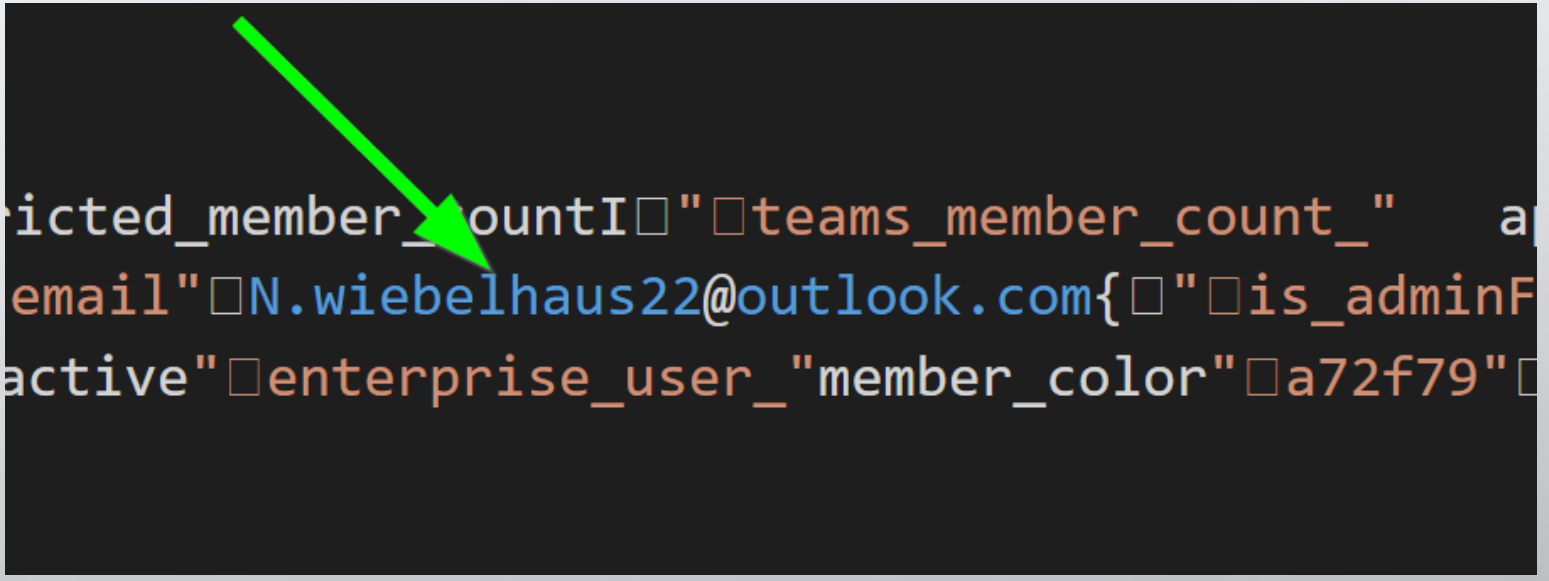
- %localappdata%\Google\Chrome\User Data\Default
  - \Cache\
    - Chromes current cache
  - \IndexedDB\
    - Client-Side storage and site data
  - \Login Data – sqlite file
    - Login info with site, username, and encrypted passwords
  - \Cookies – sqlite file
    - Stored Encrypted Cookies
  - \AutoFillDatabase\
    - Saved AutoFill Data
  - \Web Data – sqlite file
    - Searches, form data, and autofill data

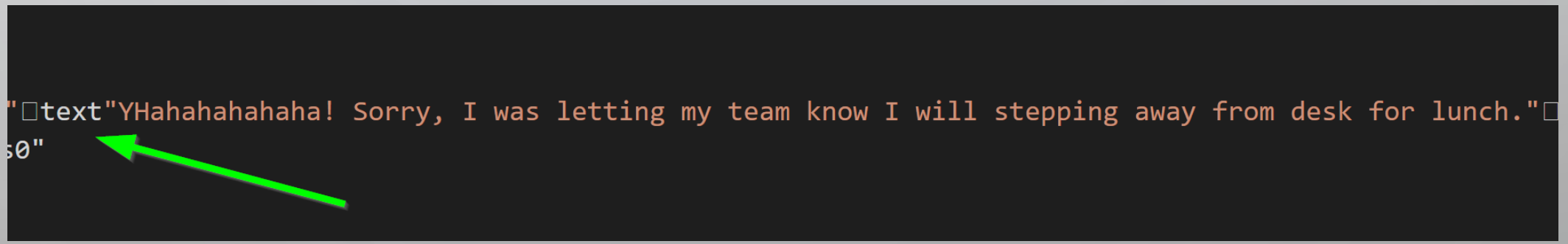
FIREFOX APPDATA ARTIFACT LOCATIONS

- %appdata%\Mozilla\Firefox\Profiles\<randomnumbers>
  - \logins.json & \key4.db
    - Password files
  - \formhistory.sqlite
    - Searches, and form data
  - \cookies.sqlite
    - Cookies to steal
  - \places.sqlite
    - Bookmarks, files downloaded, websites visted
  - \storage\
    - Client-side storage

SLACK DATA

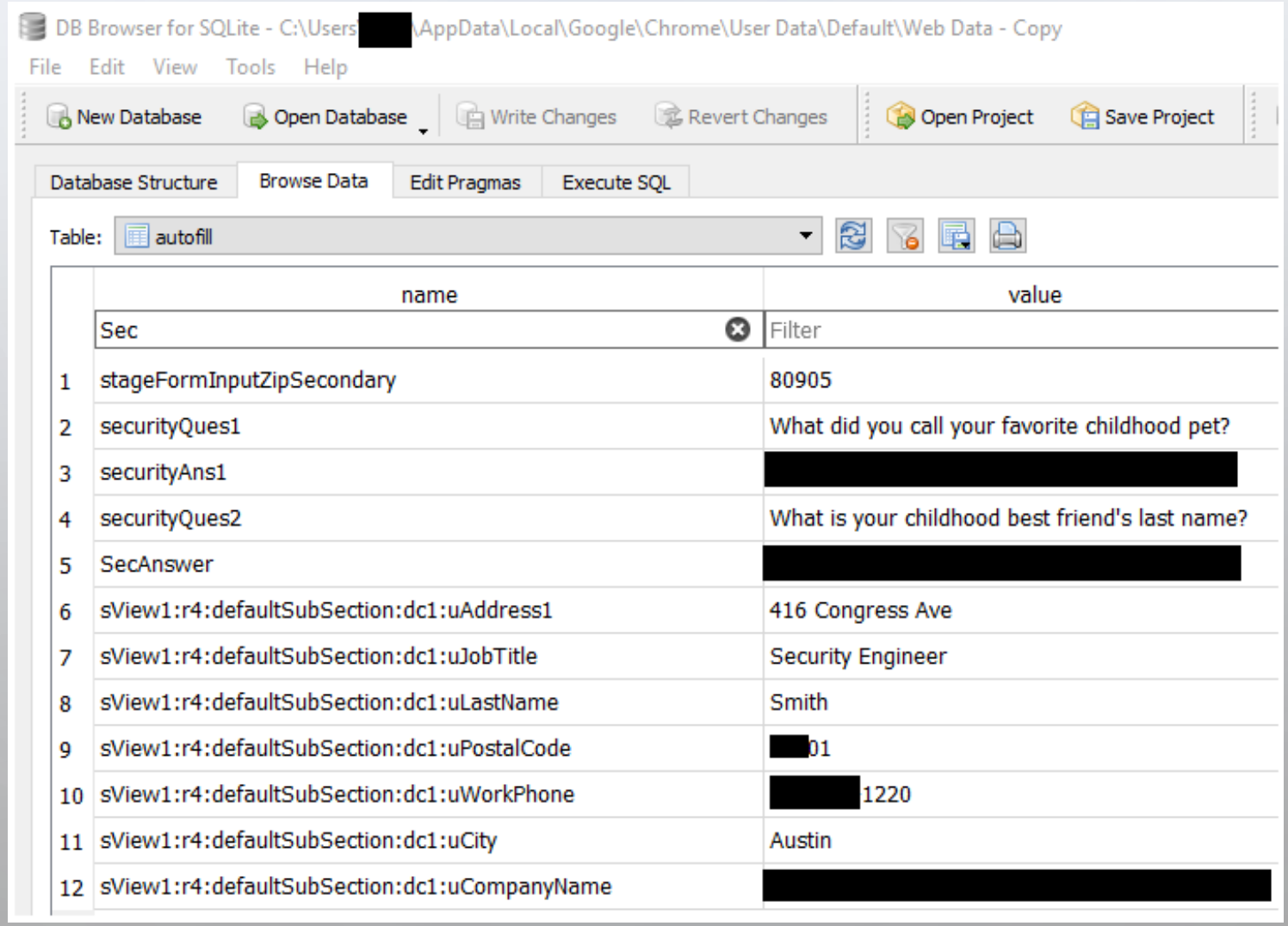
%LOCALAPPDATA%\GOOGLE\CHROME\USER DATA\DEFAULT\INDEXDB\HTTPS_APP.SLACK.COM_0.INDEXEDDB.LEVELDB





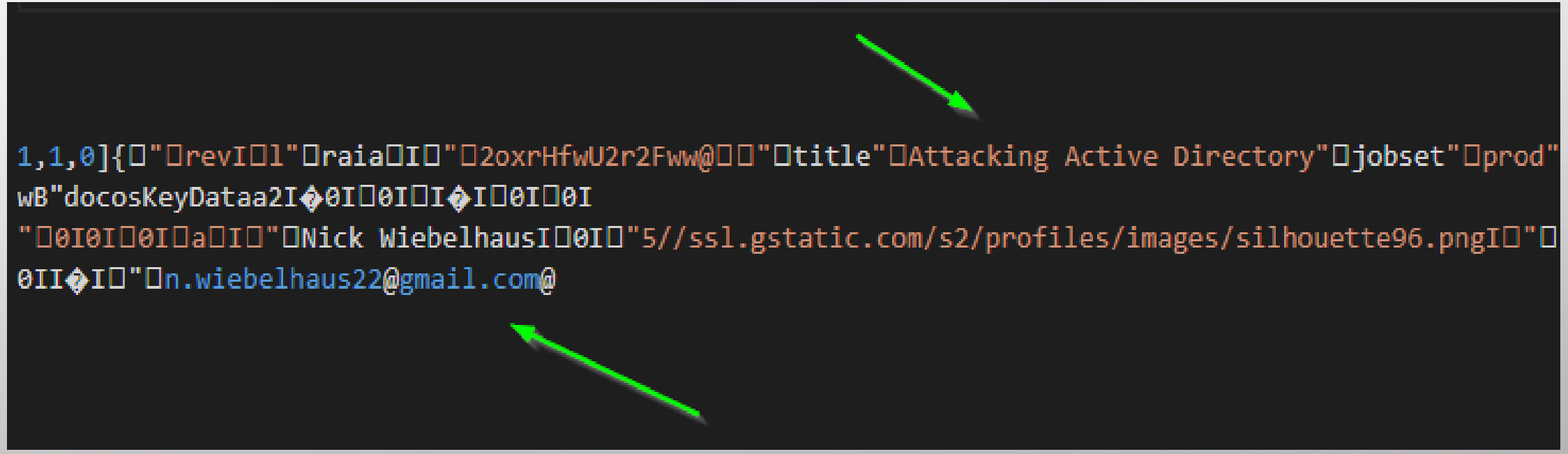
CHROME WEB DATA

%LOCALAPPDATA%\GOOGLE\CHROME\USER DATA\DEFAULT\WEB DATA



GOOGLE DOCS

%LOCALAPPDATA%\GOOGLE\CHROME\USER DATA\DEFAULT\INDEXEDDB\HTTPS_DOCS.GOOGLE.COM_0.INDEXEDDB.LEVELDB



DECRYPTING BROWSER PASSWORDS

- Different browsers have small difference
- Chrome
  - Metasploit: enum_chrome
  - Mimikatz: DPAPI
  - SharpWeb: https://github.com/djhohnstein/SharpWeb
- FireFox
  - Metasploit: firefox_creds
  - SharpWeb: https://github.com/djhohnstein/SharpWeb
- Internet Explorer
  - Metasploit: enum_ie (versions >=7)
  - Mimikatz: DPAPI
  - SharpWeb: https://github.com/djhohnstein/SharpWeb

DECRYPTING CHROME PASSWORDS AND COOKIES MIMIKATZ DPAPI

- Chrome uses the Windows Data Protect API (DPAPI) to protect the data in the “Cookies” and “Login Data” databases
- DPAPI is a Windows API that uses two functions to encrypt and decrypt data tied to a specific user or system
  - Encrypt: CryptProtectData()
  - Decrypt: CryptUnprotectData()
- Need a user master key
  - %appdata%\Microsoft\Protect\<SID>\<GUID>
- Decrypted using the user’s password or the domain backup key

APPDATA OS APPLICATION ARTIFACTS

- PowerShell PSReadline
  - %appdata%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
- Windows Subsystem for Linux (Plain text does not follow Linux permissions)
  - %localappdata%\Packages\KaliLinux.5fdsv
- KeePass Config
  - %appdata%\Keepass\KeePass.config.xml
- Notepad++ and VS Code
  - %appdata%\Notepad++\backup\<files>

DOMAIN ADMIN FROM PSREADLINE

%APPDATA%\MICROSOFT\WINDOWS\POWERSHELL\PSREADLINE\CONSOLEHOST_HISTORY.TXT

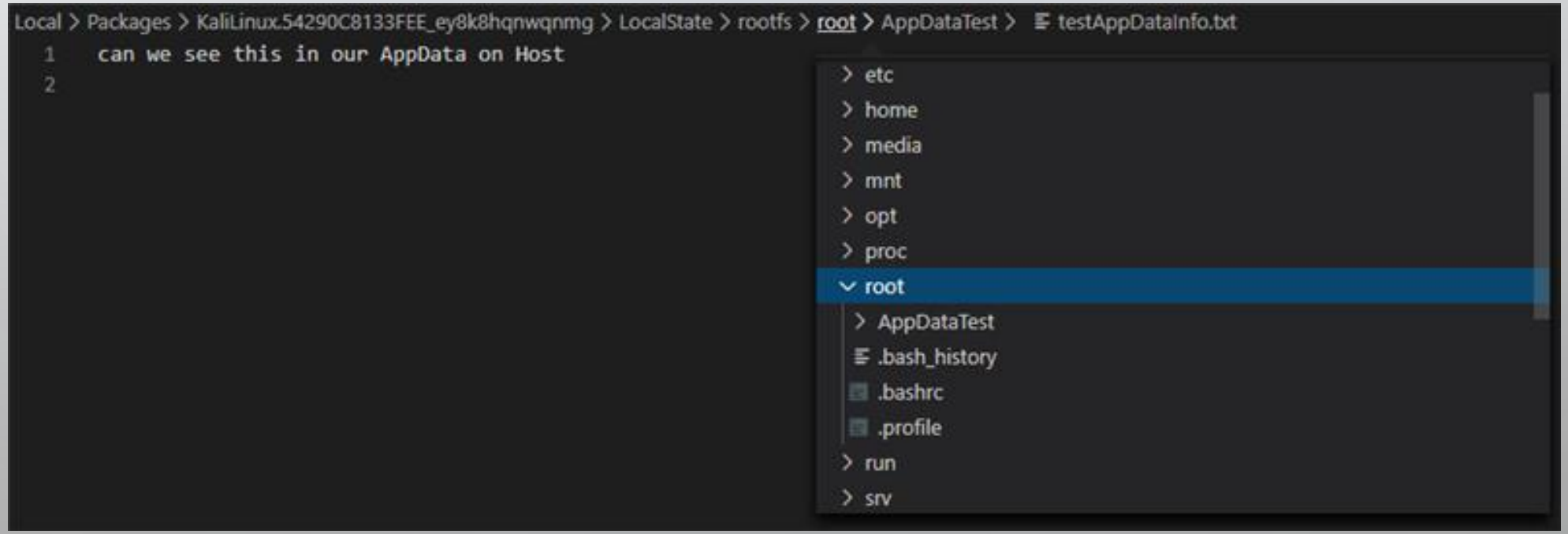
```
PS C:\WINDOWS\system32> .\CreateTicket.ps1 -Mode "CREATE" -TicketID-ErrorIncidentRequestType "2" -ErrorUDF_ResourceCriticality1 "4" -Category "2
" -ErrorItemOwner "2723" -ReferencedObjectName "HACKERS" -ErrorMonitoringPlatform "2" -Webserver "http://TalkServer/" -GetURLBase "RestAPI/api/"
 -User "HAcker\Awesome_Domain_Admin" -Password "Awesome_Domain_Admin_Password"
```

```
r "http://TalkServer/" -GetURLBase "RestAPI/api/" -User "HAcker\Awesome_Domain_Admin" -Password "Awesome_Domain_Admin_Password"
```

WINDOWS SUBSYSTEM FOR LINUX

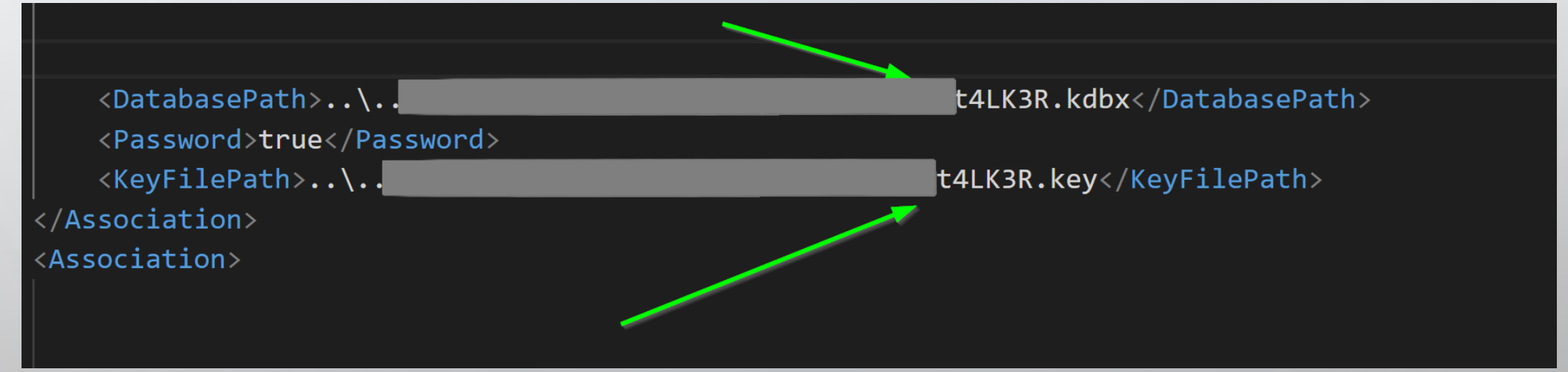
%LOCALAPPDATA%\PACKAGES\KALILINUX.5FDSV\LOCALSTATE\ROOTFS\ROOT

```
gh0st@gh0st:~$ sudo su
[sudo] password for gh0st:
root@gh0st:/home/gh0st# mkdir /root/AppDataTest
root@gh0st:/home/gh0st# cd /root/AppDataTest/
root@gh0st:~/AppDataTest# echo "can we see this in our AppData on Host" > testAppDataInfo.txt
root@gh0st:~/AppDataTest#
```



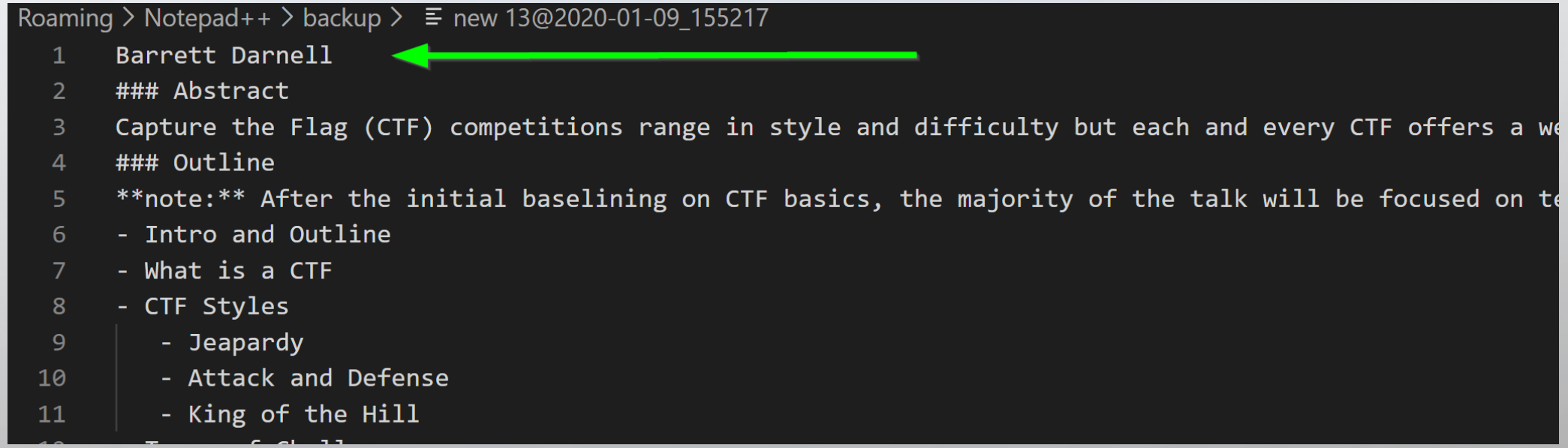
KEEPASS CONFIG

%APPDATA%\KEEPASS\KEEPASS.CONFIG.XML



NOTEPAD++ AND VS CODE

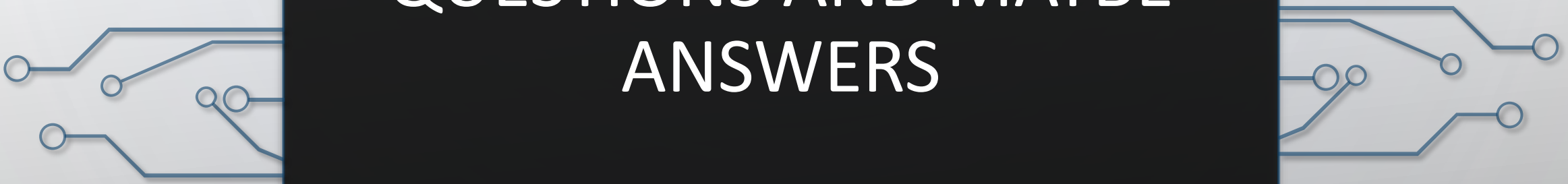
%APPDATA%\NOTEPAD++\BACKUP\<FILE>



WHAT CAN WE DO ABOUT IT?

- Avoid Client-Side Storage and Processing
  - HTTP header “Cache Control:”
  - Avoid storing sensitive data with IndexDB
  - OWASP HTML5 Security Cheat Sheet – Storage APIs
    - https://owasp.org/www-project-cheat-sheets/cheatsheets/HTML5_Security_Cheat_Sheet
- Understanding native OS features
- Create an Application Whitelist
  - Understand what data is being stored for all applications
  - Understand where the data is and why for all applications
  - Make a risk based assessment for whitelist

QUESTIONS AND MAYBE ANSWERS



DECRYPTING CHROME PASSWORDS AND COOKIES MIMIKATZ DPAPI PART 2

- Dump “Cookies” and “Login Data” as logged in user
  - Mimikatz dpapi::chrome /in:”%localappdata%\Google\Chrome\User Data\Default\Login Data” /unprotect
  - Mimikatz dpapi::chrome /in:”%localappdata%\Google\Chrome\User Data\Default\Cookies” /unprotect
- Dump “Cookies” and “Login Data” of target logged in user (Need to be Admin)
  - Locate the GUID and SHA1 hash for the targets master key
  - C:\Users\<target>\AppData\Roaming\Microsoft\Protect\<SID>\GUID>
  - sekurlsa::dpapi
  - Mimikatz dpaip:chrome /in:”C:\Users\<target>\AppData\Local\Google\Chrome\User Data\Default\Cookies” /masterkey:<SHA1 Hash>
  - Mimikatz dpaip:chrome /in:”C:\Users\<target>\AppData\Local\Google\Chrome\User Data\Default\Login Data” /masterkey:<SHA1 Hash>