Multi-factor Authentication

And Access Control Management

Right of Boom

CIS Control 6 - Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

☑	6.1	Establish an Access Granting Process	Users	●	●	●
☑	6.2	Establish an Access Revoking Process	Users	●	●	●
☑	6.3	Require MFA for Externally-Exposed Applications	Users	●	●	●
☑	6.4	Require MFA for Remote Network Access	Users	●	●	●
☑	6.5	Require MFA for Administrative Access	Users	●	●	●
☑	6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Users		●	●
☑	6.7	Centralize Access Control	Users		●	●
☑	6.8	Define and Maintain Role-Based Access Control	Data			●

Password Controls

Password Problems: Password Spraying

- Password Spraying is using the same password across multiple accounts
- <Season><Year> i.e Spring2023
- Requires the attacker to conduct a user harvesting attack first
- Then, the attacker feeds the IDs through a tools like Burp to try all accounts with a single password
- Stay under the account lockout threshold

Time to Compromise

- Depends on the size of the network
- Bread and butter for most attackers
- Remote on a medium (10,000) network, about an hour
    - Spring2021
- Once in, very hard to detect
- Using cloud providers to attack cloud providers
- Credking
- Fireprox

Password Spraying

```
PS C:\Tools> Get-GlobalAddressList -UserName [redacted]\bamas -Password Summer2016 -ExchHostname mail.[redacted].com
[*] First trying to log directly into OWA to enumerate the Global Address List using FindPeople...
[*] Using https://mail.[redacted].com/owa/auth.owa
[*] Logging into OWA...
[*] OWA Login appears to be successful.
[*] Retrieving OWA Canary...
[*] Successfully retrieved the X-OWA-CANARY cookie: wJbH-x__FUWPFP0zTHpKA-mXChUn6dMIAat-1ehtktv99KfRPRQkwSmS2579gJidoFvE
OFTCmX0.
[*] Retrieving AddressListId from GetPeopleFilters URL.
[*] Global Address List Id of 5775714f-98e2-4737-949c-d9a4259fee60 was found.
[*] Now utilizing FindPeople to retrieve Global Address List
[*] Now cleaning up the list...
AndresG@[redacted].com
BamaS@[redacted].com
CaptainV@[redacted].com
CarlT@[redacted].com
itadmin@[redacted].com
vladi@[redacted].com
[*] A total of 6 email addresses were retrieved
PS C:\Tools>
```

Password Problems: Short Passwords

- Back to the NIST Greenbook
- Far too many organizations have password policies that are between 8 and 10 characters
- Sometimes the excuse is that it's OK because they have 2FA
- This only works if all (as in 100%) of authentication APIs and portals have 2FA enabled
- So, it never works

Password Problems: Hidden 2FA Bypass

- An attacker has to find only one portal that does not support 2FA
- Then, all accounts and passwords they have harvested can be used
- OWA and EWS example
- How can you audit all of your authentication points?
- Regular scanning coupled with a regular penitent

Password Problems: Hidden 2FA Bypass

- The only thing that matters with passwords is length
- The. Only. Thing.
- Move to passphrase
- !igraduatedfromwyoming3037101171
  - Don’t use that
- Allow users to use dictionary words
- I also recommend requiring one special character and numbers as well

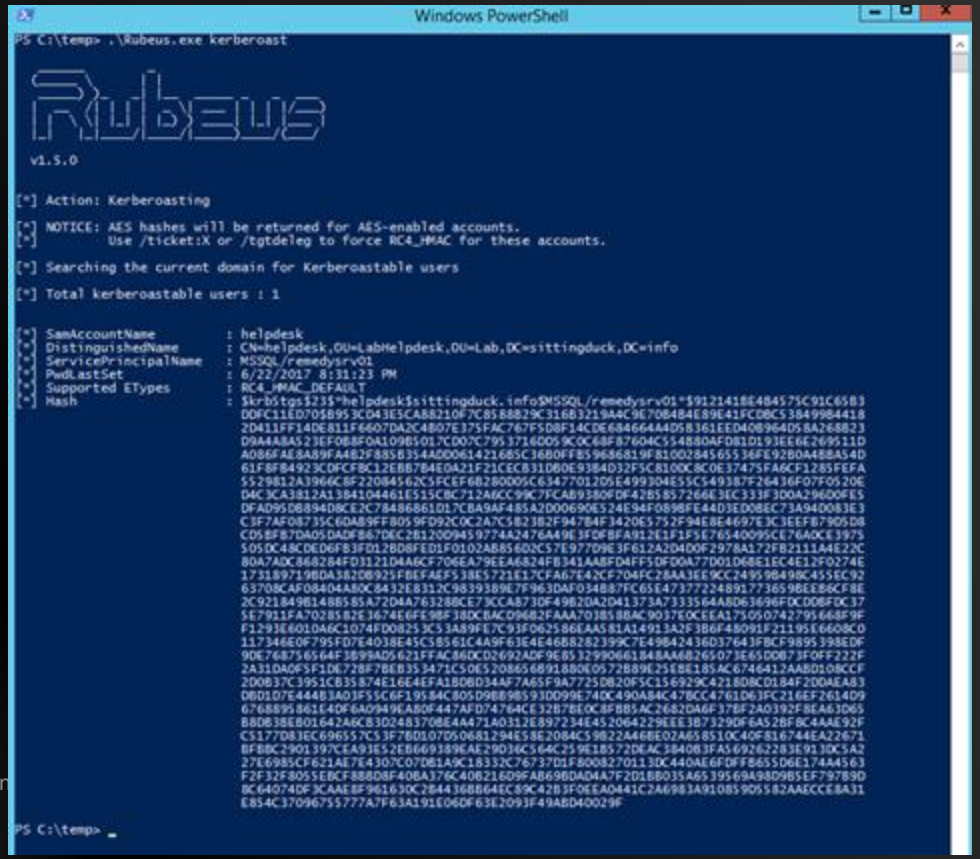
2FA

- Something you know and something you have
- Token based
- SMS Based
- App-based
  - All are better than no 2FA
- How would you attack SMS 2FA
  - Just ask the user to let you in
  - SIM cloning

Service Accounts

- Often forgotten in many environments
- Accounts for services
- Need for no lockout
- Need for never-ending passwords
- Often overlooked by security teams and beloved by attackers everywhere

Kerberoasting



Dedicated Administration System

Right of Boom

Dedicated Administrators

- Never, ever surf with an admin account
- Ever
- Audit Domain Admin accounts
- Look for other over privileged groups as well

Right of Boom

Dedicated Administration

- Common attack, get a sysadmin
- Inconvenience to administrators to change accounts
- Attackers say "Thanks!"
- Internal password spraying for more accounts

Right of Boom

Dedicated Administrators - Jump Hosts

- This does a couple things
- Reduction in attack path
- Enhanced alerting opportunities
- If someone attempts to access an admin account anywhere else, alert and react
- It is also a good idea to restrict access to admin accounts from a dedicated terminal server

Right of Boom

Secure Account Management

Right of Boom

CIS Control 5 - Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

☑	5.1	Establish and Maintain an Inventory of Accounts	Users	●	●	●
☑	5.2	Use Unique Passwords	Users	●	●	●
☑	5.3	Disable Dormant Accounts	Users	●	●	●
☑	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Users	●	●	●
☑	5.5	Establish and Maintain an Inventory of Service Accounts	Users		●	●
☑	5.6	Centralize Account Management	Users		●	●

Right of Boom

Privileged Access Management

Right of Boom

Network Level Authentication

Right of Boom

Network Access Control

- Authentication of the user and the device
  - MAC Address, Certificates, UA Strings, monitoring Kerberos authentication
  - Some claim to be "behavioral"
- Possible quarantine capabilities
  - Quick isolation, possible fake network emulation
- BYOD stopping?
  - We can hope…
- Incident Response
- The single biggest thing…. Isolation

Right of Boom

Network Access Control Bypasses

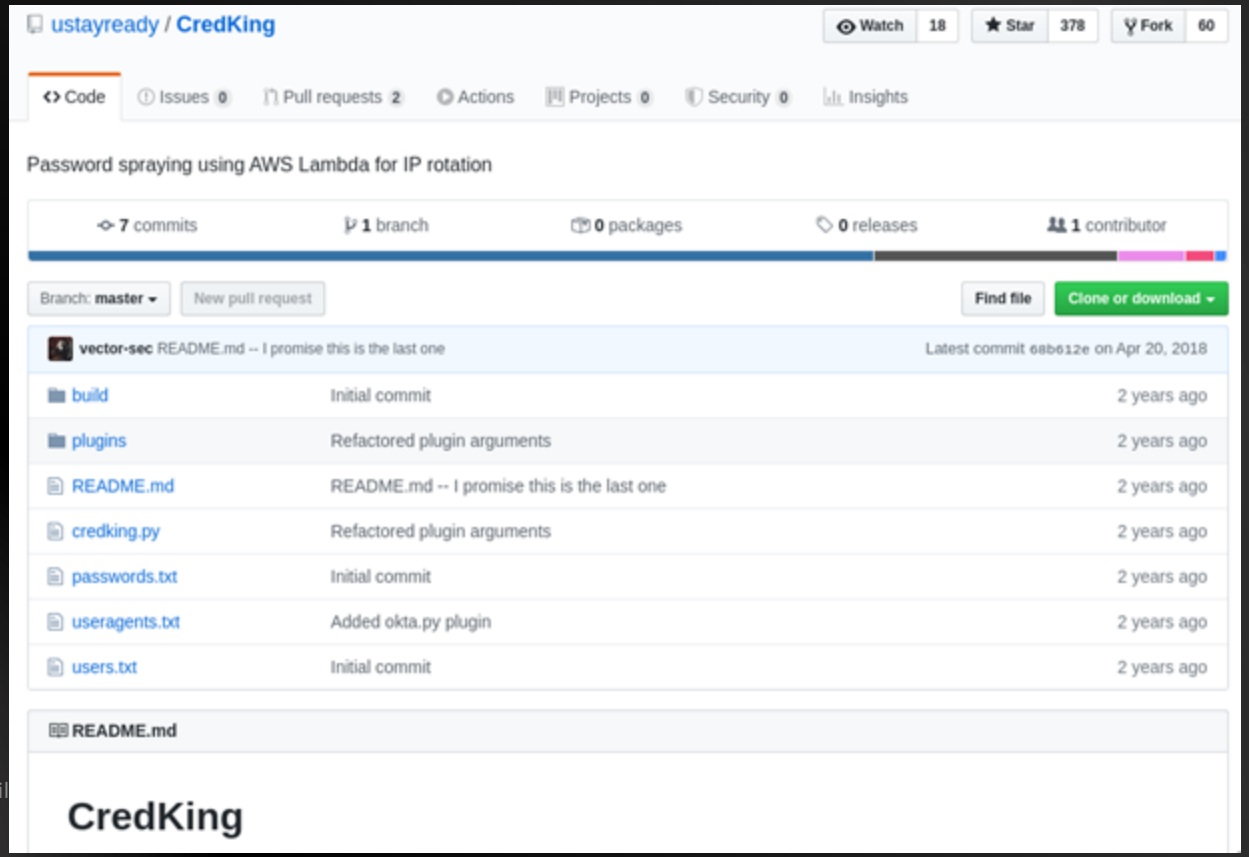
- Focus on mimmicking authenticated devices
- Finding non-protected VLANs
  - VLAN hopping
- Layer 2 attacks
  - SCTP, Spanning Tree, HSRP, etc.
- Silent Bridge
  - GitHub - s0lst1c3/silentbridge: Silentbridge is a toolkit for bypassing 802.1x-2010 and 802.1x-2004.

Right of Boom

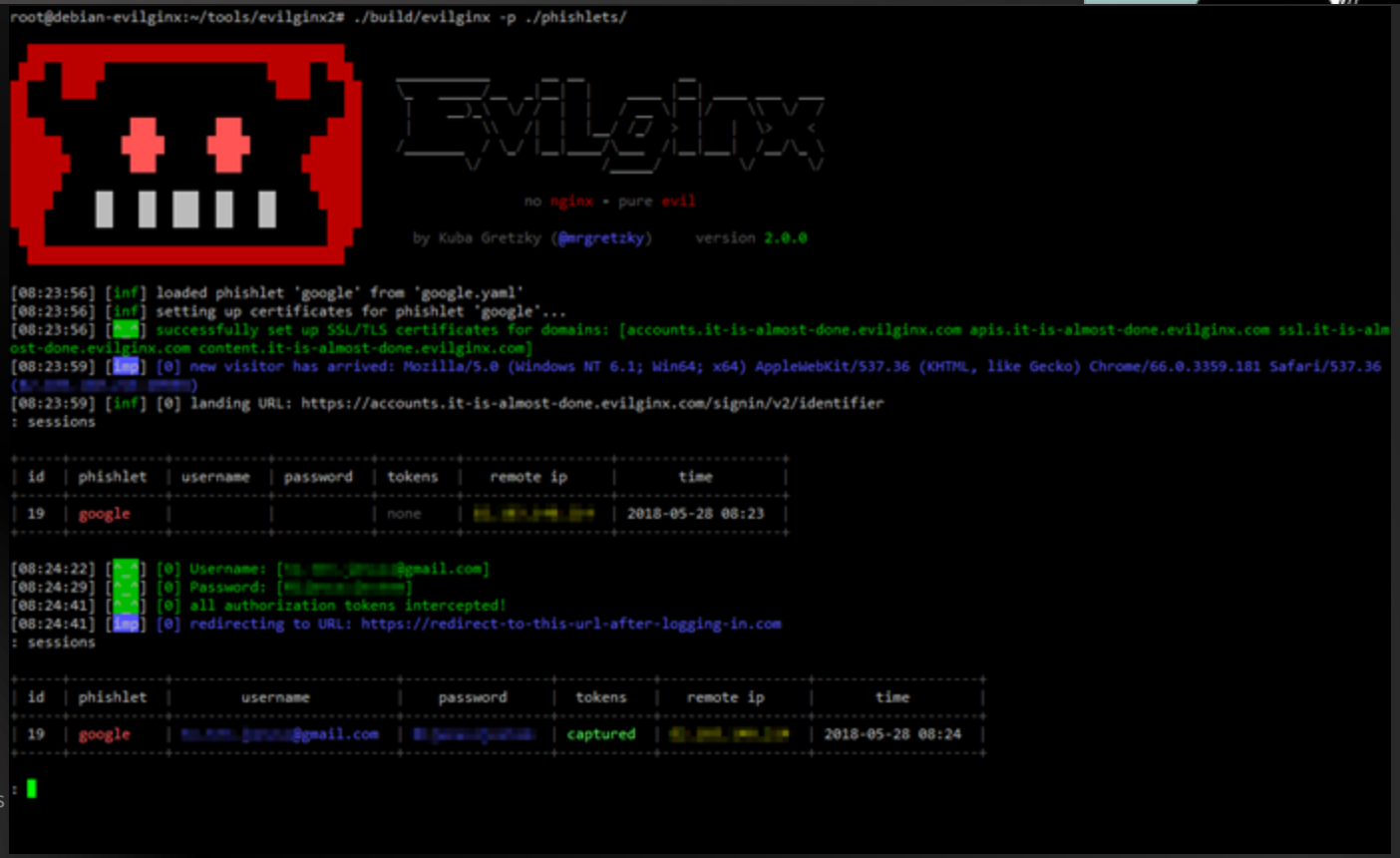
LLMNR/MDNS/NBNS

```
root@DESKTOP-I1T2G01:/opt/Responder# ./Responder.py -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
```

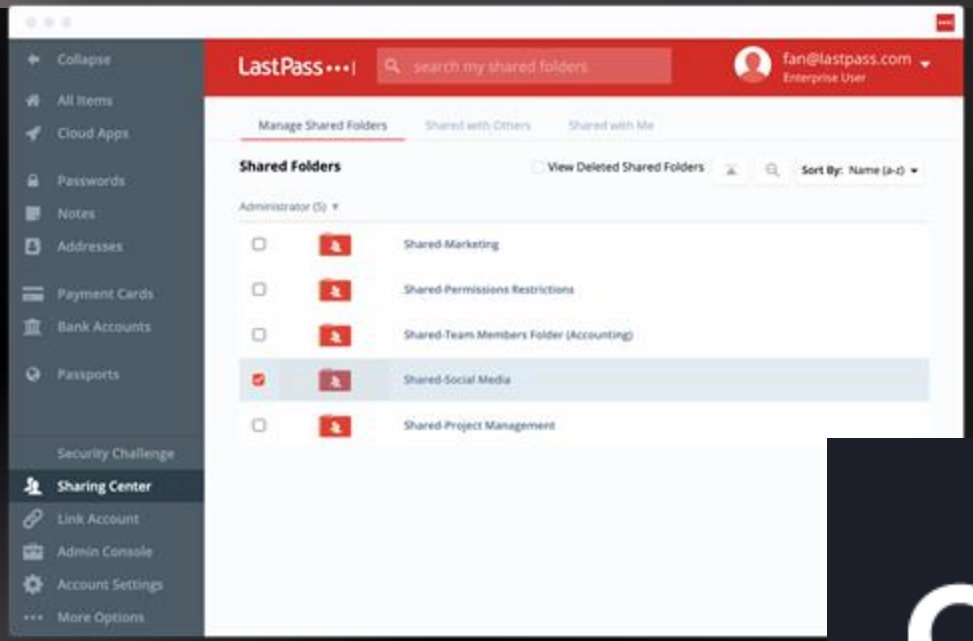
Credking



Bypassing 2FA: Evilginx



Password Managers



onelogin

Privileged Identity Management

BeyondTrust

CYBERARK

Centrify

MICROSOFT LOCAL ADMINISTRATOR PASSWORD SOLUTION