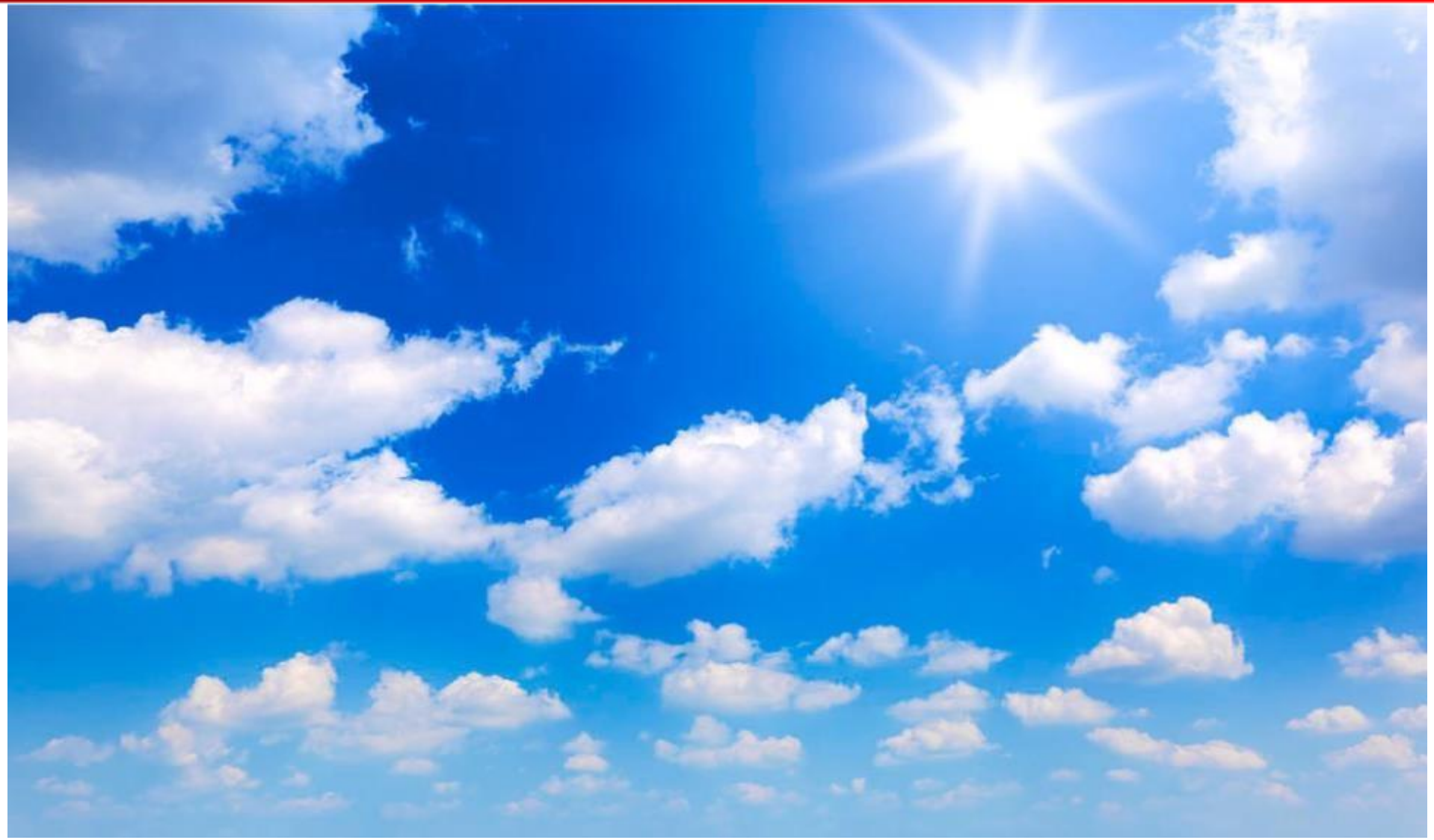
Cyber Security
Lession 15



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

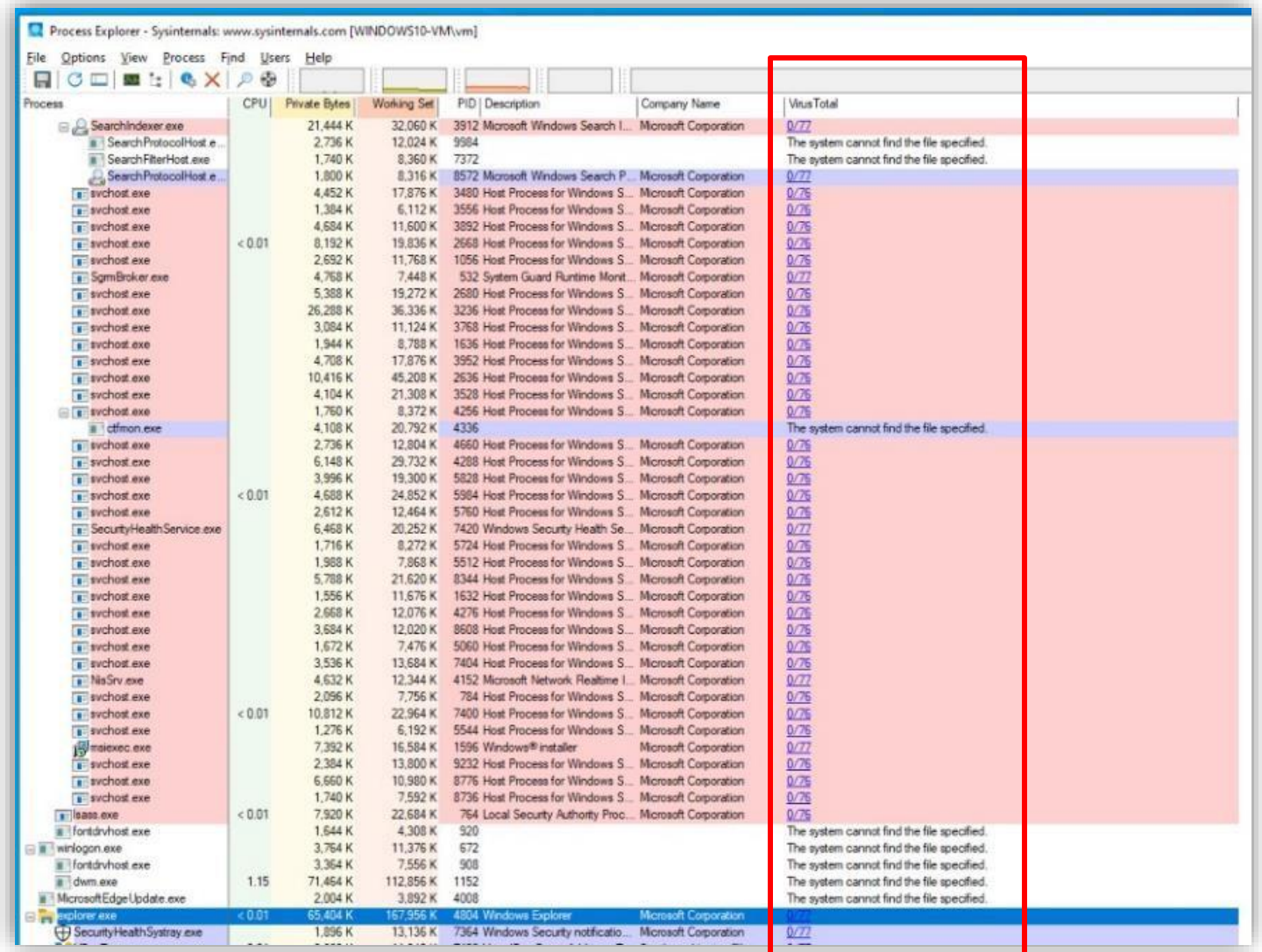
Assignments

Published: May 28, 2024

Download Process Explorer (3.3 MB)

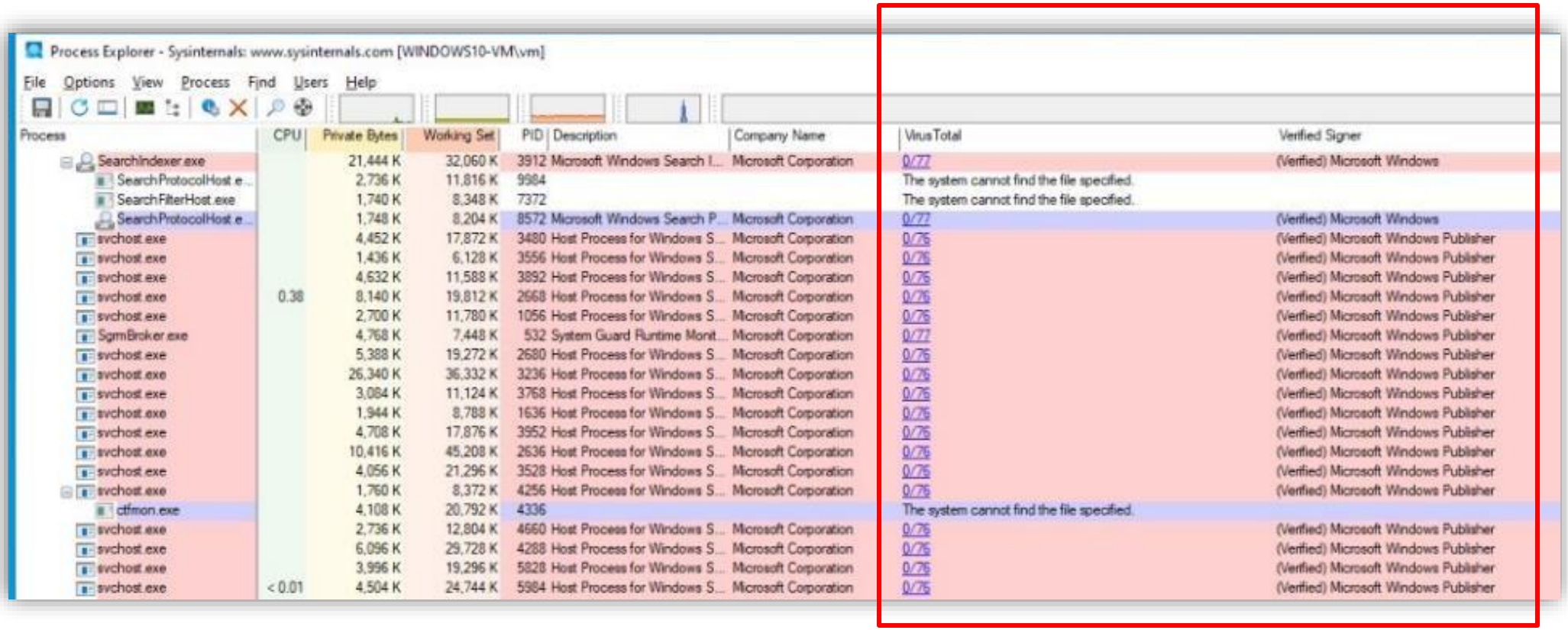
Run now from Sysinternals Live.

https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Assignments



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

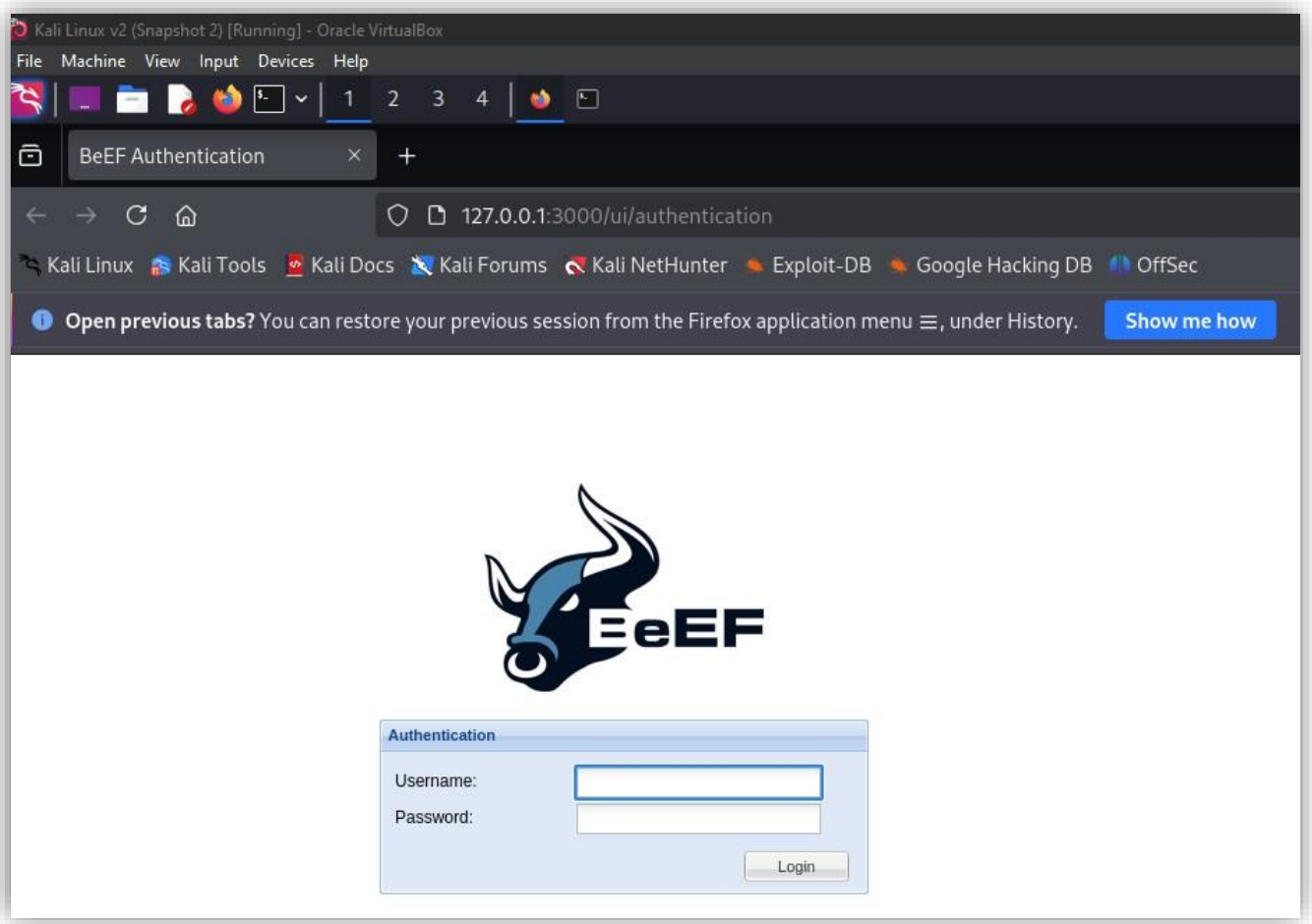
Assignments

sudo apt install beef-xss

LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Assignments

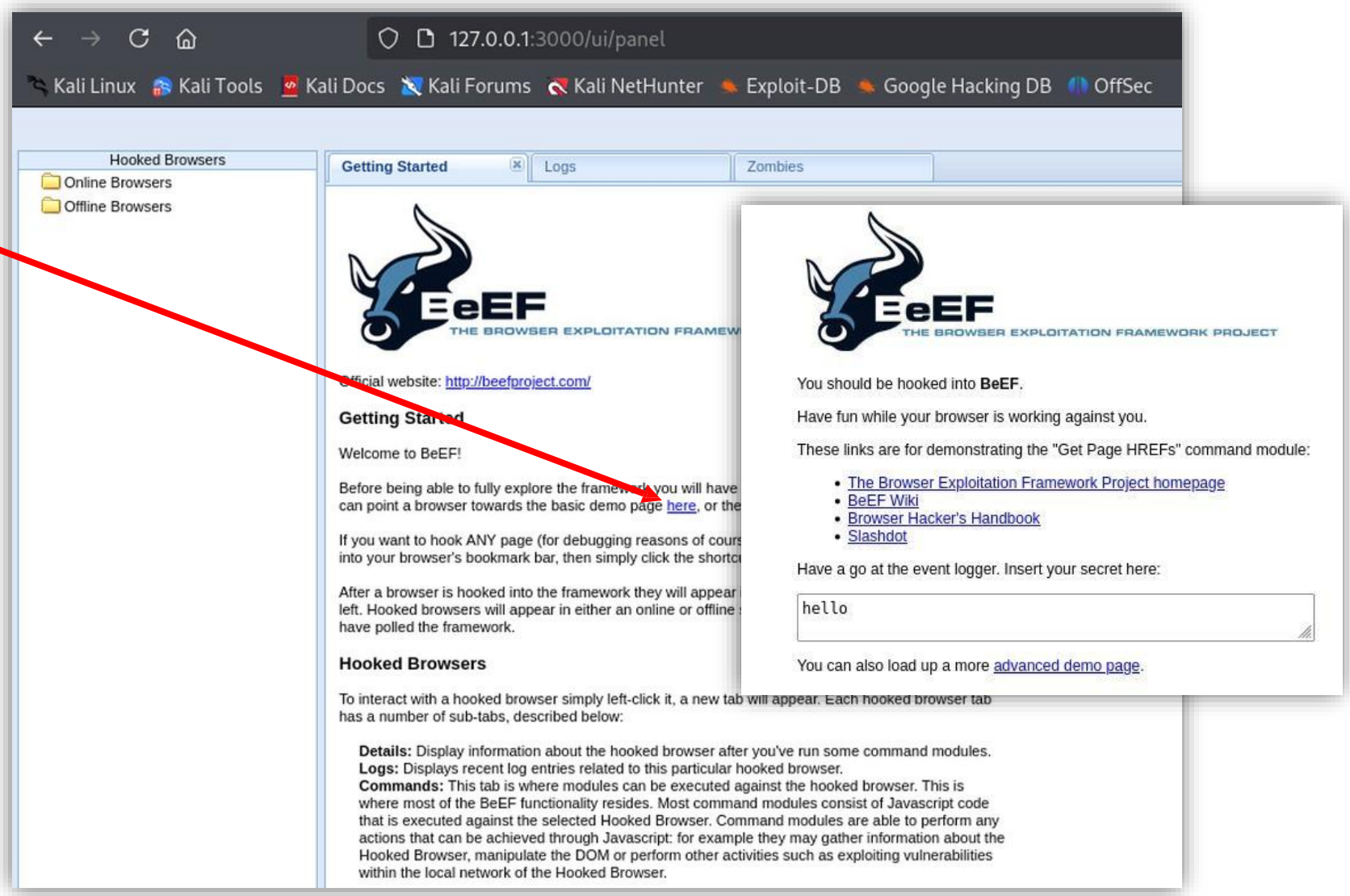
Username: beef
Password: <.....>



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Assignments

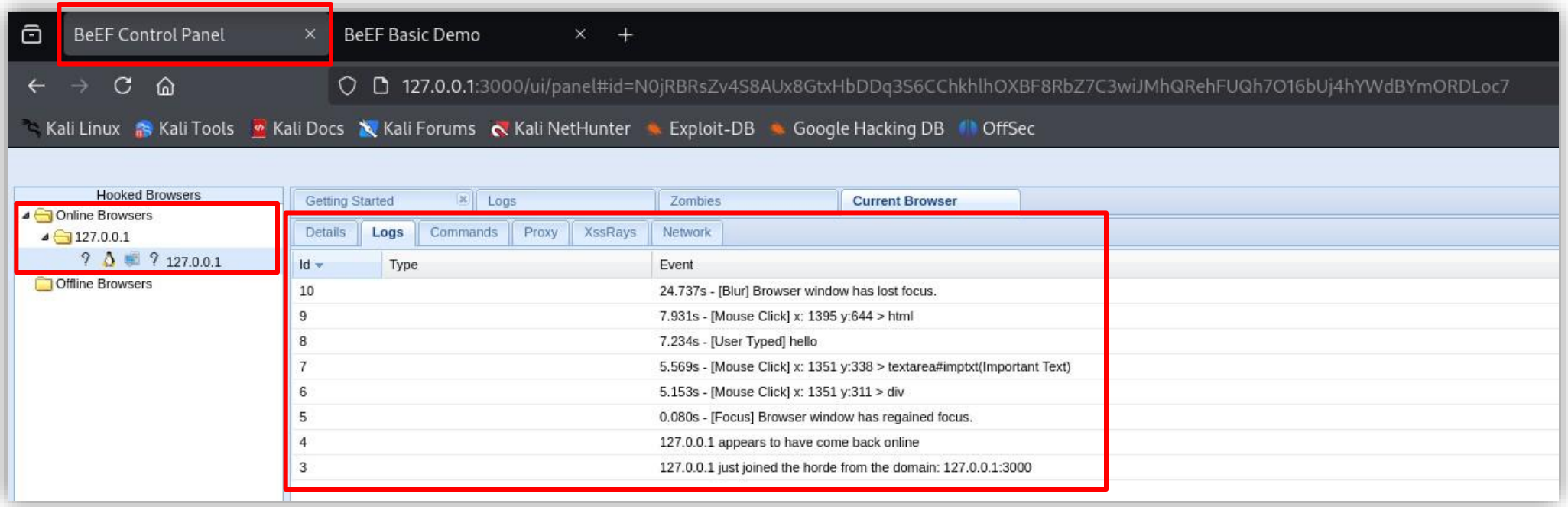
Basic demo page [link]



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Assignments

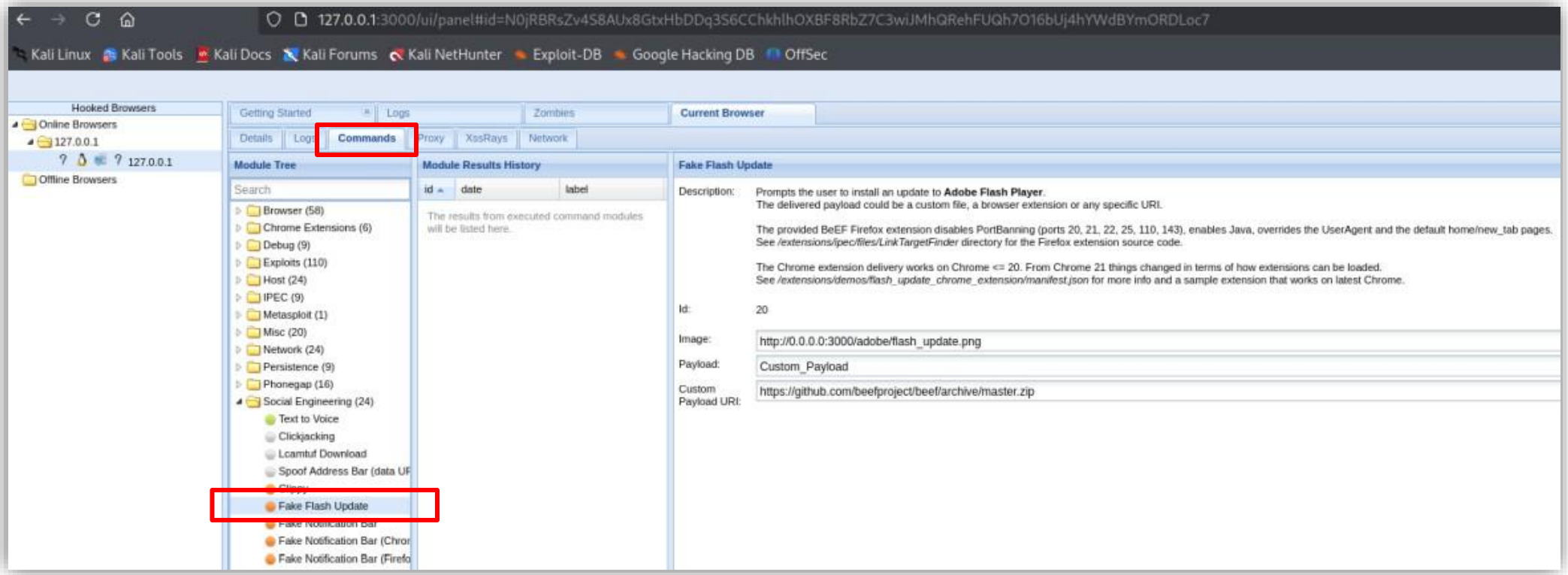
Where is **Logs** tab?



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

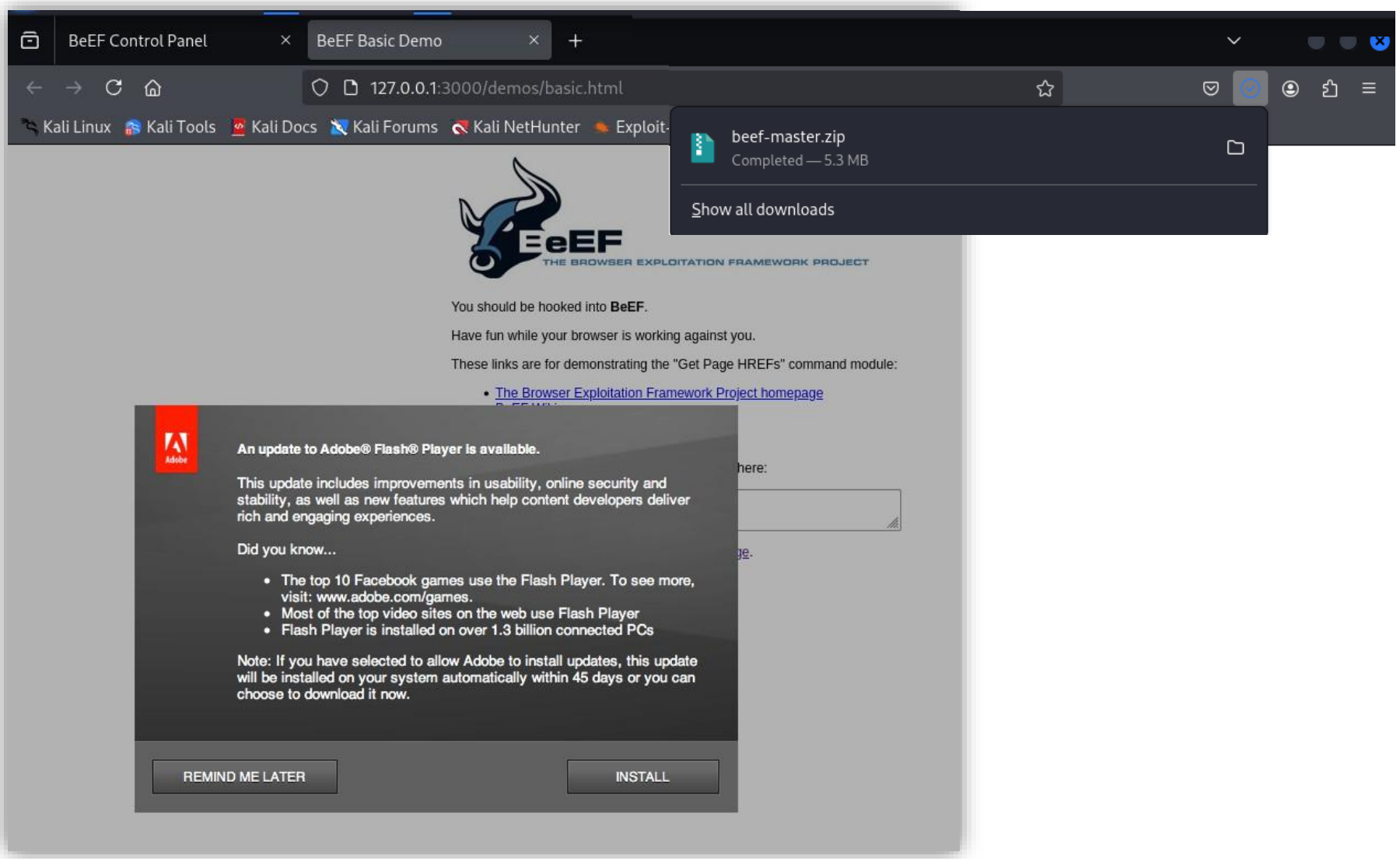
Assignments

Fake Flash Update command



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

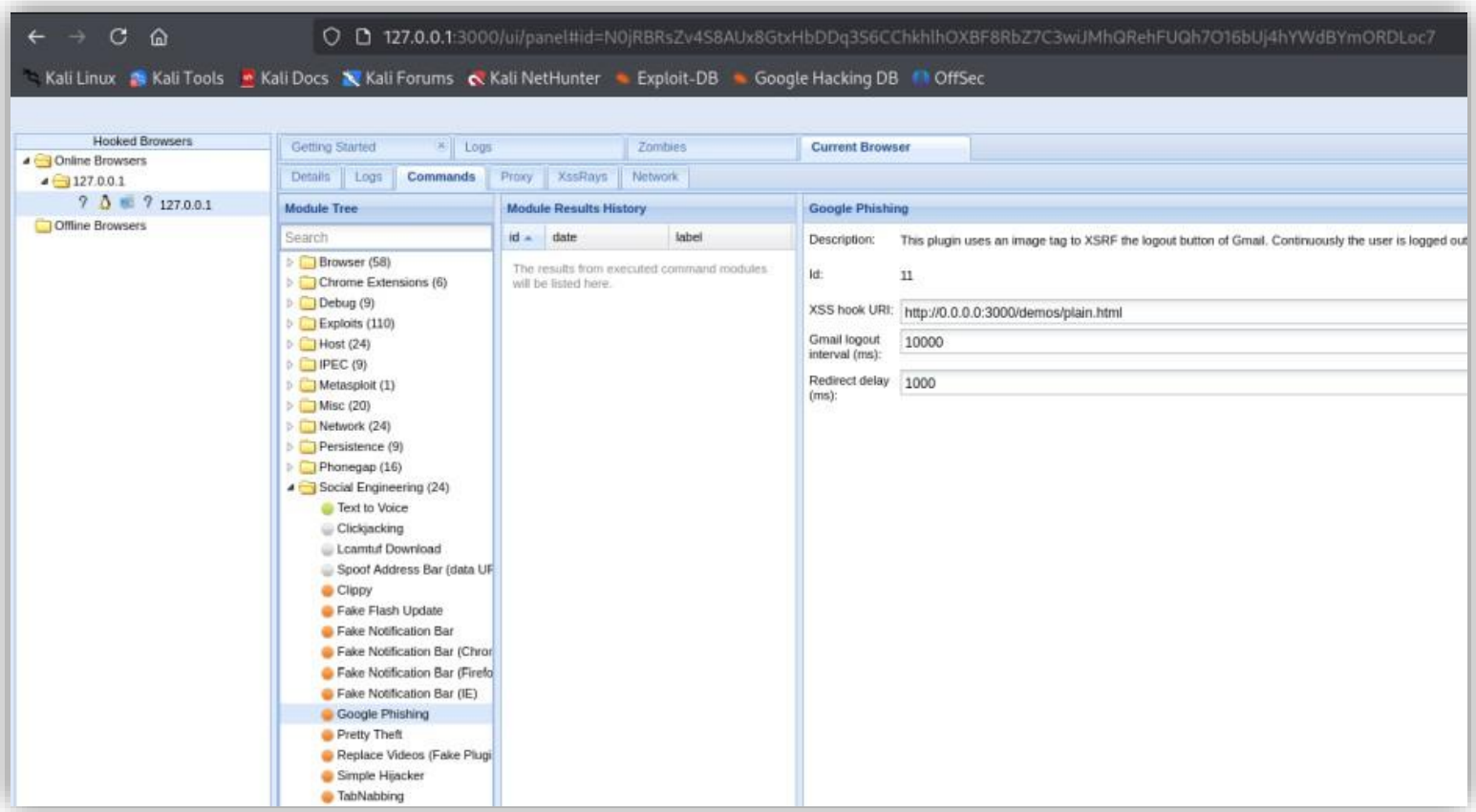
Assignments



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

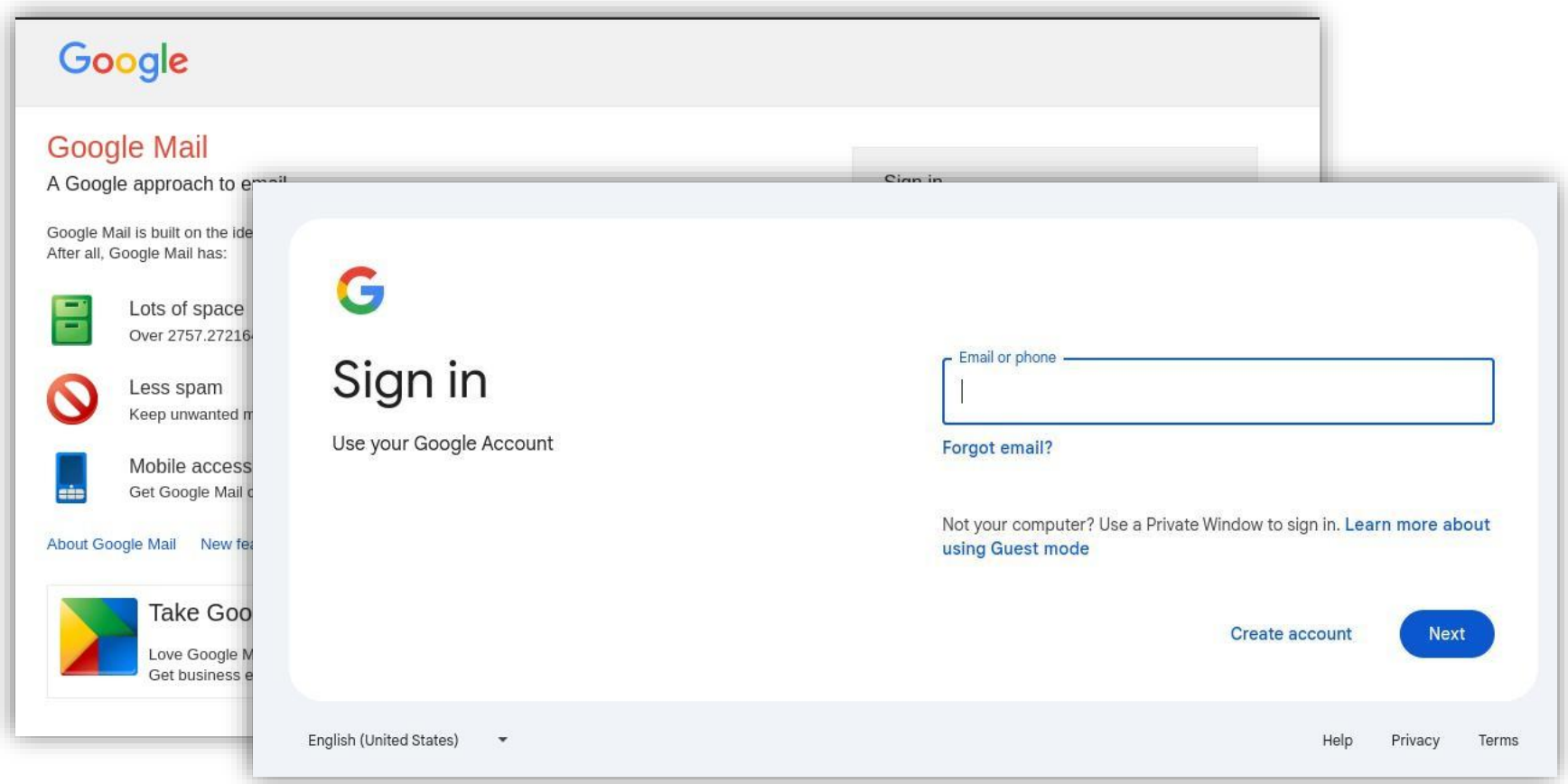
Assignments

Google Phishing command



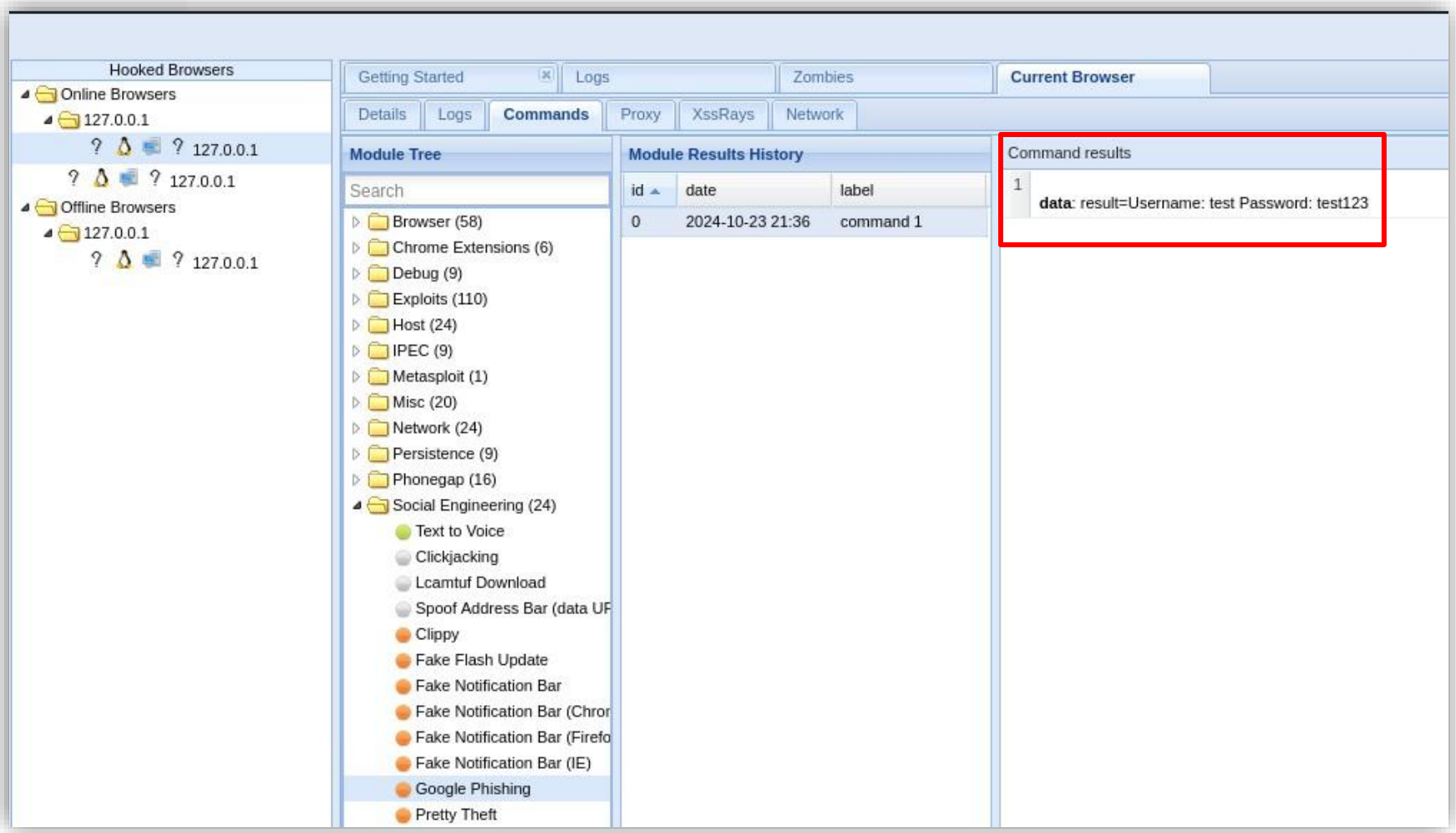
LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Assignments



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Assignments



Social engineering and neuro-linguistic programming

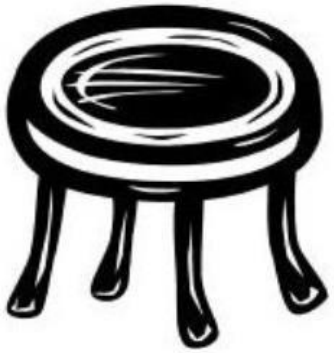
(Chapter 2)

Introduction

- What is social engineering; DONE
- The most popular techniques (methods); DONE
- Psychological attacks; DONE
- Neurolinguistic programming and neurolinguistics; DONE
- Hybrid attack. TO BE CONTINUE...

In the previous lession…

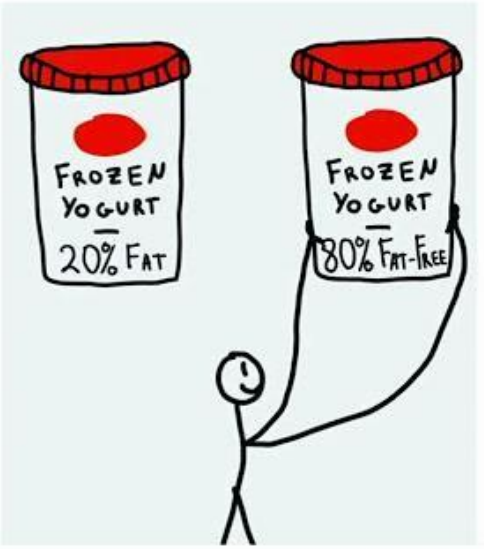
The Four Legs (Pillars) of NLP

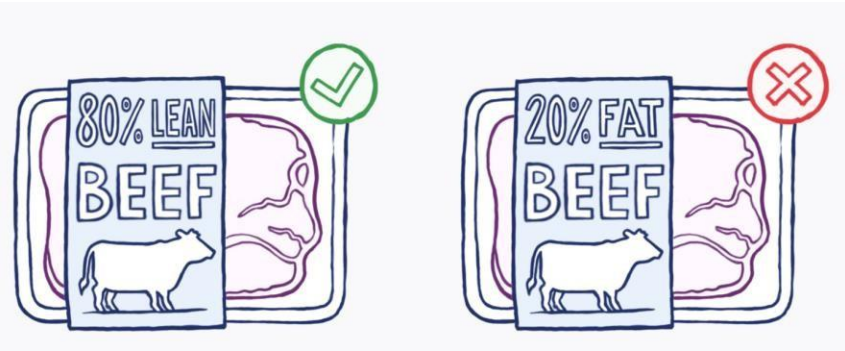


The following are the four pillars of NLP:

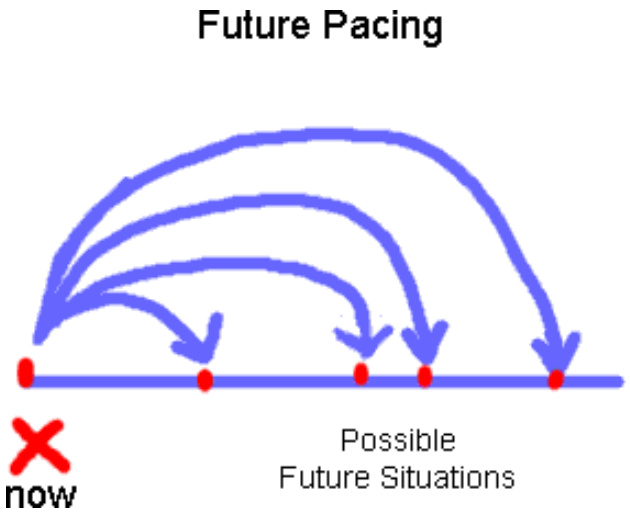
Rapport	Outcome Orientation	Sensory Acuity	Behavioral Flexibility
Rapport is about getting on with and trusted by another person.	Outcome Orientation is about knowing what you want and going for and ensuring it is in your control.	Sensory Acuity is about tuning into our senses and learning to make finer and more useful distinctions about the information we get from the world.	Behavioral Flexibility is about understanding the other's point of view and how it adds to our ability to be highly effective communicators.

Anchoring (Examples)





Future pacing (examples)

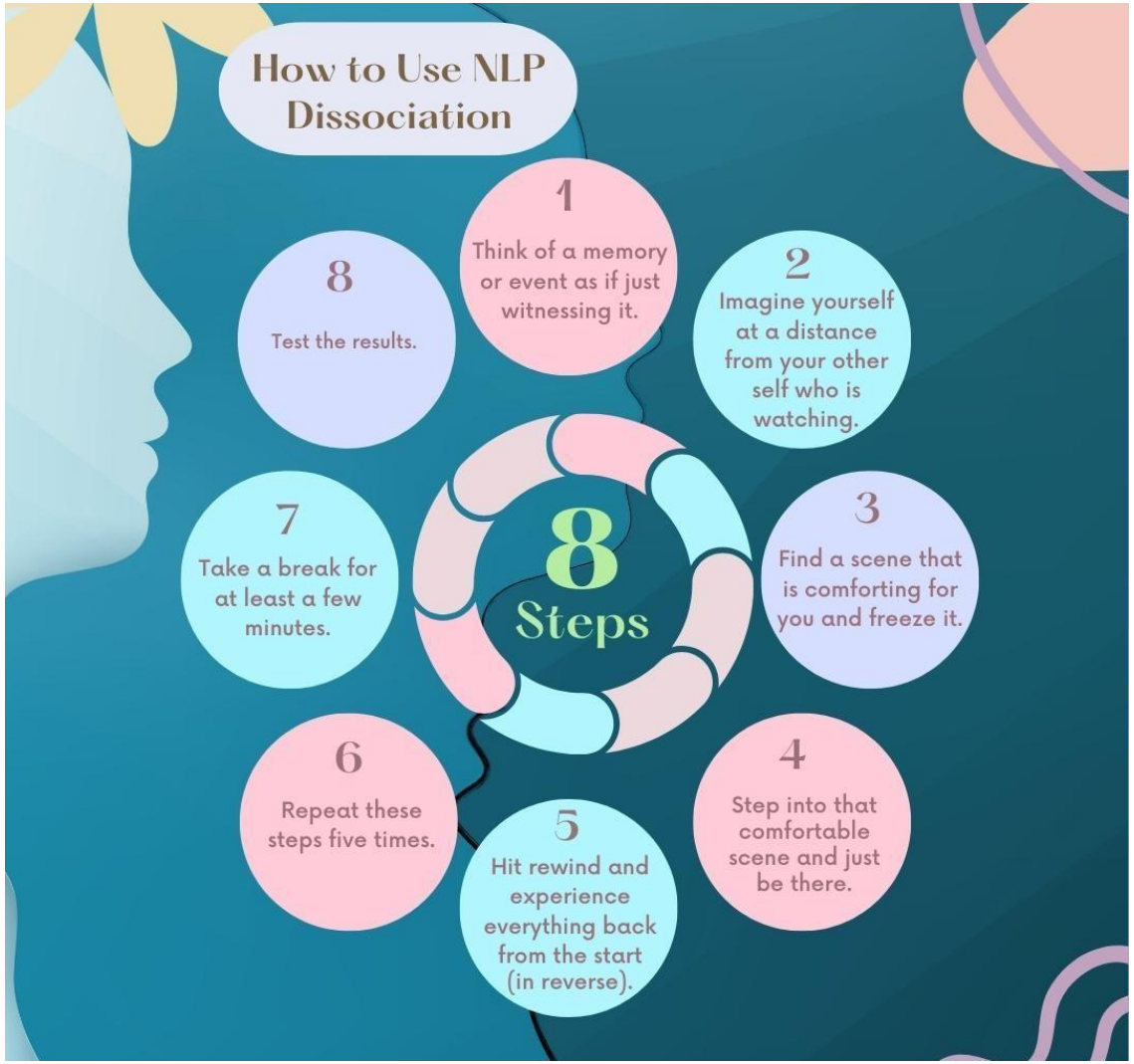


Examples of future pacing phrases:

- "Just imagine..."
- "Imagine this:"
- "What would you do with..."
- "You'll love..."
- "Can't you just see yourself now..."

Swish (examples)

Visual Kinesthetic Dissociation (VK/D)

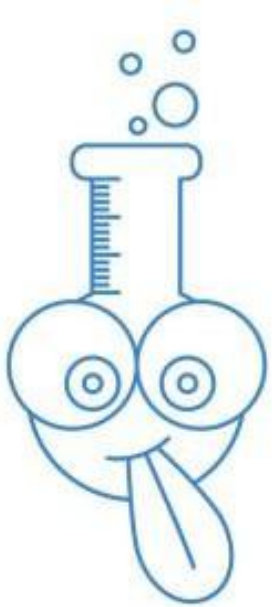


Lession 15

Quiz

Assignments

12 Questions
20 minutes



Understanding Identity and Access Management

Introduction

- Exploring Authentication Management
- Managing Accounts
- Comparing Authentication Services
- Comparing Access Control Schemes

Exploring Authentication Concepts

- Identification
  - User professes an identity
- Authentication
  - User proves identity
- Authorization
  - Access to resources granted based on proven identity

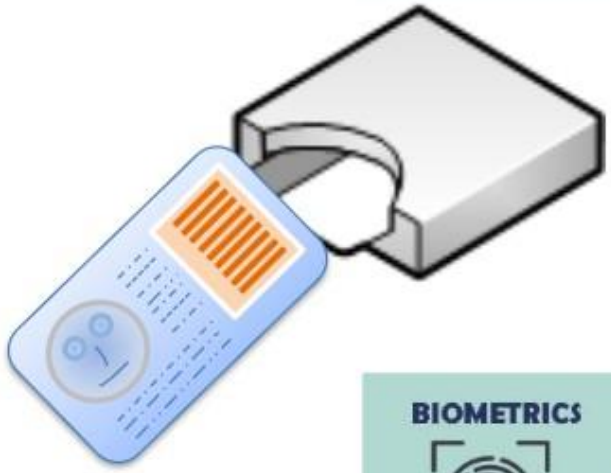
Exploring Authentication Concepts

- AAA (authentication, authorization, and accounting)
- Accounting
- Audit trail

Factors of Authentication

- Something you know
  - Such as username and password

- Something you have
  - Such as a smart card

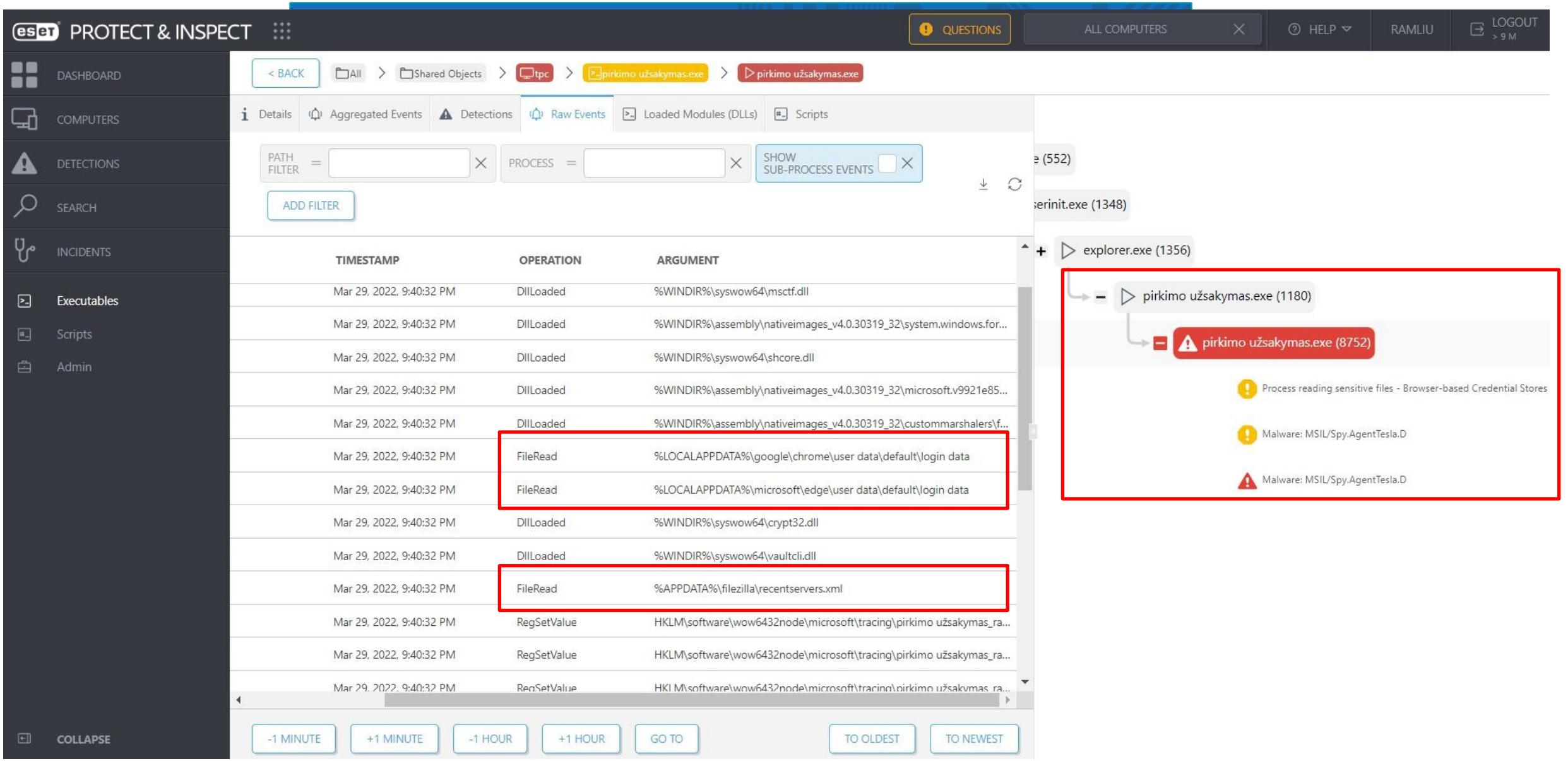


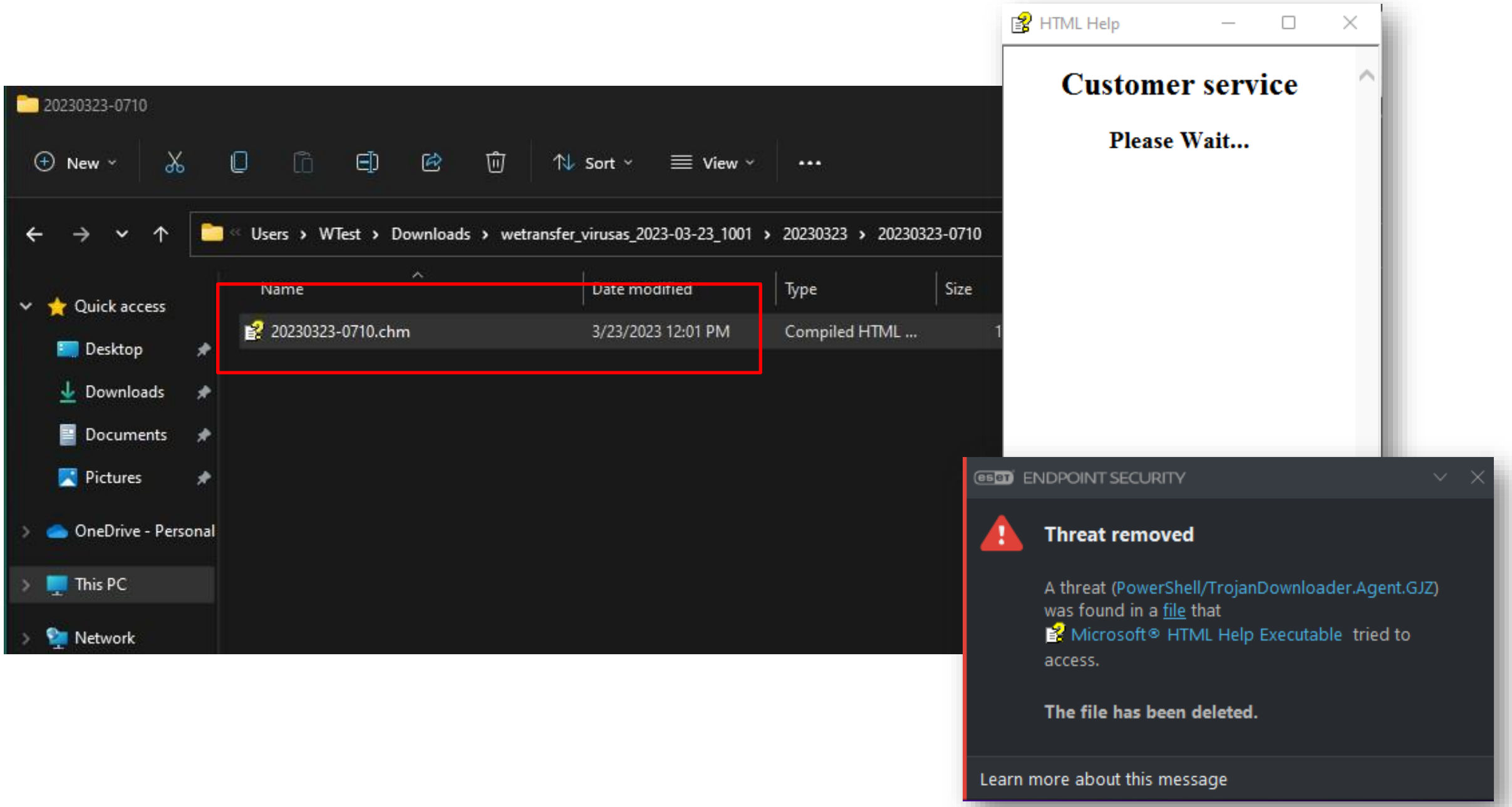
- Something you are
  - Such as a fingerprint or other biometric identification

Something You Know

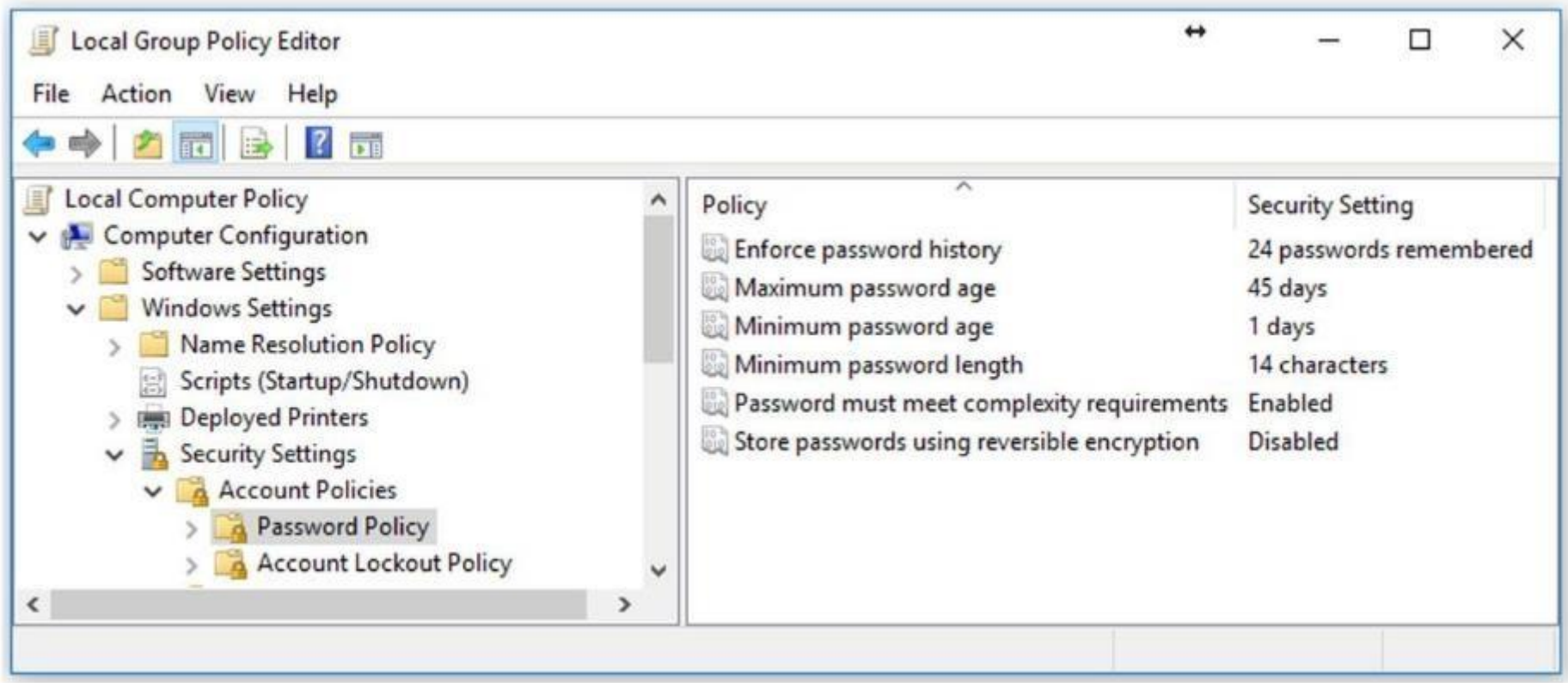
- Password complexity
  - Uppercase, lowercase, numbers, special characters
- Password expiration
  - Forces users to change password
- Password vaults
- Password history and password reuse
  - Prevents users from reusing same password

How steal the password from web browser?


PROTECT & INSPECT
QUESTIONS
ALL COMPUTERS
HELP
RAMLIU
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Admin
COLLAPSE
< BACK
All
Shared Objects
tpc
pirkimo užsakymas.exe
pirkimo užsakymas.exe
Details
Aggregated Events
Detections
Raw Events
Loaded Modules (DLLs)
Scripts
PATH FILTER
PROCESS
SHOW SUB-PROCESS EVENTS
ADD FILTER
TIMESTAMP
OPERATION
ARGUMENT
Mar 29, 2022, 9:40:32 PM DllLoaded %WINDIR%\syswow64\msctf.dll
Mar 29, 2022, 9:40:32 PM DllLoaded %WINDIR%\assembly\nativeimages_v4.0.30319_32\system.windows.for...
Mar 29, 2022, 9:40:32 PM DllLoaded %WINDIR%\syswow64\shcore.dll
Mar 29, 2022, 9:40:32 PM DllLoaded %WINDIR%\assembly\nativeimages_v4.0.30319_32\microsoft.v9921e85...
Mar 29, 2022, 9:40:32 PM DllLoaded %WINDIR%\assembly\nativeimages_v4.0.30319_32\custommarshalers\f...
Mar 29, 2022, 9:40:32 PM FileRead %LOCALAPPDATA%\google\chrome\user data\default\login data
Mar 29, 2022, 9:40:32 PM FileRead %LOCALAPPDATA%\microsoft\edge\user data\default\login data
Mar 29, 2022, 9:40:32 PM DllLoaded %WINDIR%\syswow64\crypt32.dll
Mar 29, 2022, 9:40:32 PM DllLoaded %WINDIR%\syswow64\vaultcli.dll
Mar 29, 2022, 9:40:32 PM FileRead %APPDATA%\filezilla\recentservers.xml
Mar 29, 2022, 9:40:32 PM RegSetValue HKLM\software\wow6432node\microsoft\tracing\pirkimo užsakymas_ra...
Mar 29, 2022, 9:40:32 PM RegSetValue HKLM\software\wow6432node\microsoft\tracing\pirkimo užsakymas_ra...
-1 MINUTE
+1 MINUTE
-1 HOUR
+1 HOUR
GO TO
TO OLDEST
TO NEWEST
e (552)
serinit.exe (1348)
explorer.exe (1356)
pirkimo užsakymas.exe (1180)
pirkimo užsakymas.exe (8752)
Process reading sensitive files - Browser-based Credential Stores
Malware: MSIL/Spy.AgentTesla.D
Malware: MSIL/Spy.AgentTesla.D


20230323-0710
New
Sort
View
Users › WTest › Downloads › wetransfer_virusas_2023-03-23_1001 › 20230323 › 20230323-0710
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive - Personal
This PC
Network
Name
Date modified
Type
Size
20230323-0710.chm
3/23/2023 12:01 PM
Compiled HTML ...
HTML Help
Customer service
Please Wait...
ENDPOINT SECURITY
Threat removed
A threat (PowerShell/TrojanDownloader.Agent.GJZ) was found in a file that
Microsoft® HTML Help Executable tried to access.
The file has been deleted.
Learn more about this message

Something You Know

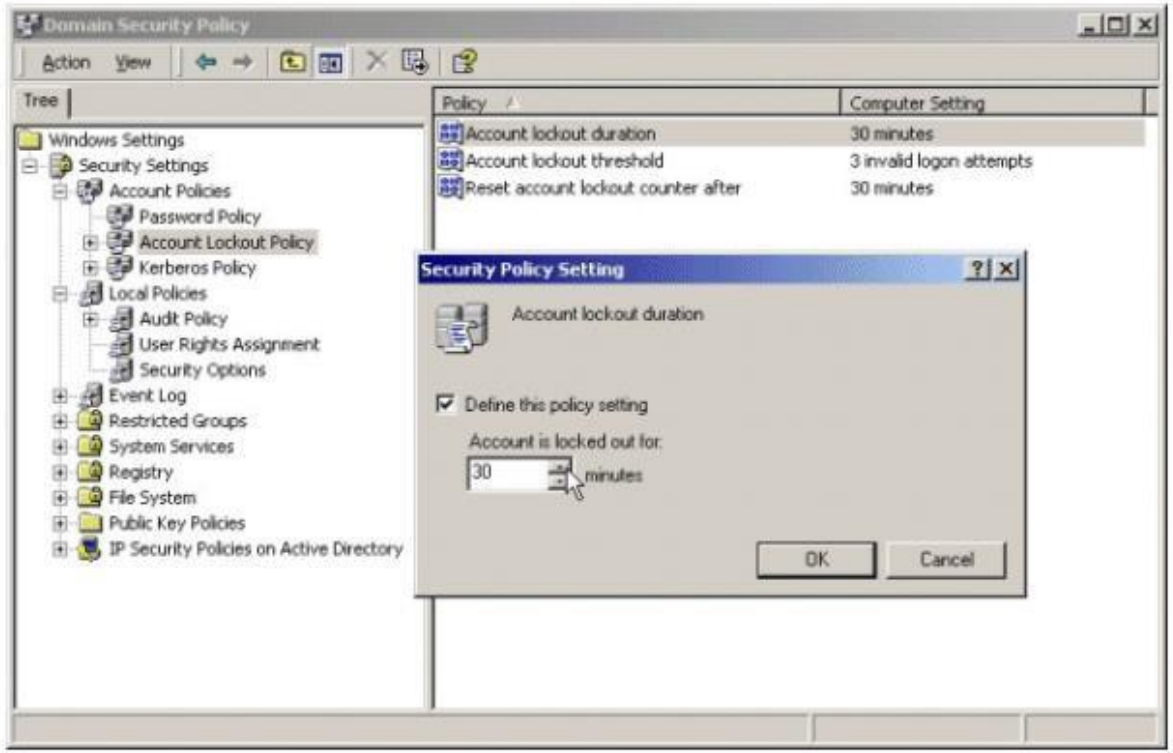


Something You Know

- Password keys
- Knowledge-Based Authentication
- Changing Default Passwords
- Training Users About Password Behaviors

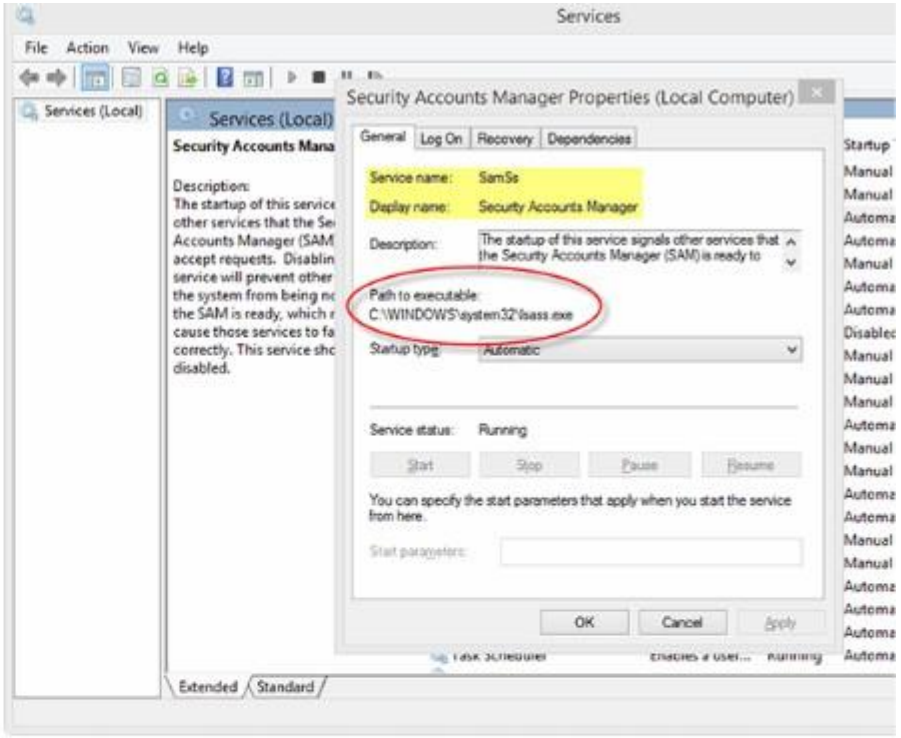
Something You Know

- Account lockout policies
  - Account lockout threshold
  - Account lockout duration



Security Account Manager (SAM)

- A database file in Windows XP, Windows Vista, Windows 7, 8.1, 10 and 11 that stores users' passwords;
- It can be used to authenticate local and remote users;
- Beginning with Windows 2000 SP4, Active Directory authenticates remote users;
- SAM uses cryptographic measures to prevent unauthenticated users accessing the system;
- The user passwords are stored in a hashed format in a registry hive either as an LM hash or as an NTLM hash;
- This file can be found in **%SystemRoot%/system32/config/SAM** and is mounted on HKLM/SAM and SYSTEM privileges are required to view it;
- In an attempt to improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0;
- When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted, so that the password hash values for all local accounts stored in the SAM are encrypted with a key (usually also referred to as the "SYSKEY");
- It can be enabled by running the ***syskey*** program;
- As of Windows 10 version 1709, ***syskey*** was removed due to a combination of insecure security and misuse by bad actors to lock users out of systems;



- LM hash is a compromised protocol and has been replaced by NTLM hash;
- Most versions of Windows can be configured to disable the creation and storage of valid LM hashes when the user changes their password;
- Windows Vista and later versions of Windows disable LM hash by default.

Linux “SAM”

- **/etc/passwd file**
  - ✓ Stores user account information important for the login process in Unix-like operating systems.
  - ✓ Is a plain text file with information for all user accounts;
  - ✓ It includes a list of user accounts on the system, as well as details such as user ID, group ID, home directory, and default shell;
  - ✓ The root user owns the file, and only the root user or users with sudo privileges are able to modify the file;
  - ✓ *All system users have read access*.

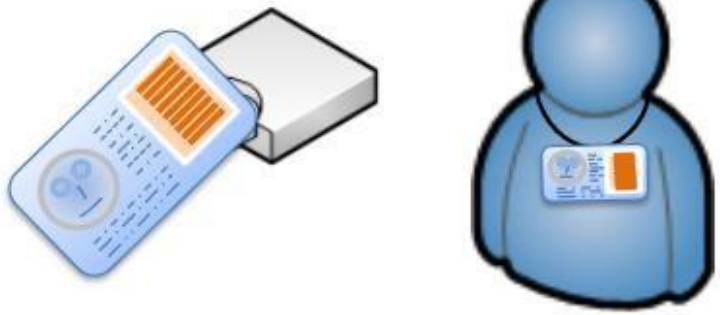
- **/etc/shadow file**
  - ✓ Is a companion file to /etc/passwd, designed to store encrypted user passwords;
  - ✓ The file follows a specific format for each entry.
  - ✓ Each line represents a user account and consists of several fields separated by colons “:”;
  - ✓ The fields include:
    - ➢ The username;
    - ➢ Encrypted password;
    - ➢ Password aging info (such as password expiration and change history);
    - ➢ Account locking status;
  - ✓ *Is readable only by privileged users*.

SAM dump

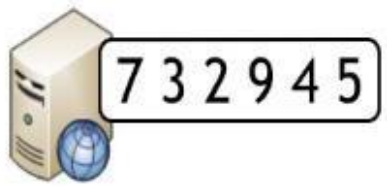
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >
```

Something You Have

- Smart cards
  - CACs and PIVs (US government)



- Tokens or Key fobs



Key fobs


DIIO


HSBC
1
2
3
4
5
6
7
8
9
0

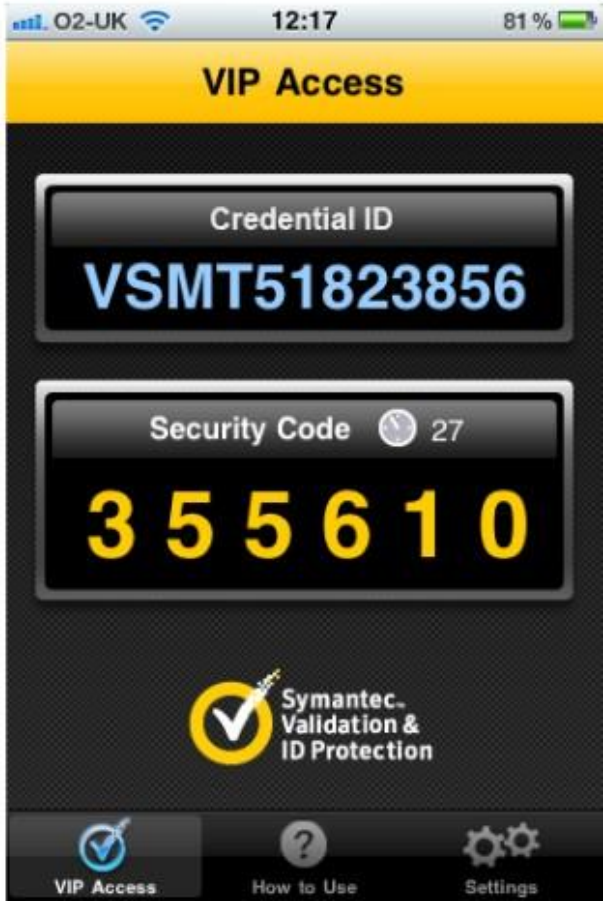

TOKEN


SafeID
DEEPNET SECURITY


OTP c200
ONE TIME PASSWORD

Something You Have

- HOTP and TOTP used in hardware tokens
- HOTP
  - HMAC-based One-Time Password
- TOTP
  - Time-based One-Time Password
  - Expire after 30 seconds

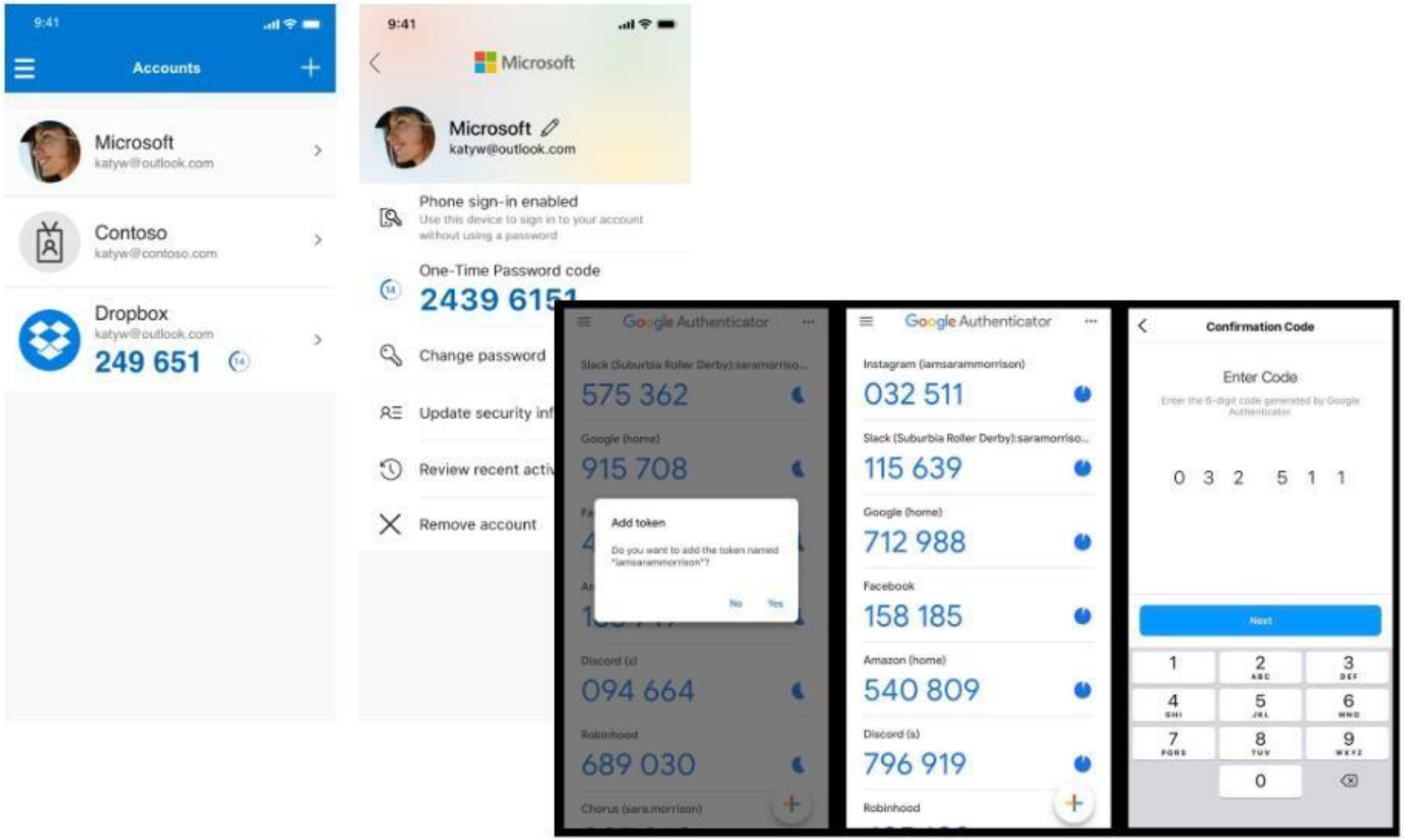


Something You Have

- Authentication applications

- Two-Step Verification
  - Sent via SMS, a phone call, a push notification

Software key fobs



Something You Are

- Biometrics Methods
  - Fingerprint, thumbprint, or handprints;
  - Retinal scanners (scans the retina of one or both eyes);
  - Iris scanners (scans the iris of one or both eyes);

Something You Are

- Biometrics Methods
  - Vein matching
  - Voice recognition
  - Facial recognition
  - Gait analysis

Biometric passport

- A biometric passport (also known as an electronic passport, e-passport or a digital passport) is a traditional passport that has an embedded electronic microprocessor chip, which contains biometric information that can be used to authenticate the identity of the passport holder;
- It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or centre page, of the passport;
- The passport's critical information is printed on the data page of the passport, repeated on the machine readable lines and stored in the chip;
- Public key infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip, supposedly making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented;
- The currently standardised biometrics used for this type of identification system are facial recognition, fingerprint recognition, and iris recognition

Data protection in biometric passports

- Non-traceable chip characteristics
- Basic Access Control (BAC)
- Passive Authentication (PA)
- Active Authentication (AA)
- Extended Access Control (EAC)
- Supplemental Access Control (SAC)
- Shielding the chip

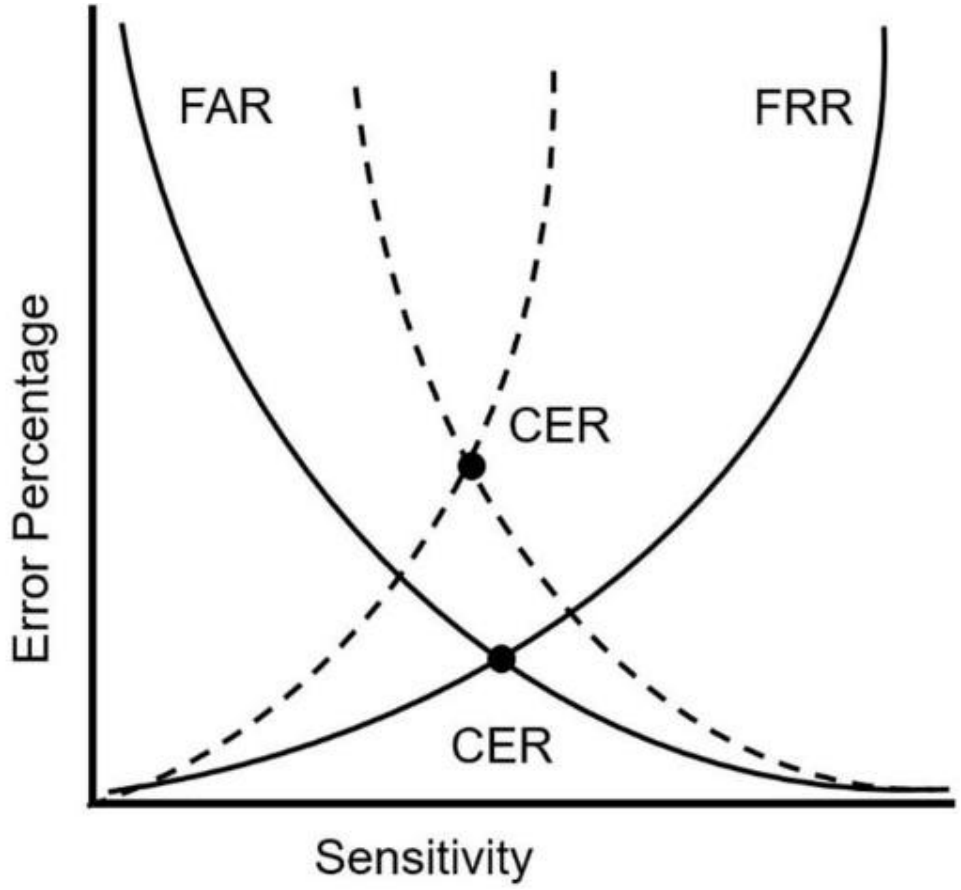
Biometrics

- False acceptance
- False rejection
- True acceptance
- True rejection

	Biometric System Not Accurate	Biometric System Accurate
Registered User	**False Acceptance**	True Acceptance
Unknown User	**False Rejection**	True Rejection

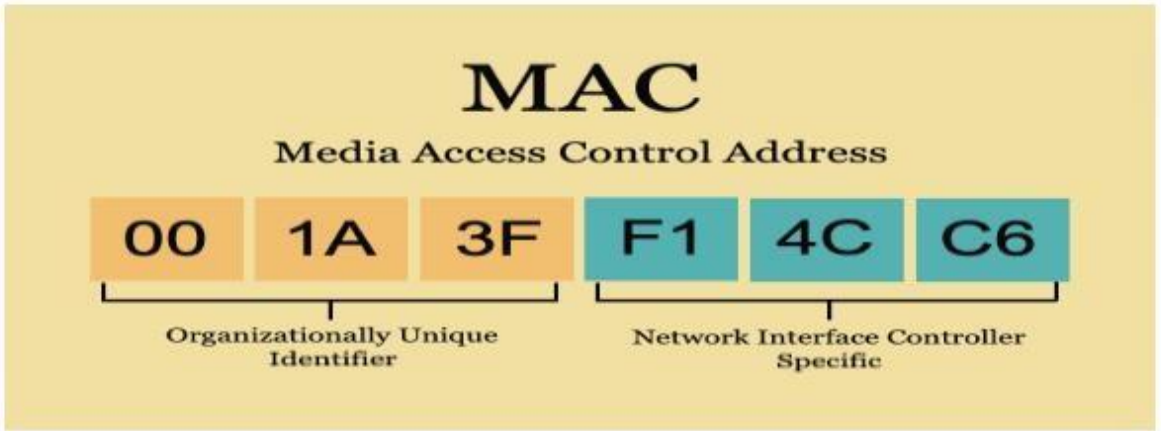
Biometrics

- Crossover error rate
  - False acceptance rate
  - False rejection rate
  - Lower CER indicates better accuracy



Somewhere You are

- Often uses geolocation
  - IP address
  - MAC address



Authentication Attributes

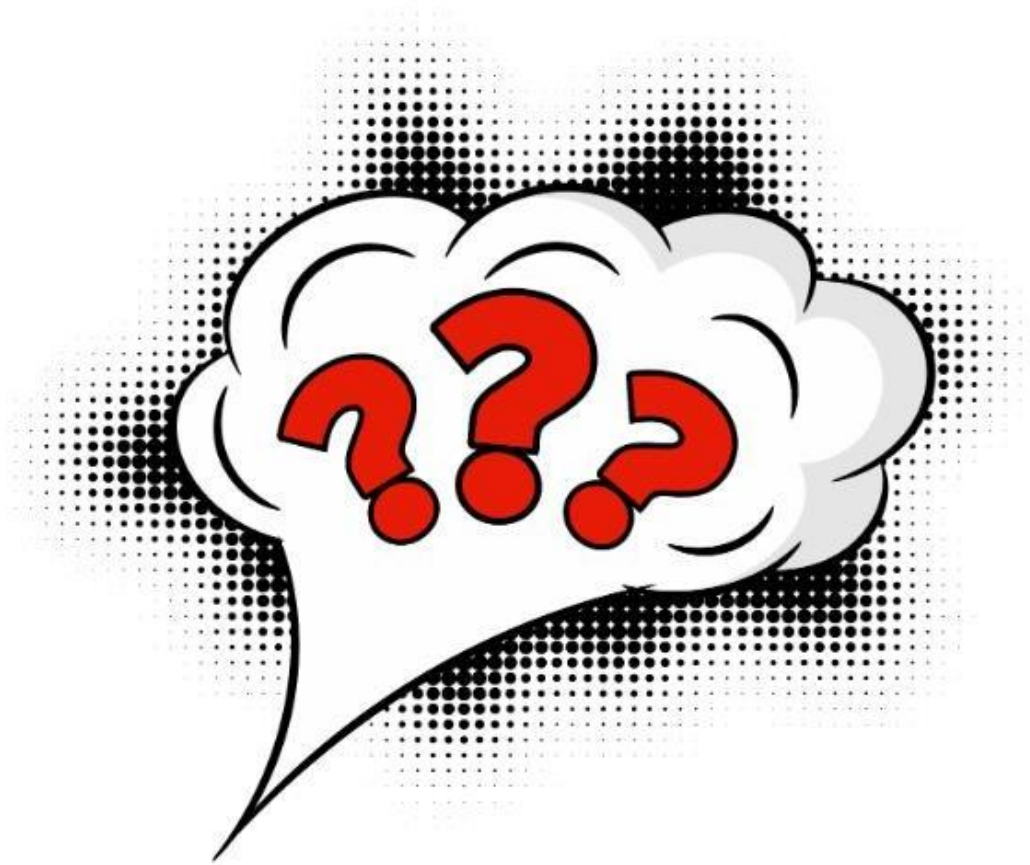
- Something You Can Do;
- Something You Exhibit;
- Someone You Know.

Two-factor/Multifactor Authentication

- Multifactor authentication
  - Combines authentication from two or more factors
- Examples:
  - PIN and CAC
  - PIV and password
  - Fingerprint and smart card

Authentication Log Files

- Authentication log files can track both successful and unsuccessful login attempts;
- It's most important to monitor login activity for any privileged accounts, such as administrators;
- It's common to send entries from authentication logs to a SIEM system for analysis and notification of suspicious events;
- Log entries help administrators determine what happened, when it happened, where it happened, and who or what did it;
- For authentication log entries :
  - ✓ What happened is either a login success or failure;
  - ✓ When it happened is determined by the time and date stamps;
  - ✓ Where it happened is typically an IP address or computer name;
  - ✓ Who or what did it refers to the user account.



Quiz

Assignments

12 Questions
20 minutes

8+ correct – passed
<8 correct – not passed