PEN Consultants

Information & Cybersecurity Testing Services

www.penconsultants.com

Experienced. Trustworthy. Transparent.

Rock Solid Security

Premier cybersecurity testing services tailored to your specific needs from experts you can trust.

Discover your vulnerabilities before an attacker does. We can help!

Breaching a Network
With Risk-Accepted Vulnerabilities

TEEX Cyber Readiness Summit

Robert Neel
PEN Consultants, LLC

Agenda

- About Me & PEN Consultants
- Objective
- Overview of the Attack
- Attack Chain
- Step-by-Step Walkthrough
- Real-World Examples
- Actionable Solutions
- Conclusion
- Questions

Robert Neel

- Founder & CEO of PEN Consultants
- NSA trained
- Over 25 years experience

LOCKHEED MARTIN

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

USAA®

PEN Consultants

PEN Consultants provides comprehensive offensive security services - including vulnerability scanning, penetration testing, red teaming, and more.

Objective

Objective #1

Show how a series of common vulnerabilities can be used in an attack that succeeds nearly every time

Objective #2

Provide you with the information needed to prevent the attack

Overview of the Attack

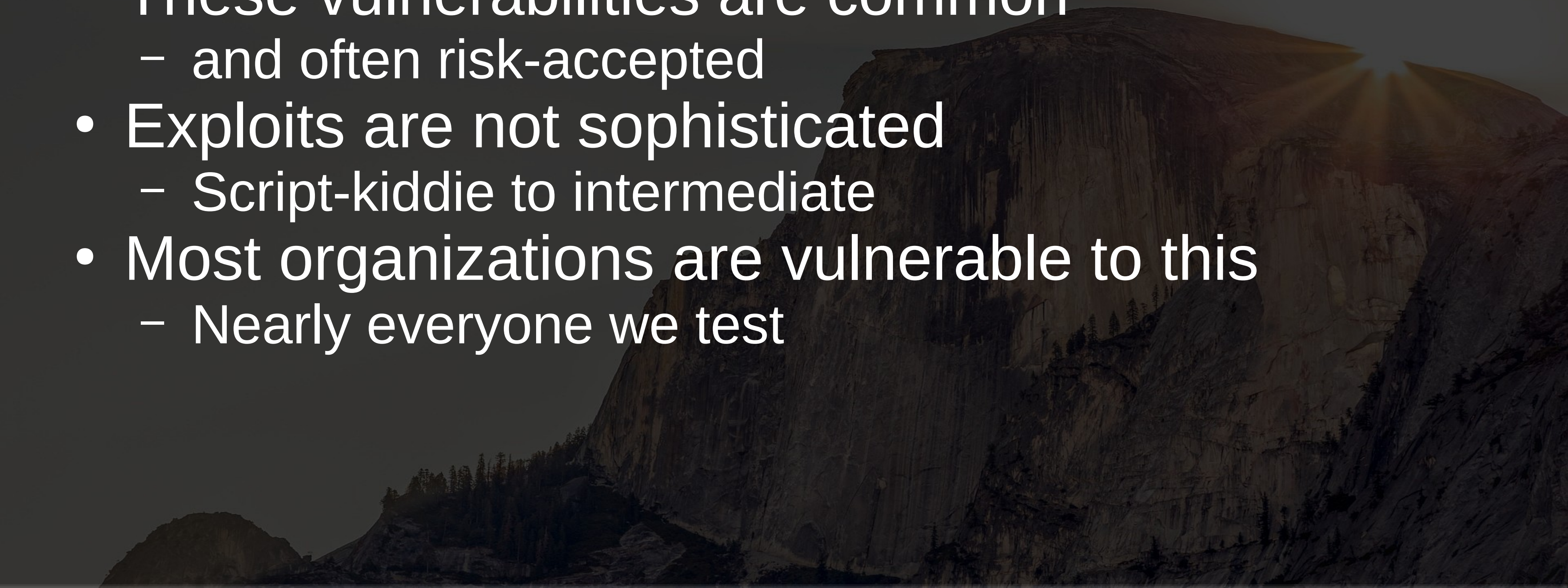
Attack Timeline

- Start with knowing nothing
- Get remote access into a corporate network
- Find & export data

Attack Chain Demo

- Single step through each phase of an attack
- Real Examples - present right now
- Actionable Solutions - what you can do to stop it

Overview of the Attack



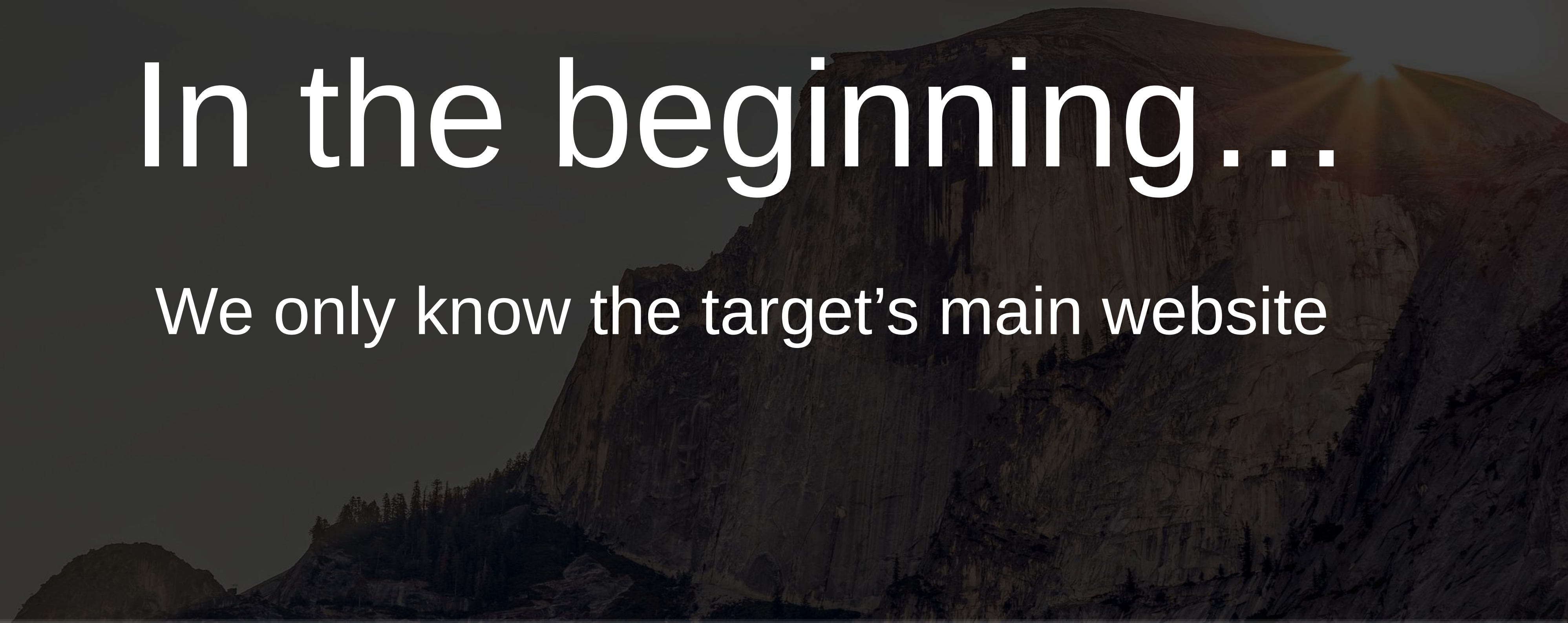
Key Points:

- These vulnerabilities are common
  - and often risk-accepted
- Exploits are not sophisticated
  - Script-kiddie to intermediate
- Most organizations are vulnerable to this
  - Nearly everyone we test

Overview of the Attack

Examples Shown:

- These are real, live, current examples (within the last few weeks)
- A reasonable level of effort was used to anonymize and obfuscate

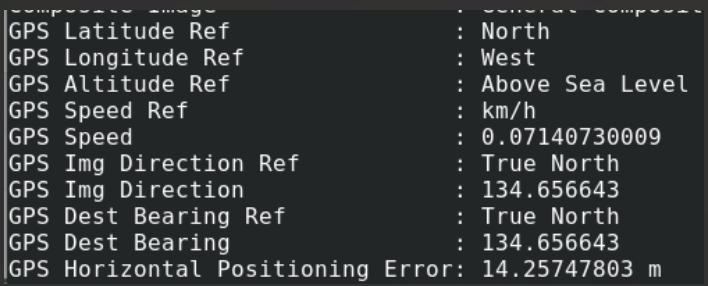


In the beginning…

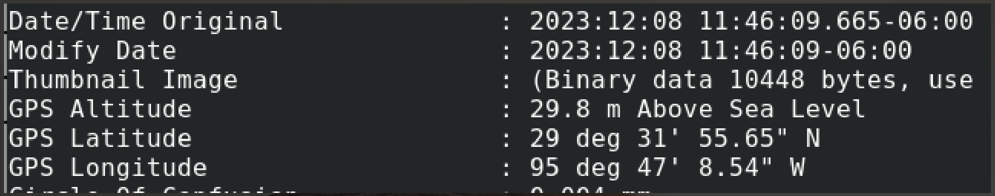
We only know the target’s main website

Document Metadata

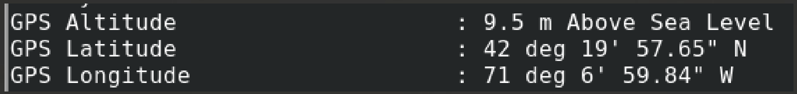
Document Metadata



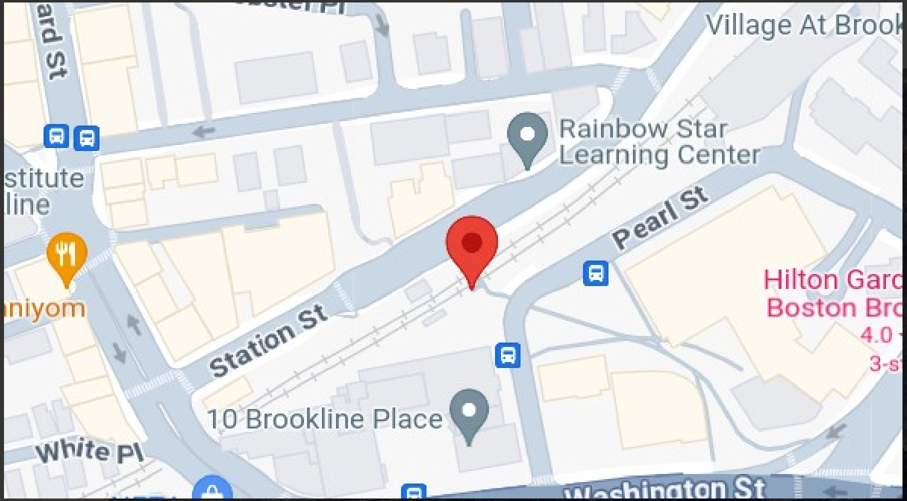
```
GPS Latitude Ref                : North
GPS Longitude Ref               : West
GPS Altitude Ref                : Above Sea Level
GPS Speed Ref                   : km/h
GPS Speed                       : 0.07140730009
GPS Img Direction Ref           : True North
GPS Img Direction               : 134.656643
GPS Dest Bearing Ref            : True North
GPS Dest Bearing                : 134.656643
GPS Horizontal Positioning Error: 14.25747803 m
```

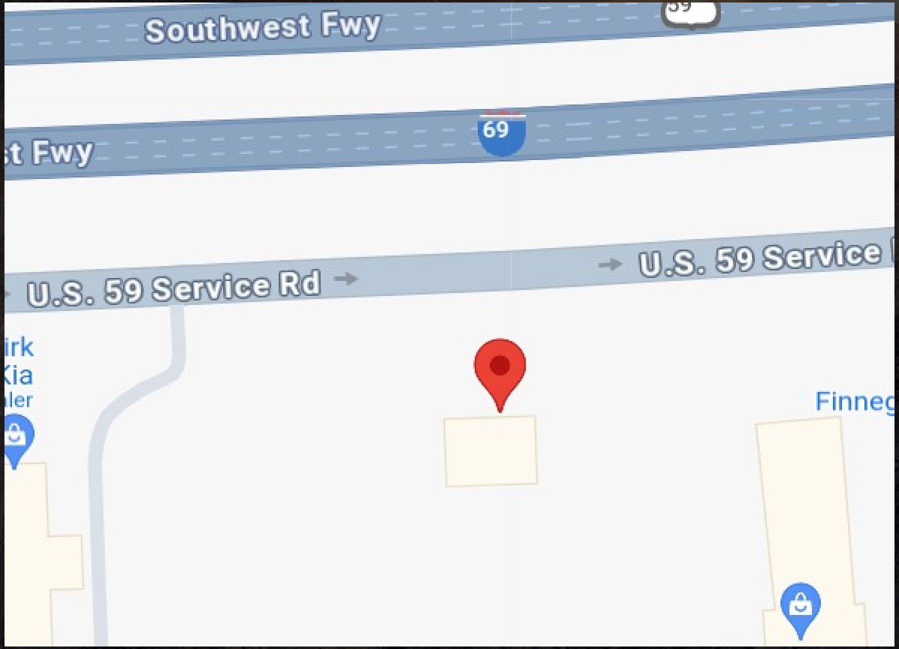


```
Date/Time Original              : 2023:12:08 11:46:09.665-06:00
Modify Date                     : 2023:12:08 11:46:09-06:00
Thumbnail Image                 : (Binary data 10448 bytes, use
GPS Altitude                    : 29.8 m Above Sea Level
GPS Latitude                    : 29 deg 31' 55.65" N
GPS Longitude                   : 95 deg 47' 8.54" W
```

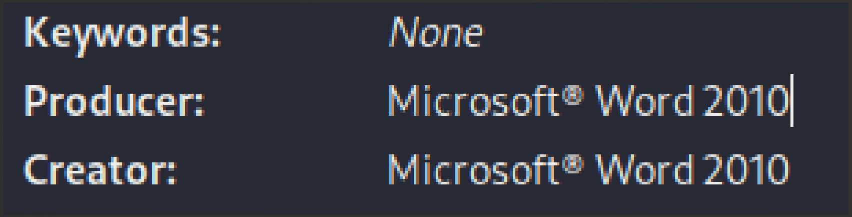


```
GPS Altitude                    : 9.5 m Above Sea Level
GPS Latitude                    : 42 deg 19' 57.65" N
GPS Longitude                   : 71 deg 6' 59.84" W
```

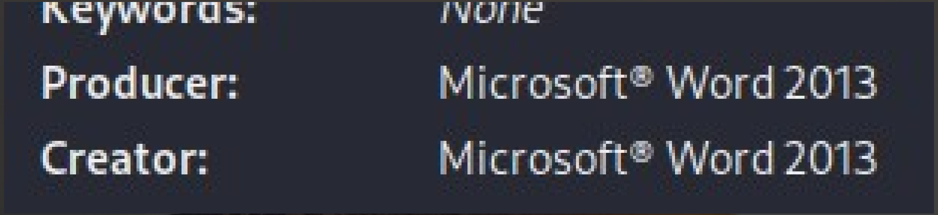




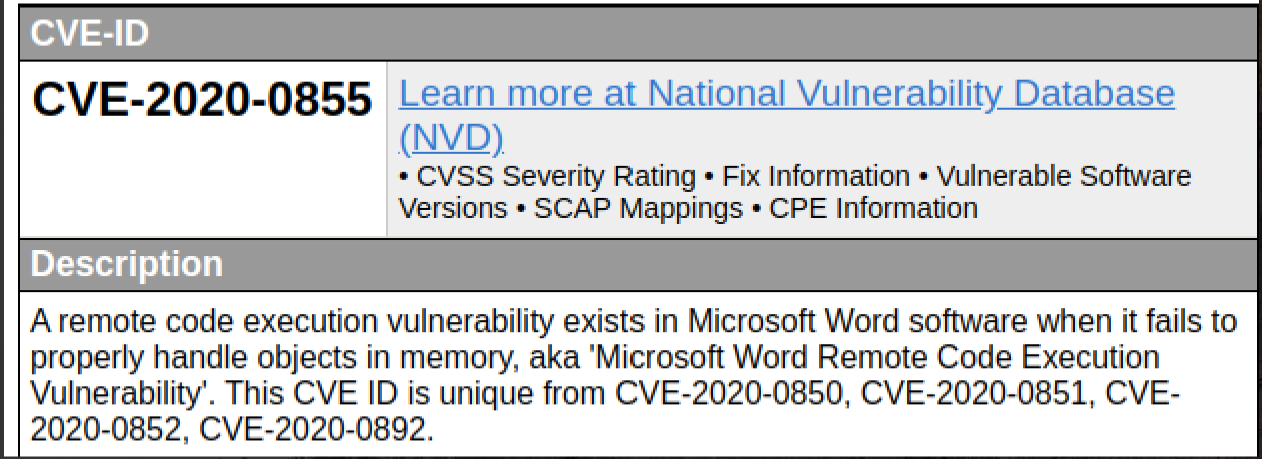
Document Metadata



Keywords:	*None*
Producer:	Microsoft® Word 2010
Creator:	Microsoft® Word 2010



Keywords:	*None*
Producer:	Microsoft® Word 2013
Creator:	Microsoft® Word 2013

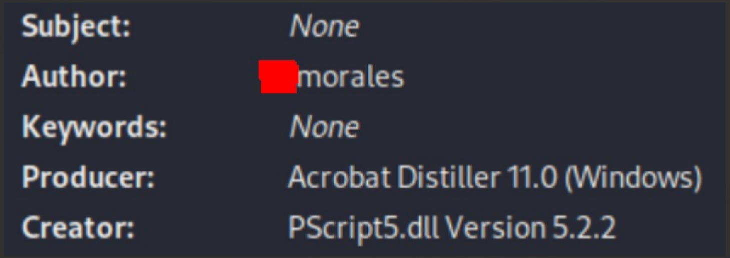


CVE-ID	
CVE-2020-0855	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

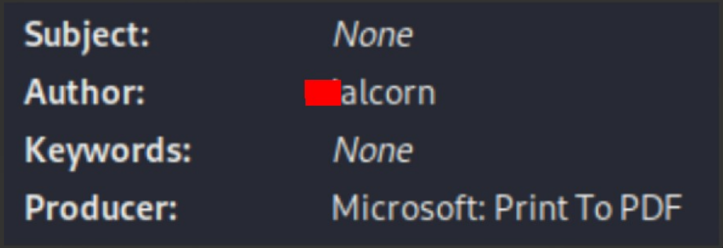
Description

A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0850, CVE-2020-0851, CVE-2020-0852, CVE-2020-0892.

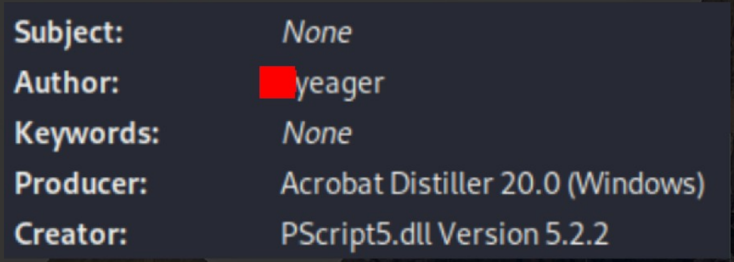
Document Metadata



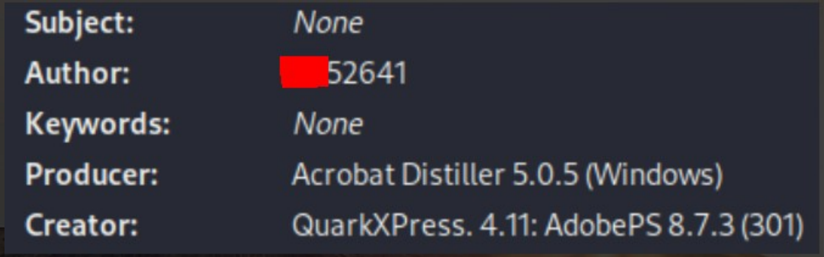
```
Subject:      None
Author:       [redacted]morales
Keywords:     None
Producer:     Acrobat Distiller 11.0 (Windows)
Creator:      PScript5.dll Version 5.2.2
```



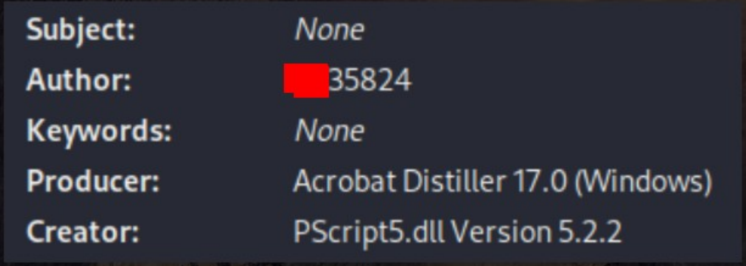
```
Subject:      None
Author:       [redacted]alcorn
Keywords:     None
Producer:     Microsoft: Print To PDF
```



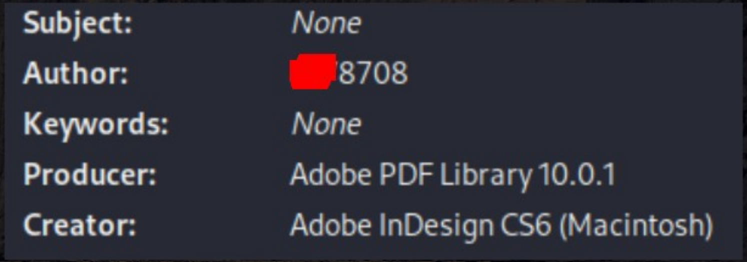
```
Subject:      None
Author:       [redacted]yeager
Keywords:     None
Producer:     Acrobat Distiller 20.0 (Windows)
Creator:      PScript5.dll Version 5.2.2
```



```
Subject:      None
Author:       [redacted]52641
Keywords:     None
Producer:     Acrobat Distiller 5.0.5 (Windows)
Creator:      QuarkXPress. 4.11: AdobePS 8.7.3 (301)
```



```
Subject:      None
Author:       [redacted]35824
Keywords:     None
Producer:     Acrobat Distiller 17.0 (Windows)
Creator:      PScript5.dll Version 5.2.2
```



```
Subject:      None
Author:       [redacted]8708
Keywords:     None
Producer:     Adobe PDF Library 10.0.1
Creator:      Adobe InDesign CS6 (Macintosh)
```

Document Metadata

Blue Team / Defenders

- Disable metadata from docs
  - ex. Group Policy Object (GPO)
- Scrub metadata from docs
  - many prepub/scrubber solutions
- Update ALL vulnerabilities
  - internal vulnerabilities lead to RCE also!

Username Format

Username Format

- Re: Usernames from document metadata
- Username format
  - Often same as name or email address
    - John Doe > john.doe@acme.com > john.doe
  - Second most common, easily derived from name or email address
    - JDoe, JohnD, JADoe, etc.
- Importance to attacker:
  - a small list they can immediately attack
  - able to determine domain username convention
  - used to derive a larger list for a broader attack
- Attacks possible (just a few examples)
  - Phishing
  - DoS attacks - if you have a lockout policy
  - Password attacks - ex. password spray
  - More on these later

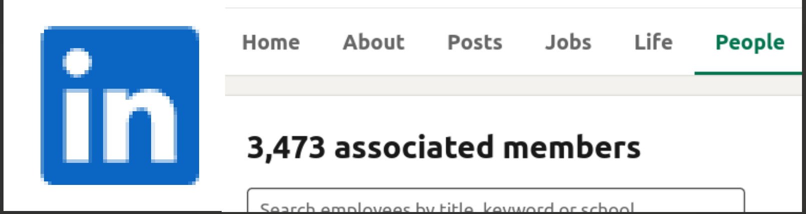
Username Format

Blue Team / Defenders

- Username convention NOT:
  - based on name or email address
  - sequential
- Should not be easily predicable
  - an employee number - ex. cf213692132
  - a predictable prefix with random numbers - ex. jdoe_92613

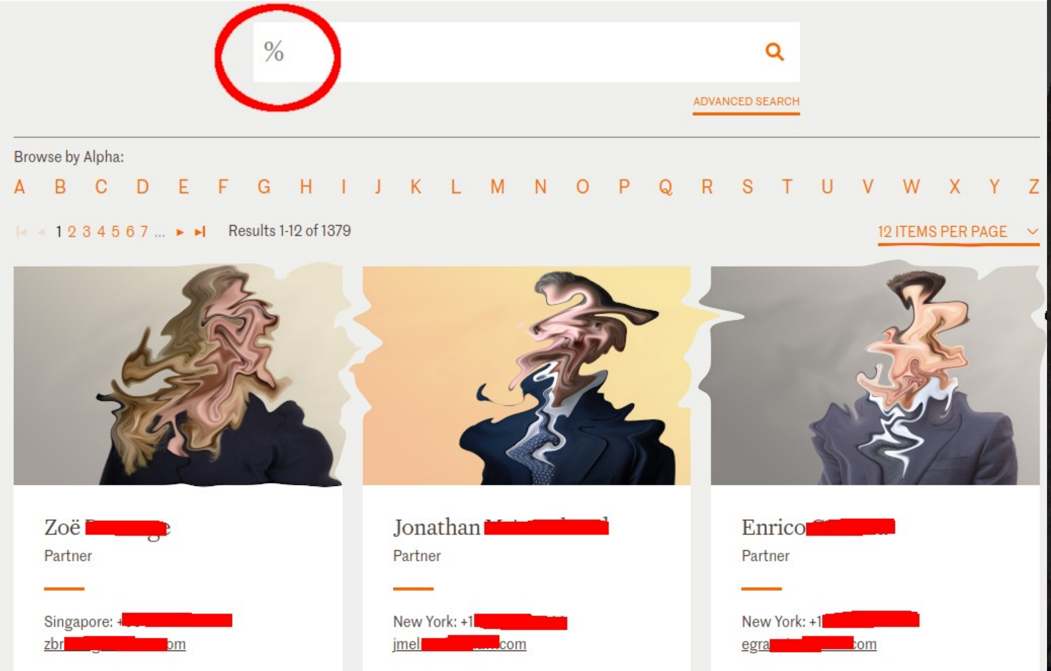
Candidate Username List

Candidate Username List



3,473 associated members

Search employees by title, keyword or school



%

Browse by Alpha:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

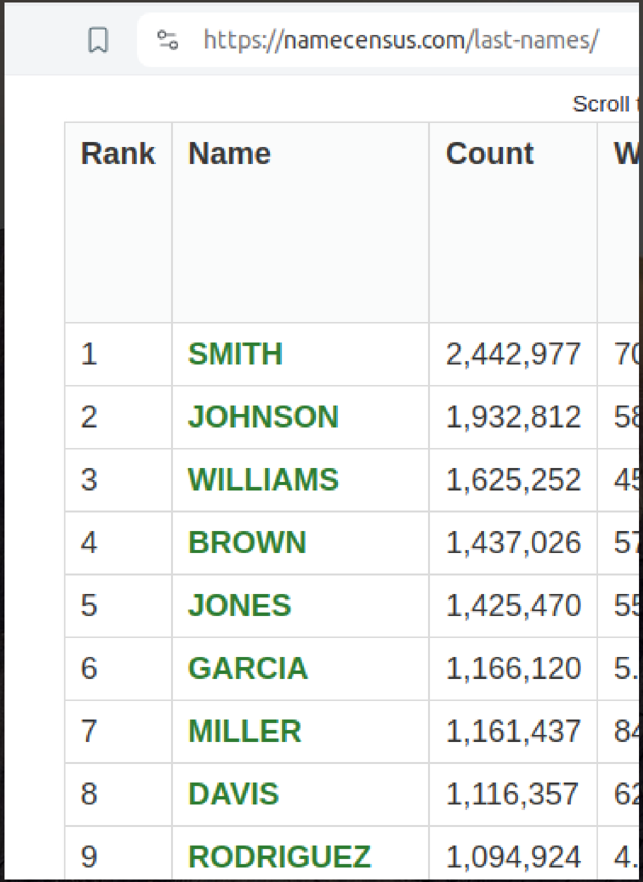
1 2 3 4 5 6 7 ... Results 1-12 of 1379

12 ITEMS PER PAGE

Zoë [redacted]
Partner
Singapore: +[redacted]
zbr[redacted]om

Jonathan [redacted]
Partner
New York: +1[redacted]
jmel[redacted]com

Enrico [redacted]
Partner
New York: +1[redacted]
egra[redacted]com



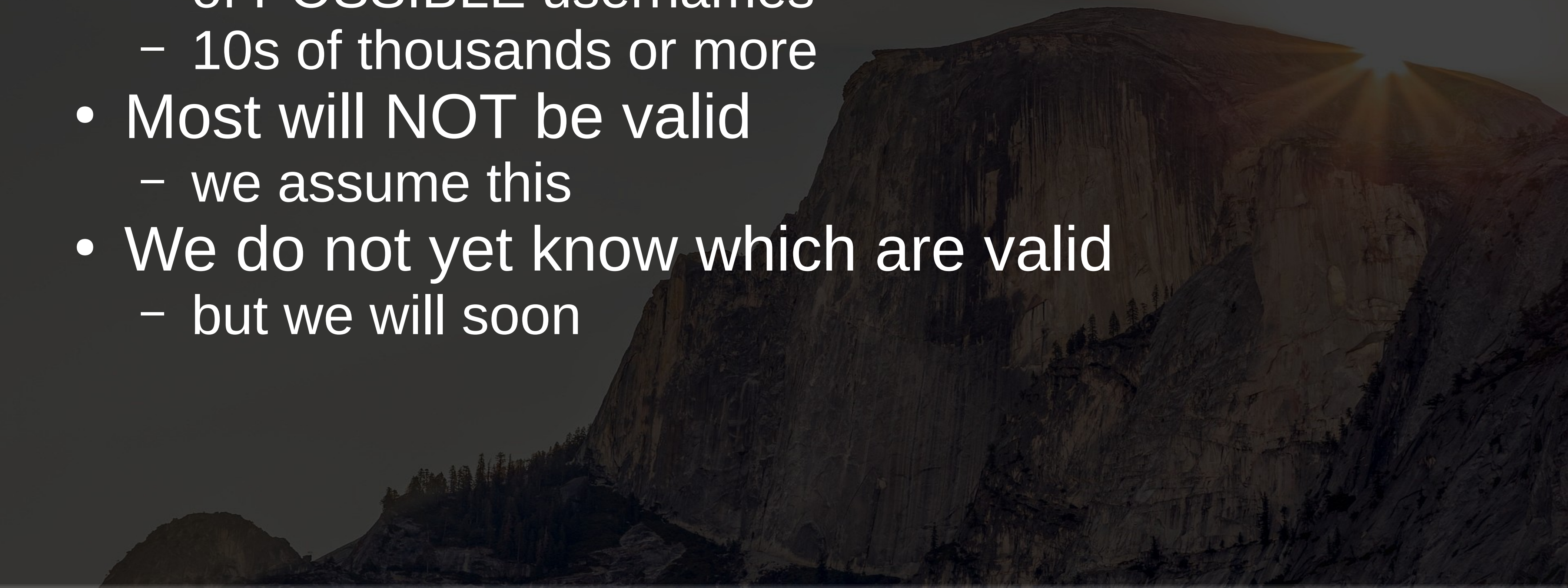
https://namecensus.com/last-names/

Scroll

Rank	Name	Count	W
1	SMITH	2,442,977	70
2	JOHNSON	1,932,812	58
3	WILLIAMS	1,625,252	45
4	BROWN	1,437,026	57
5	JONES	1,425,470	55
6	GARCIA	1,166,120	5.
7	MILLER	1,161,437	84
8	DAVIS	1,116,357	62
9	RODRIGUEZ	1,094,924	4.

Candidate Username List

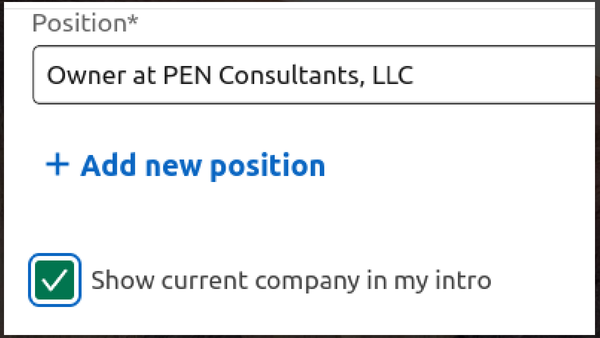
- Generate a list:
  - of POSSIBLE usernames
  - 10s of thousands or more
- Most will NOT be valid
  - we assume this
- We do not yet know which are valid
  - but we will soon



Candidate Username List

Blue Team / Defenders

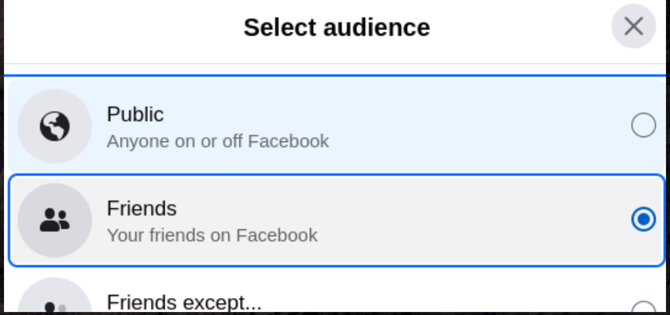
- Limit the usage of online directories
  - Place behind login, if able
  - Minimize who is listed
  - Minimize what is listed for each
  - Prevent wildcard searches
- User training
  - Hide current company on social media
  - Vet connection requests



Position*

Owner at PEN Consultants, LLC

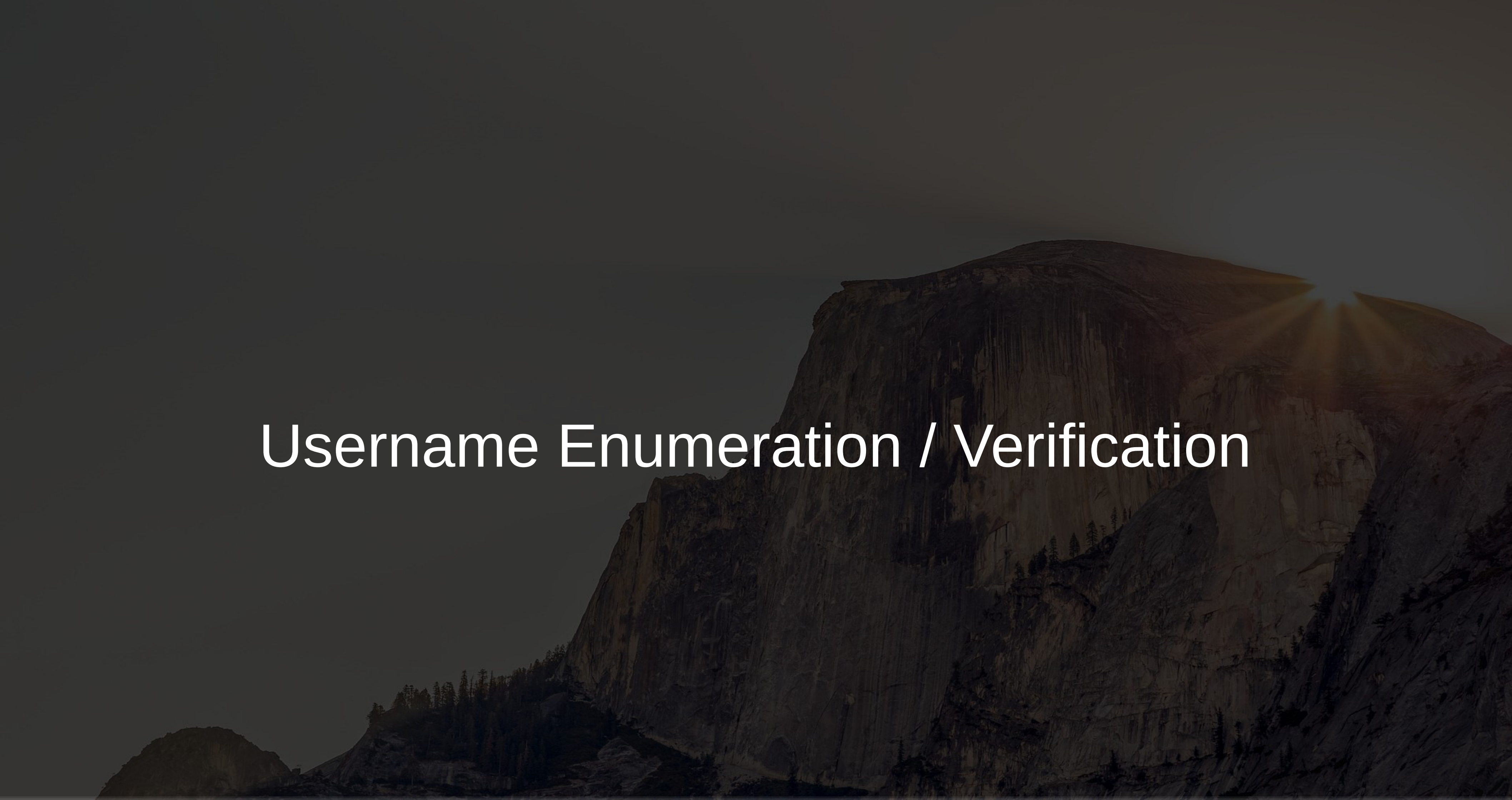
☑ Show current company in my intro



Public
Anyone on or off Facebook ○

Friends
Your friends on Facebook ●

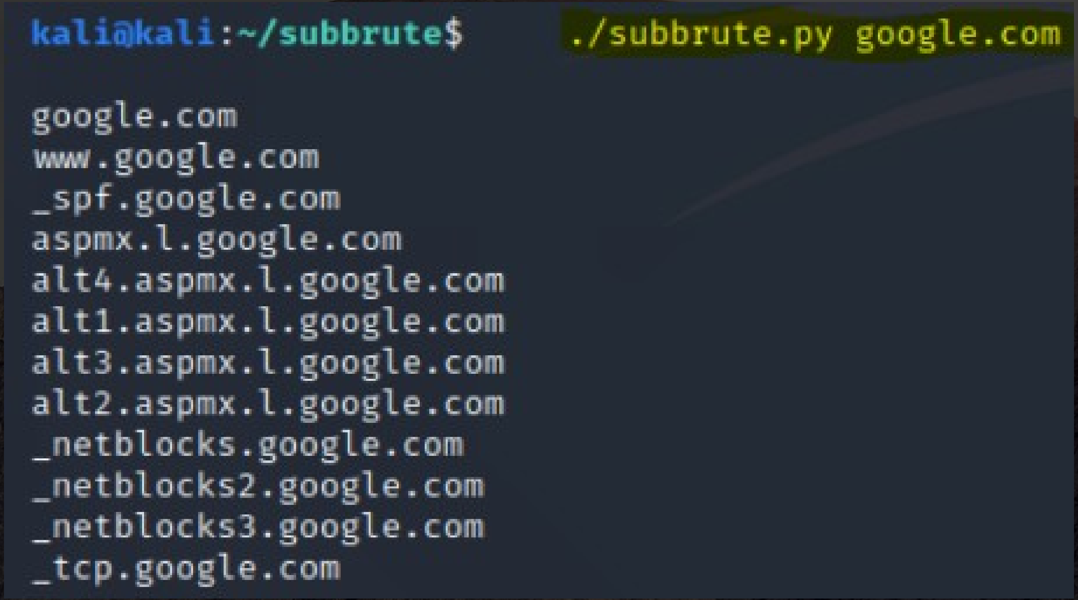
Friends except... ○



Username Enumeration / Verification

Username Enumeration / Verification

- Fully Qualified Domain Names (FQDNs)
  - OSINT
  - Brute force
  - Public Certificate Transparency (CT) records

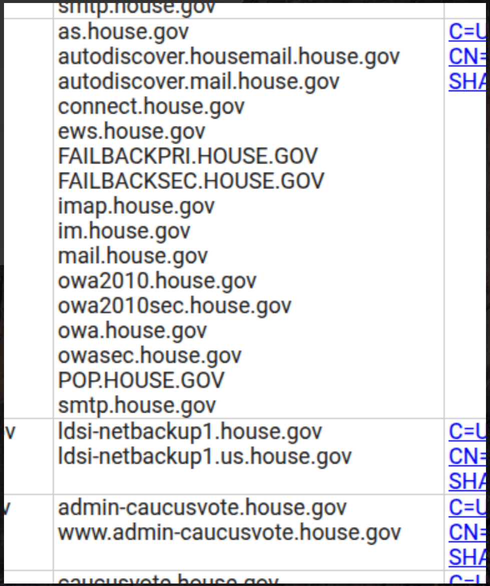


```
kali@kali:~/subbrute$    ./subbrute.py google.com

google.com
www.google.com
_spf.google.com
aspmx.l.google.com
alt4.aspmx.l.google.com
alt1.aspmx.l.google.com
alt3.aspmx.l.google.com
alt2.aspmx.l.google.com
_netblocks.google.com
_netblocks2.google.com
_netblocks3.google.com
_tcp.google.com
```

Username Enumeration / Verification

- Certificate registrations
  - Each FQDN often has its own SSL cert
    - Don’t do this ^^^
  - Search CT records
  - Collect FQDNs

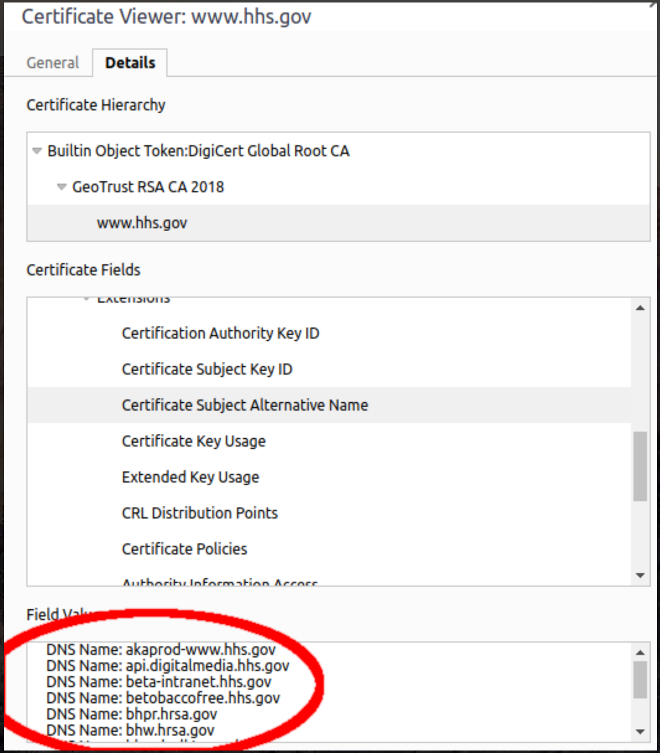


smtp.house.gov
as.house.gov
autodiscover.housemail.house.gov
autodiscover.mail.house.gov
connect.house.gov
ews.house.gov
FAILBACKPRI.HOUSE.GOV
FAILBACKSEC.HOUSE.GOV
imap.house.gov
im.house.gov
mail.house.gov
owa2010.house.gov
owa2010sec.house.gov
owa.house.gov
owasec.house.gov
POP.HOUSE.GOV
smtp.house.gov
C=U
CN=
SHA

ldsi-netbackup1.house.gov
ldsi-netbackup1.us.house.gov
C=U
CN=
SHA

admin-caucusvote.house.gov
www.admin-caucusvote.house.gov
C=U
CN=
SHA

caucusvote.house.gov



Certificate Viewer: www.hhs.gov

Certificate Hierarchy

- Builtin Object Token:DigiCert Global Root CA
  - GeoTrust RSA CA 2018
    - www.hhs.gov

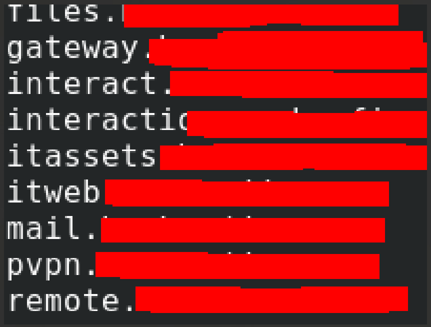
Certificate Fields

Extensions
- Certification Authority Key ID
- Certificate Subject Key ID
- Certificate Subject Alternative Name
- Certificate Key Usage
- Extended Key Usage
- CRL Distribution Points
- Certificate Policies
- Authority Information Access

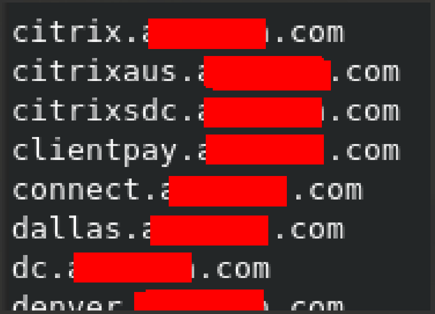
Field Value

DNS Name: akaprod-www.hhs.gov
DNS Name: api.digitalmedia.hhs.gov
DNS Name: beta-intranet.hhs.gov
DNS Name: betobaccofree.hhs.gov
DNS Name: bhpr.hrsa.gov
DNS Name: bhw.hrsa.gov

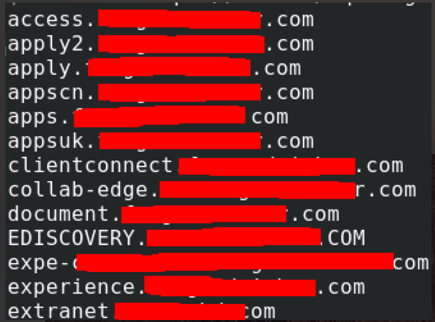
Username Enumeration / Verification



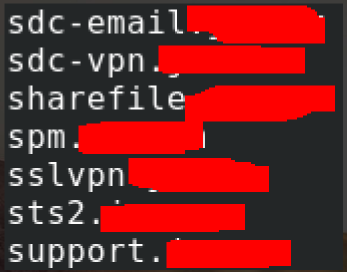
```
files.[redacted]
gateway.[redacted]
interact.[redacted]
interacti[redacted]
itassets[redacted]
itweb[redacted]
mail.[redacted]
pvpn.[redacted]
remote.[redacted]
```



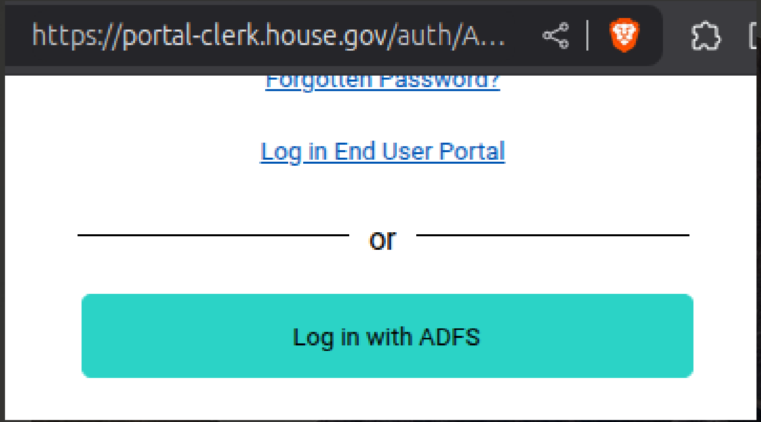
```
citrix.[redacted].com
citrixaus.[redacted].com
citrixsdc.[redacted].com
clientpay.[redacted].com
connect.[redacted].com
dallas.[redacted].com
dc.[redacted].com
denver[redacted].com
```



```
access.[redacted].com
apply2.[redacted].com
apply.[redacted].com
appscn.[redacted].com
apps.[redacted] com
appsuk.[redacted].com
clientconnect [redacted].com
collab-edge.[redacted].com
document.[redacted].com
EDISCOVERY.[redacted].COM
expe-[redacted]com
experience.[redacted].com
extranet [redacted]com
```



```
sdc-email[redacted]
sdc-vpn.[redacted]
sharefile[redacted]
spm.[redacted]
sslvpn[redacted]
sts2.[redacted]
support.[redacted]
```



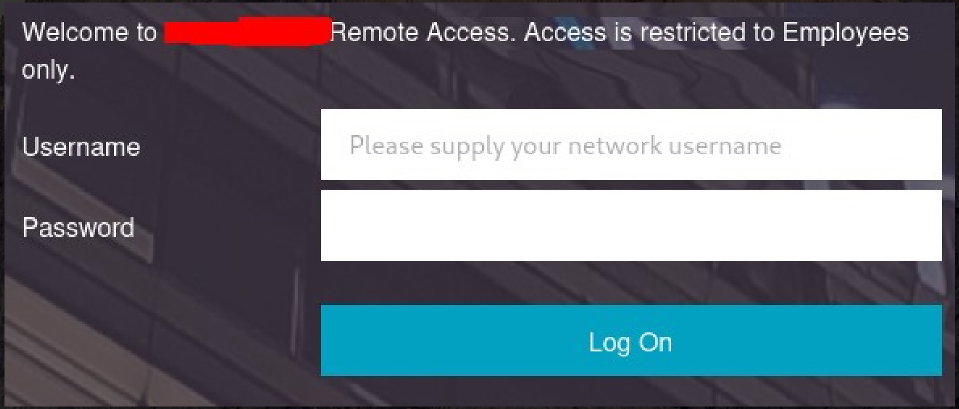
https://portal-clerk.house.gov/auth/A...

Forgotten Password?

Log in End User Portal

or

Log in with ADFS



Welcome to [redacted] Remote Access. Access is restricted to Employees only.

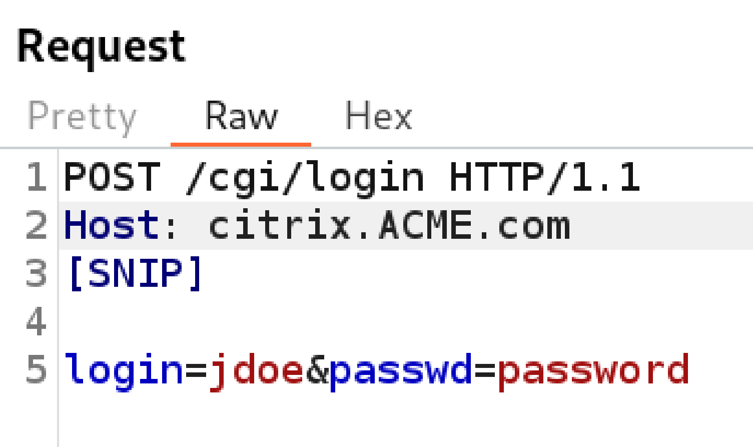
Username: Please supply your network username

Password:

Log On

Username Enumeration / Verification

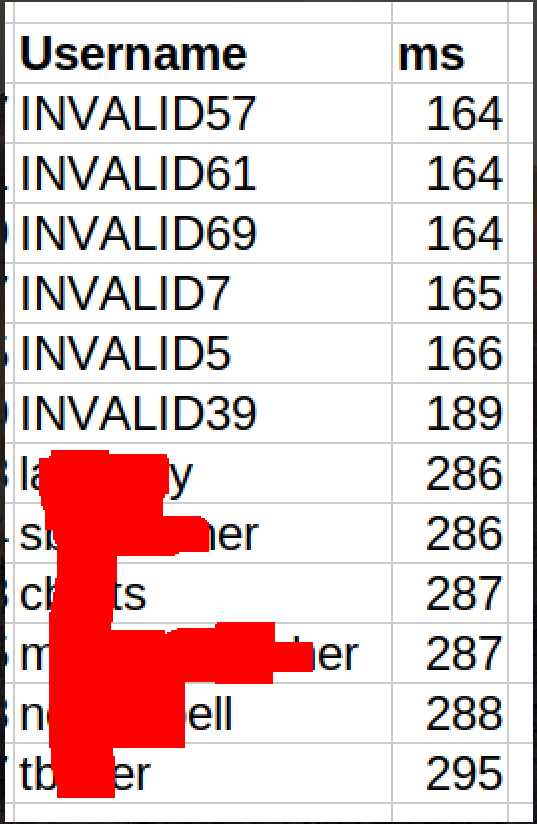
- Attempt a login with each candidate username
- Look for difference in:
  - response status/text/size
  - timing (very common)



Request

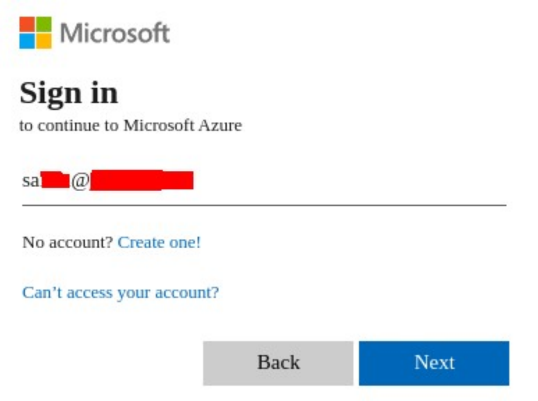
```
POST /cgi/login HTTP/1.1
Host: citrix.ACME.com
[SNIP]

login=jdoe&passwd=password
```



Username	ms
INVALID57	164
INVALID61	164
INVALID69	164
INVALID7	165
INVALID5	166
INVALID39	189
[redacted]	286
[redacted]	286
[redacted]	287
[redacted]	287
[redacted]	288
[redacted]	295

Username Enumeration / Verification



Sign in

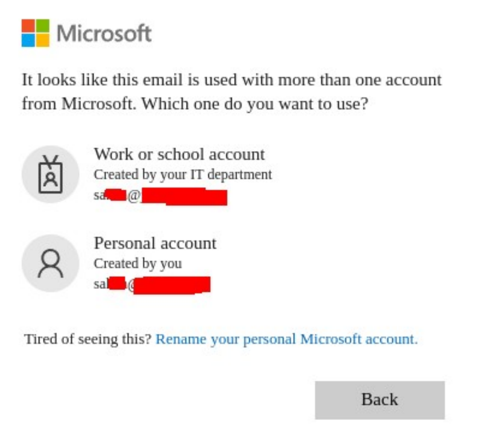
to continue to Microsoft Azure

sa[redacted]@[redacted]

No account? Create one!

Can’t access your account?

VALID

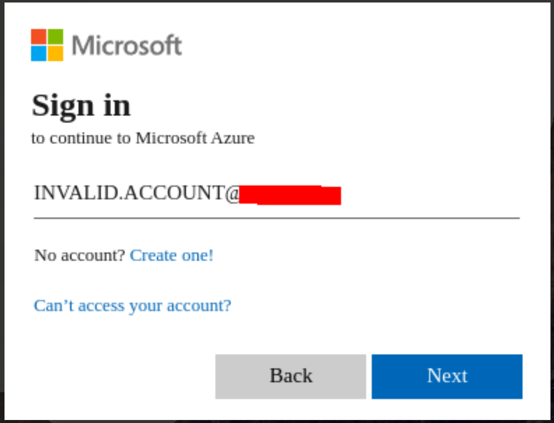


It looks like this email is used with more than one account from Microsoft. Which one do you want to use?

Work or school account
Created by your IT department
sa[redacted]@[redacted]

Personal account
Created by you
sa[redacted]@[redacted]

Tired of seeing this? Rename your personal Microsoft account.



Sign in

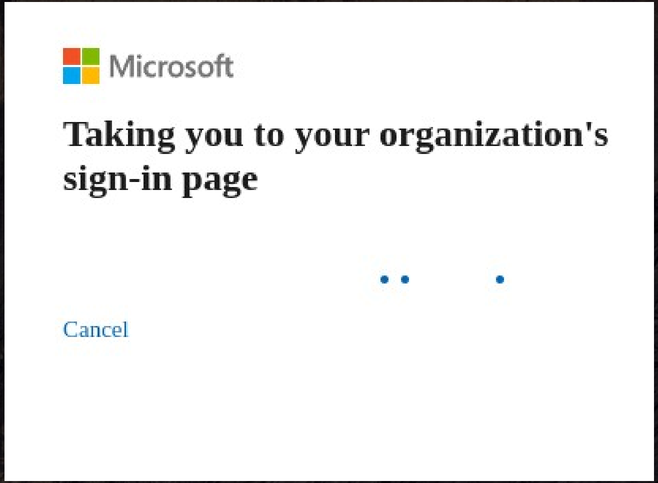
to continue to Microsoft Azure

INVALID.ACCOUNT@[redacted]

No account? Create one!

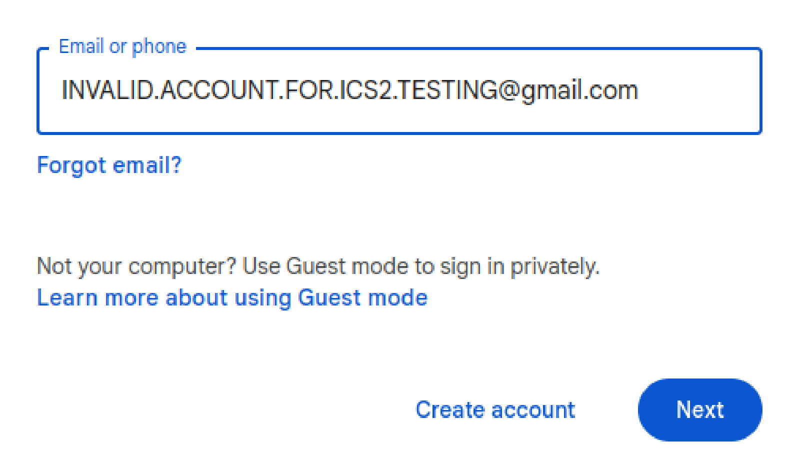
Can’t access your account?

INVALID



Taking you to your organization's sign-in page

Username Enumeration / Verification

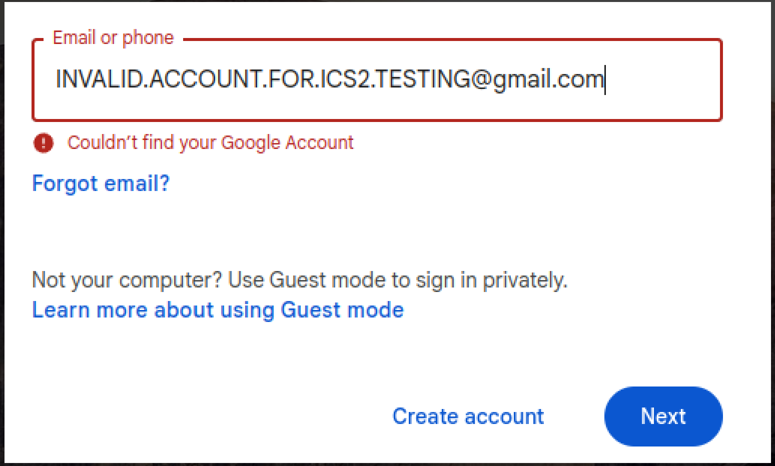


Email or phone: INVALID.ACCOUNT.FOR.ICS2.TESTING@gmail.com

Forgot email?

Not your computer? Use Guest mode to sign in privately.
Learn more about using Guest mode

INVALID



Email or phone: INVALID.ACCOUNT.FOR.ICS2.TESTING@gmail.com

Couldn’t find your Google Account

Forgot email?

Not your computer? Use Guest mode to sign in privately.
Learn more about using Guest mode

Username Enumeration / Verification

We now have:

- A list of known valid usernames
  - 100% valid
- Potentially a list of ALL usernames
- Information needed for various attacks
  - DoS
    - assuming there is a lockout policy
    - we launch an external attack that disrupts your internal operations!
  - Password attacks
    - ex. brute force, password spray, etc.
    - illustration up next

Username Enumeration / Verification

Blue Team / Defenders

- Wildcarded domains, but with a 2 or 3 tier approach
  - Ex: prodDBServer.internal.example.com
    - *.internal.example.com
  - Ex: citrix.external.example.com
    - *.external.example.com
  - keeps FQDNs out of CT logs
  - but protects most FQDNs if a cert is compromised

Username Enumeration / Verification

Blue Team / Defenders (cont.)

- STOP risk accepting Username Enumeration!
  - Don’t use vendors that do
  - The difference between valid and invalid accounts should be indistinguishable

Username Enumeration / Verification

Blue Team / Defenders (cont.)

- Ensure responses are the same for:
  - login attempts, password reset requests, and so on
- Introduce a randomized time delay
  - Example: If valid account take 100 ms longer
  - Add a 0.1 - 1.0 sec random delay for invalid
  - Add a 0 - 0.9 sec random delay for valid

Predictable Passwords

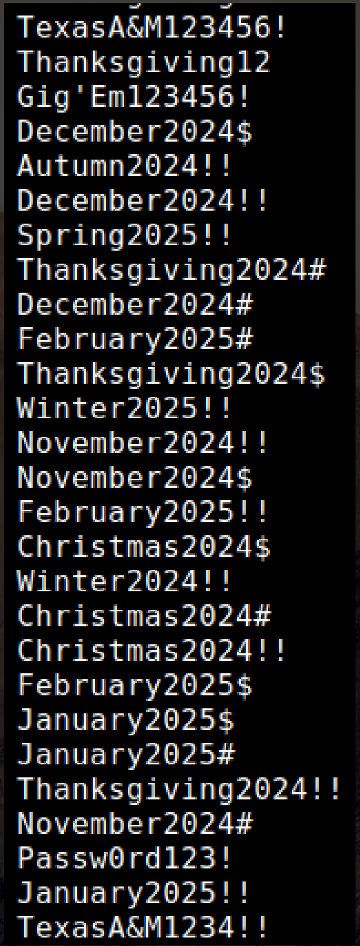
due to forced password rotation policy

Predictable Passwords

- Many users are forced to change passwords
  - arbitrarily - ex. every 90 days
- NOT a meaningful protection from breached passwords
  - breached passwords are used in minutes - few days
- All reputable standards advise against this practice
  - NIST, OWASP, and so on

Predictable Passwords

- Forced changes lead to VERY predictable passwords
  - Spring2025!, ACMECORP_2025#
  - Incrementing: Password1, Password2, Password3, etc.
- Our internal script
  - generates a short list of prioritized passwords - ~hundreds/thousands
  - reliably compromises ~20% of accounts
- A 90-day rotation policy is worse than useless
  - it’s what will enable us to compromise your network

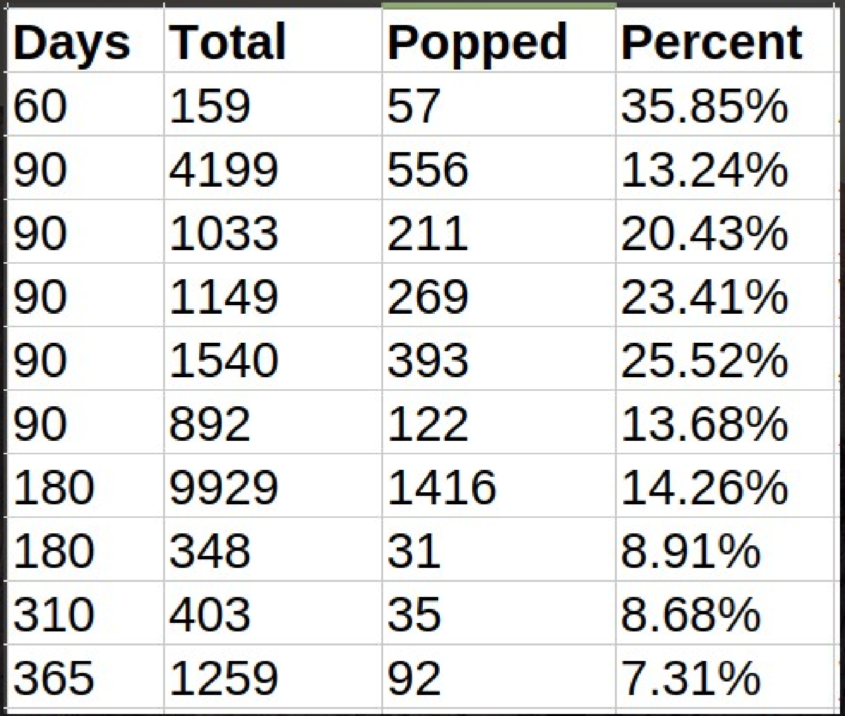


```
TexasA&M123456!
Thanksgiving12
Gig'Em123456!
December2024$
Autumn2024!!
December2024!!
Spring2025!!
Thanksgiving2024#
December2024#
February2025#
Thanksgiving2024$
Winter2025!!
November2024!!
November2024$
February2025!!
Christmas2024$
Winter2024!!
Christmas2024#
Christmas2024!!
February2025$
January2025$
January2025#
Thanksgiving2024!!
November2024#
Passw0rd123!
January2025!!
TexasA&M1234!!
```

Predictable Passwords

Blue Team / Defenders

- Do NOT force rotate passwords arbitrarily
  - Disable password expiration
- DO rotate IMMEDIATELY if compromised



Days	Total	Popped	Percent
60	159	57	35.85%
90	4199	556	13.24%
90	1033	211	20.43%
90	1149	269	23.41%
90	1540	393	25.52%
90	892	122	13.68%
180	9929	1416	14.26%
180	348	31	8.91%
310	403	35	8.68%
365	1259	92	7.31%

Predictable Passwords

Blue Team / Defenders

- Identity Management solution that
  - restricts
    - passwords less than 14 characters
    - weak passwords
    - compromised passwords
  - rate limits intelligently
    - ex. exponentially, based on IP, etc.
    - Do NOT lockout accounts - this creates a DoS vulnerability
  - has anomaly detection - ex. odd login behavior
- Audit password hashes at least quarterly

Password Spray

Password Spray

- Password spraying:
  - Try one password across all accounts
  - Select next password, try across all accounts
  - pause as needed to avoid lockout or detections
- Typical rate ~200 passwords/day
- With ~1000 passwords
  - historically compromise ~20% of accounts
- Could rotate IP every request
  - rarely needed
- Is often completely missed by monitoring

Password Spray

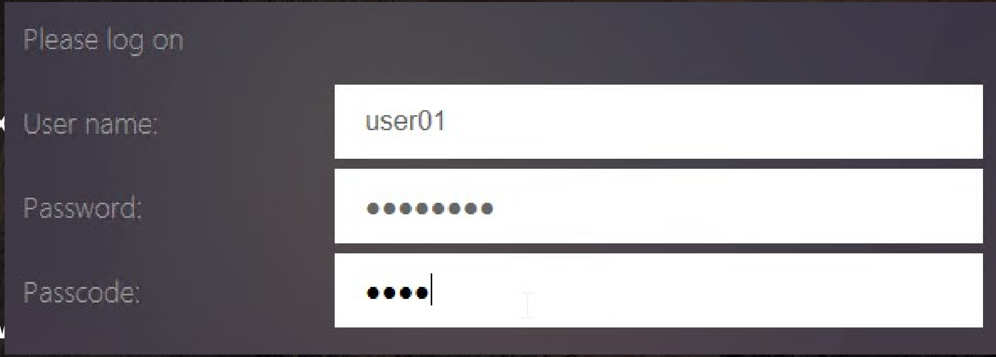
Blue Team / Defenders

- Mitigate what allowed this:
  - Internal Usernames in Metadata
  - Predictable Usernames
  - User enumeration
  - Password Policy
  - Weak passwords
  - MFA (next)
- Monitor for password attacks

Multi Factor Authentication (MFA) Misconfigurations

MFA - Misconfigurations

- MFA could have protected against the
  - user enumeration, password spray, DoS, and more
  - IF it were configured securely
- The problem: MFA doesn’t come in until AFTER password
  - You’ve already see how dangerous this is
- Back in the day…
  - the login screen had
    - the username box, password box
    - AND a box for your RSA token
  - if ANY of those were wrong
    - you got a failed login
    - you didn't know which one was w
- Usability drove us to where it is now
  - able to verify a password
  - before MFA



Please log on

User name: user01

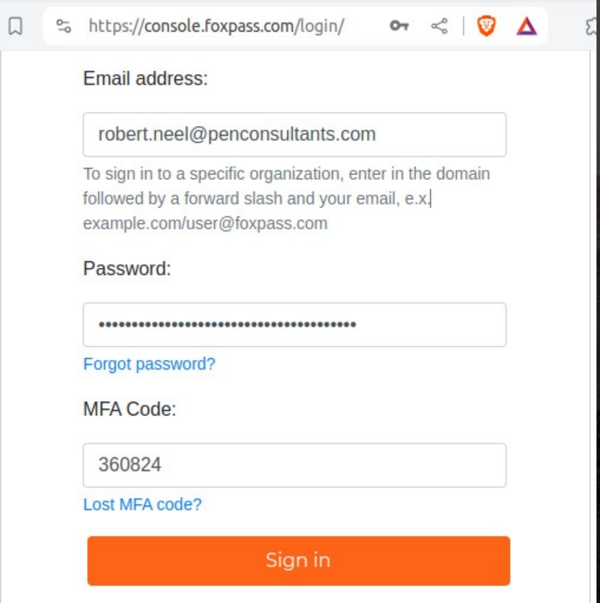
Password: ●●●●●●●●●

Passcode: ●●●●

MFA - Misconfigurations

Blue Team / Defenders

- Check MFA before the password
  - in the back-end
  - dual benefit of
    - protecting against password attacks
    - preventing a DoS attack
- For SMS-based or push notification
  - collect all three pieces of information (username+password+mfa)
  - verify the username+password - on the back-end only - before sending out the OTP/push
    - prevents a flood of SMS/pushes
  - Also verify the OTP/push before giving a pass/fail back to the user or counting against a failed/lockout counter
- Resources
  - https://penconsultants.com/MFAFUD
  - https://penconsultants.com/MFAAttacks



https://console.foxpass.com/login/

Email address:

robert.neel@penconsultants.com

To sign in to a specific organization, enter in the domain followed by a forward slash and your email, e.x. example.com/user@foxpass.com

Password:

••

MFA Code:

360824

Multi Factor Authentication (MFA) Bypasses

MFA - Bypasses

- Common misconception:
  - even though we have compromised passwords
  - we cannot get past MFA
- Easy MFA bypasses…

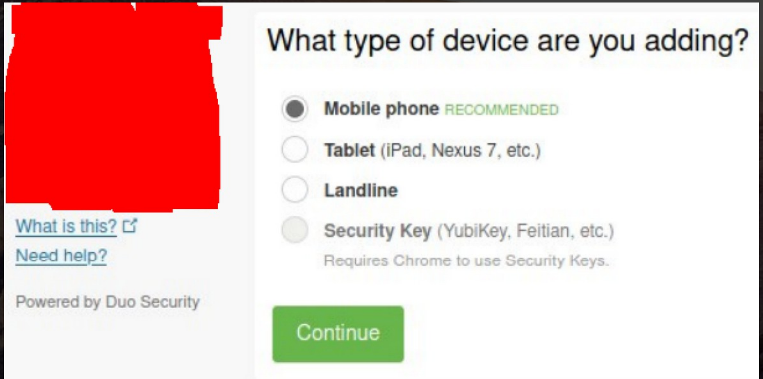
MFA - Bypasses

Bypass 1: Account without MFA

- That user or service account that got an exception

Bypass 2: Partial adoption rate

- new account / never logged in remotely
- prompt for setup after login
- we set up MFA on our phone



[redacted]

What is this?

Need help?

Powered by Duo Security

What type of device are you adding?

● **Mobile phone** RECOMMENDED

○ **Tablet** (iPad, Nexus 7, etc.)

○ **Landline**

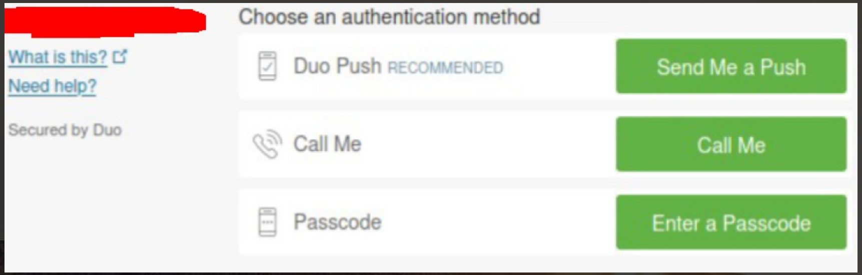
○ **Security Key** (YubiKey, Feitian, etc.)

Requires Chrome to use Security Keys.

MFA - Bypasses

Bypass 3: Send an MFA push notification

- Attackers LOVE push MFA
  - less secure than SMS/text-based
- ~20% of your users will accept the push
  - out of habit/muscle memory
- If we have more than ~5 compromised accounts
  - nearly a 100% chance of getting in



[redacted]

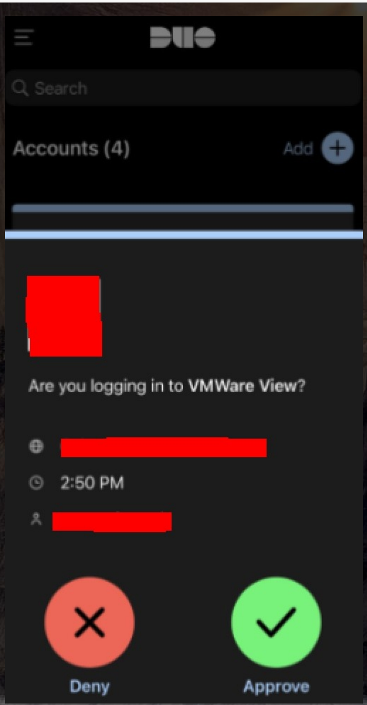
Choose an authentication method

What is this?

Need help?

Secured by Duo

Duo Push RECOMMENDED	Send Me a Push
Call Me	Call Me
Passcode	Enter a Passcode



DUO

Search

Accounts (4) Add

[redacted]

Are you logging in to VMWare View?

[redacted]

2:50 PM

[redacted]

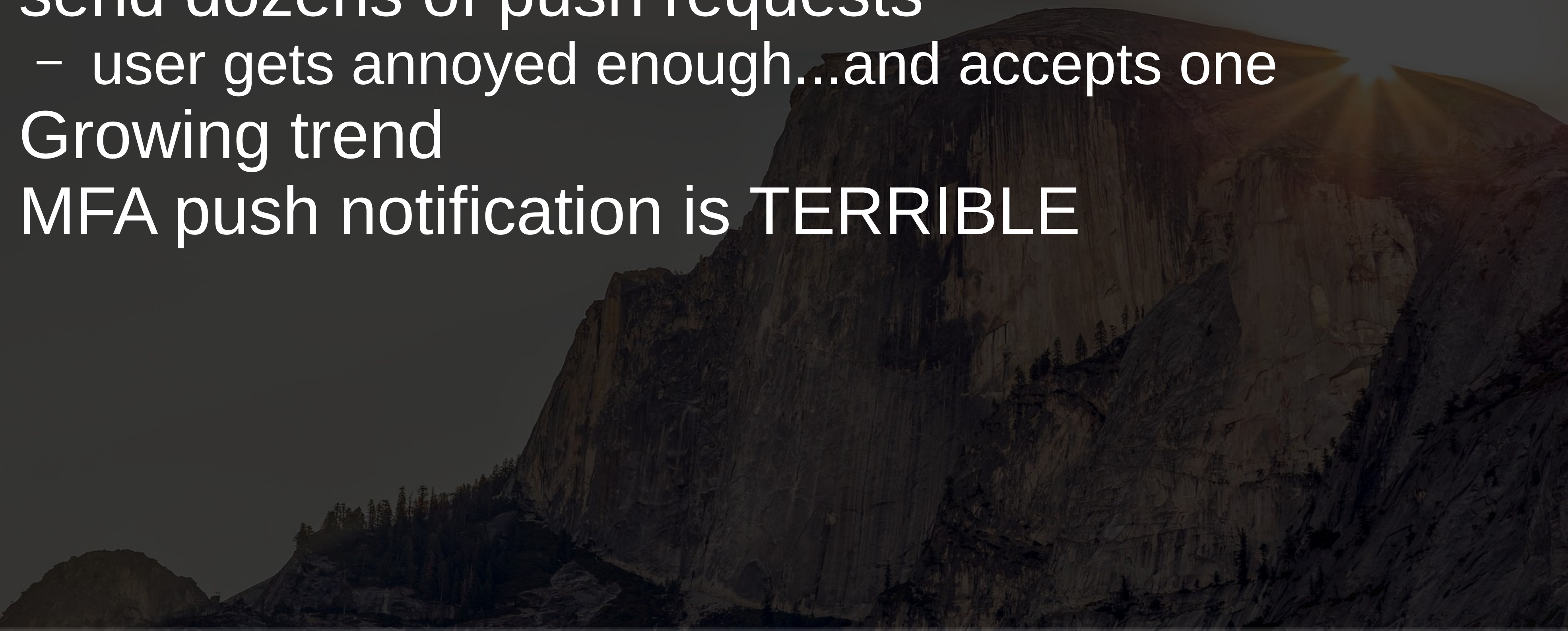
Deny

Approve

MFA - Bypasses

Bypass 4: MFA Bombing

- send dozens of push requests
  - user gets annoyed enough...and accepts one
- Growing trend
- MFA push notification is TERRIBLE



MFA - Bypasses

Other Bypass methods

- Find a service without MFA
  - always seems to be one
  - Common: Azure, Mimecast, and other cloud services that are in sync with on-prem
- Brute force the MFA OTP
- MFA OTP check is client side initiated
  - and allows another user’s MFA one-time password (OTP)
- Weak account recovery for missing MFA
  - “In what city were you born?”
- Many other ways (we’ll write a book one day)

MFA - Bypasses

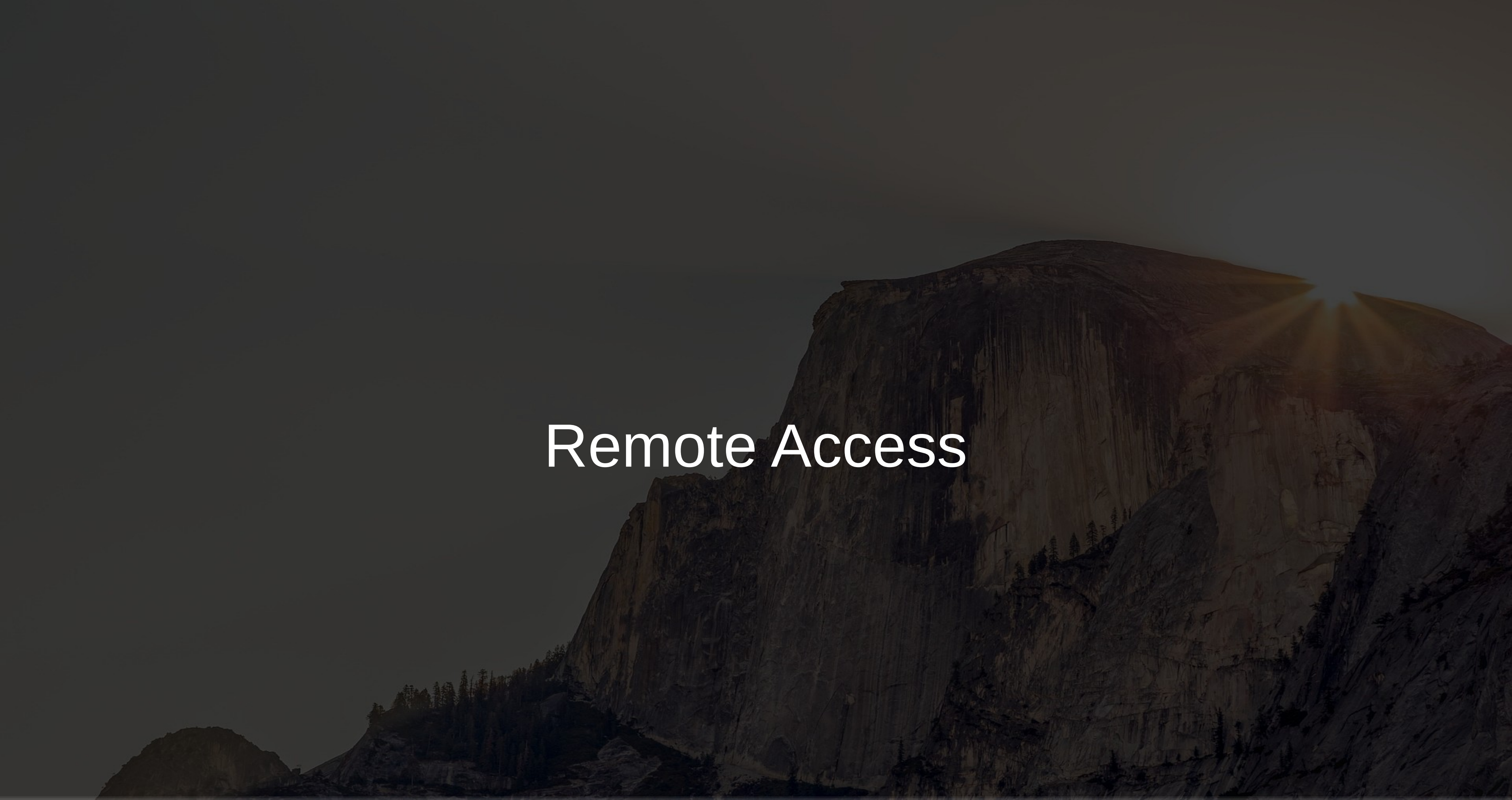
Blue Team / Defenders

- Direct correlation between usability and security with MFA
- MFA option roughly in order from strong to weak:
  - Hardware based - ex. yubikey
  - App based OTP - ex. google authenticator
  - Push with number match - ex. Microsoft’s solution
  - SMS based - It’s not the greatest, but not the worst, depends on carrier and settings
  - Push notification - no social engineering or SIM swap/jack needed
  - Email based - near worthless

MFA - Bypasses

Blue Team / Defenders (cont.)

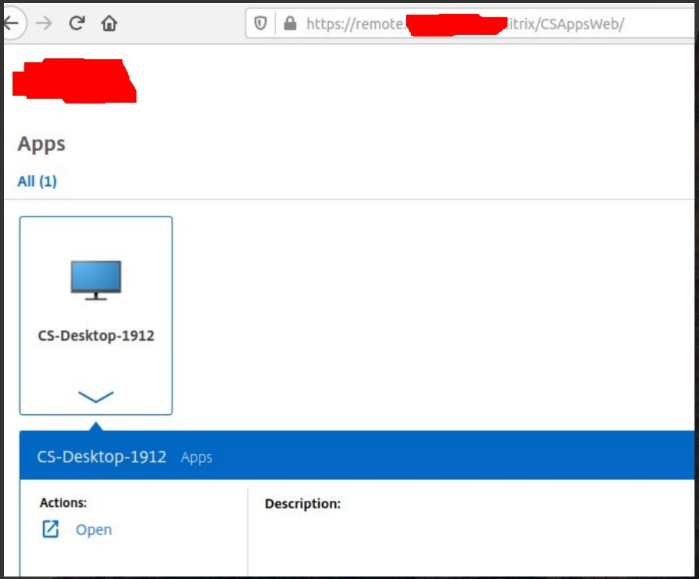
- Temporarily invalidated the OTP, once verified, to prevent brute-force
  - Note: not permanently that OTP will eventually repeat with time
- Require additional information for MFA sign-up
  - employee number, DL, DOB, etc.
  - username and password alone is not sufficient
- Send email and text message after MFA sign-up
  - increases chance it will detect a malicious takeover
  - Note: SolarWinds Armageddon of 2019-2021 was uncovered because a user received an MFA registration notification
- Resources
  - https://penconsultants.com/MFAFUD
  - https://penconsultants.com/MFAAttacks



Remote Access

Remote Access

- With access to multiple accounts
  - we gain remote access to a workstation
  - as a standard user usually



https://remote.[redacted]itrix/CSAppsWeb/

[redacted]

Apps

All (1)

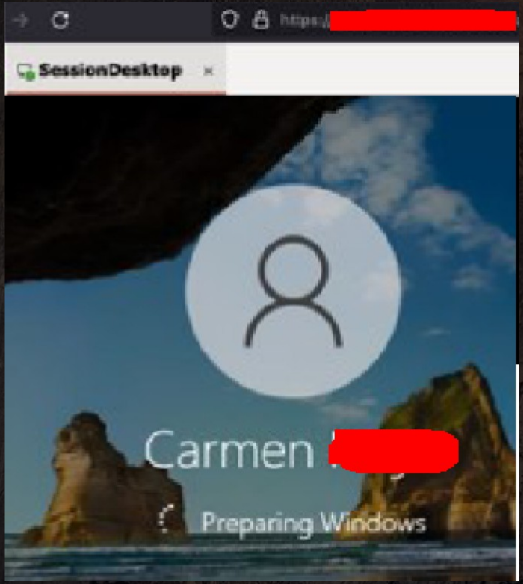
CS-Desktop-1912

CS-Desktop-1912 Apps

Actions:

Open

Description:



https://[redacted]

SessionDesktop

Carmen [redacted]

Preparing Windows

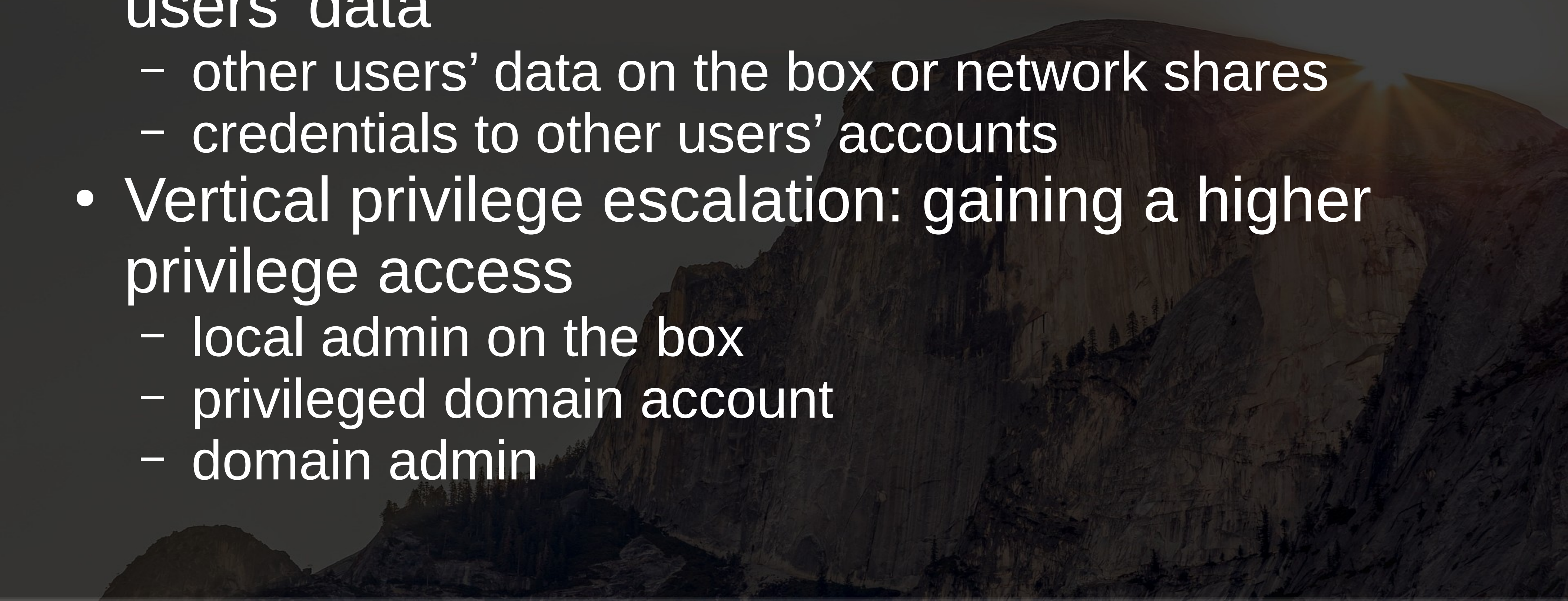
Remote Access

Blue Team / Defenders

- Anomaly detection
  - abnormal login times - 2 am?
  - abnormal login locations - non-US?
  - geographically improbable access attempts - hypersonic or teleportation?
- MFA prompt for internal authentication
  - ex. workstation, network share access, intranet, etc.
  - hopefully the user doesn’t accept twice in a row

Privilege Escalation

Privilege Escalation

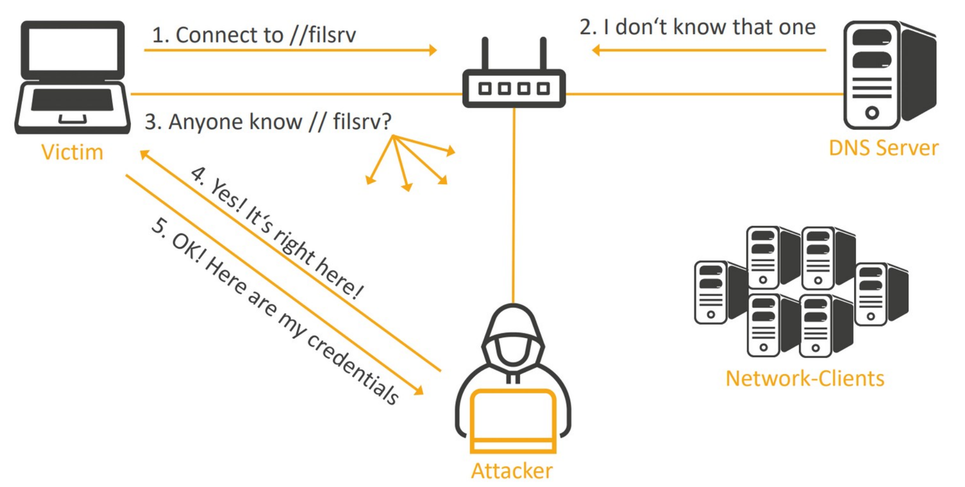


- Horizontal privilege escalation: accessing other users’ data
  - other users’ data on the box or network shares
  - credentials to other users’ accounts
- Vertical privilege escalation: gaining a higher privilege access
  - local admin on the box
  - privileged domain account
  - domain admin

Privilege Escalation

Examples

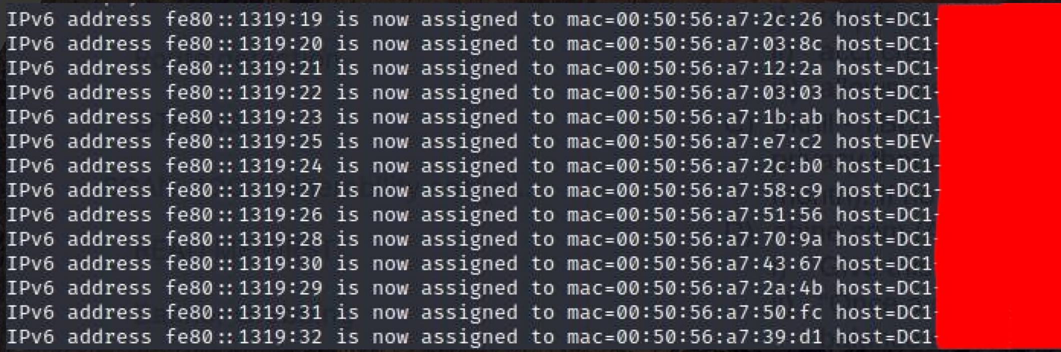
- Keylogger to grab IT admin creds
- Registry or Service weaknesses
- Creds in local or network share files
  - ~95% of the time
  - password spreadsheets
  - sysprep files
  - GPO startup scripts
  - SCCM/package installers
- Kerberoasting



Privilege Escalation

Examples (cont.)

- Man-in-the-middle legacy, weak, or unused protocols
  - ARP, LLMNR, IPv6, SSL, RDP, SMTP, etc.
- Internal phishing
- A thousand other ways
- Very common
  - we always find a way



```
IPv6 address fe80::1319:19 is now assigned to mac=00:50:56:a7:2c:26 host=DC1-[redacted]
IPv6 address fe80::1319:20 is now assigned to mac=00:50:56:a7:03:8c host=DC1-
IPv6 address fe80::1319:21 is now assigned to mac=00:50:56:a7:12:2a host=DC1-
IPv6 address fe80::1319:22 is now assigned to mac=00:50:56:a7:03:03 host=DC1-
IPv6 address fe80::1319:23 is now assigned to mac=00:50:56:a7:1b:ab host=DC1-
IPv6 address fe80::1319:25 is now assigned to mac=00:50:56:a7:e7:c2 host=DEV-
IPv6 address fe80::1319:24 is now assigned to mac=00:50:56:a7:2c:b0 host=DC1-
IPv6 address fe80::1319:27 is now assigned to mac=00:50:56:a7:58:c9 host=DC1-
IPv6 address fe80::1319:26 is now assigned to mac=00:50:56:a7:51:56 host=DC1-
IPv6 address fe80::1319:28 is now assigned to mac=00:50:56:a7:70:9a host=DC1-
IPv6 address fe80::1319:30 is now assigned to mac=00:50:56:a7:43:67 host=DC1-
IPv6 address fe80::1319:29 is now assigned to mac=00:50:56:a7:2a:4b host=DC1-
IPv6 address fe80::1319:31 is now assigned to mac=00:50:56:a7:50:fc host=DC1-
IPv6 address fe80::1319:32 is now assigned to mac=00:50:56:a7:39:d1 host=DC1-
```

Privilege Escalation

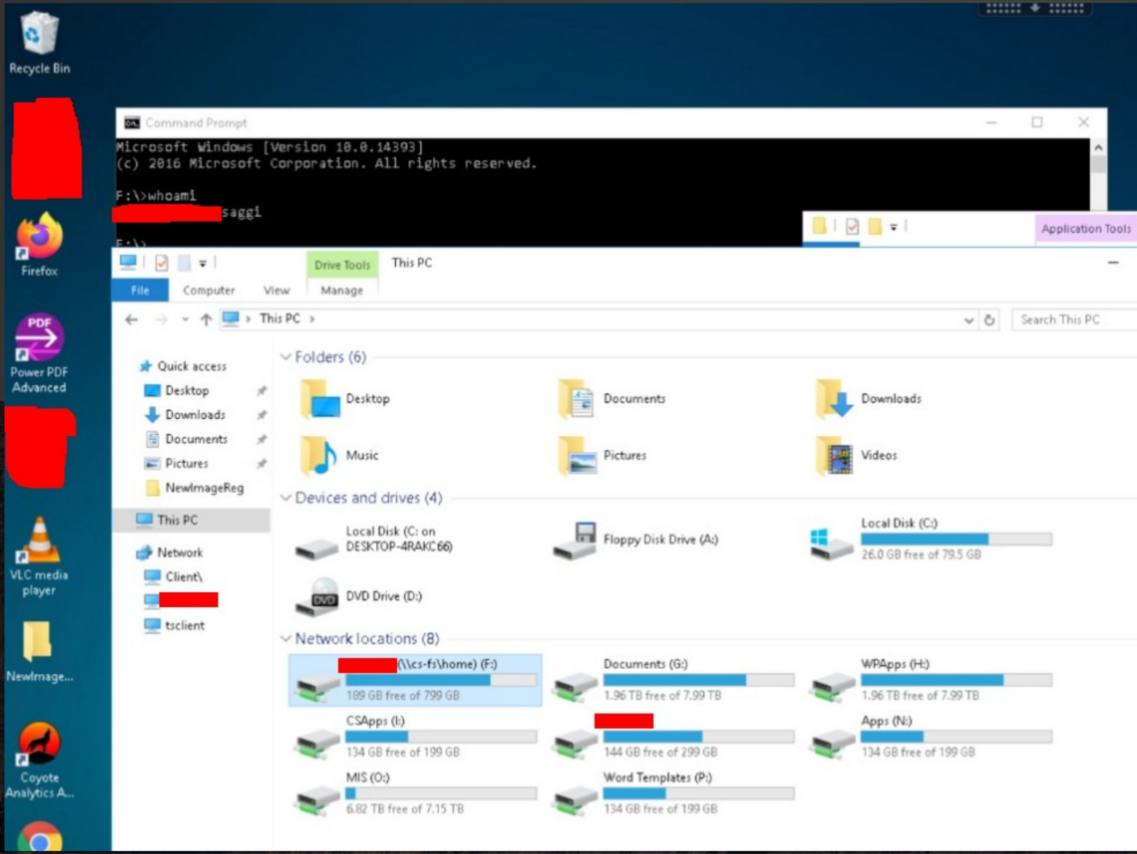
Blue Team / Defenders

- Disable and block protocols not being used
  - LLMNR & NBT-NS
  - IPv6 - all Windows enabled by default
  - etc.
- Audit network share permissions and content
  - takes time/work, but this is a goldmine for attacker
- Too numerous to list all the things
  - Secure your internal network
  - Get a pentest

Data Collection & Staging

Data Collection & Staging

1) Crawl all of your open network shares
   - always a lot of those
   - PII, PHI, IP, service account passwords, etc.
2) Compromise more systems, accounts, data
3) Repeat



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

F:\>whoami
[redacted]saggi

F:\>
```

Folders (6)

Desktop
Documents
Downloads
Music
Pictures
Videos

Devices and drives (4)

Local Disk (C: on DESKTOP-4RAKC66)
Floppy Disk Drive (A:)
Local Disk (C:) 26.0 GB free of 79.5 GB
DVD Drive (D:)

Network locations (8)

[redacted](\\cs-fs\home) (F:) 189 GB free of 799 GB
Documents (G:) 1.96 TB free of 7.99 TB
WPApps (H:) 1.96 TB free of 7.99 TB
CSApps (I:) 134 GB free of 199 GB
[redacted] 144 GB free of 299 GB
Apps (N:) 134 GB free of 199 GB
MIS (O:) 6.82 TB free of 7.15 TB
Word Templates (P:) 134 GB free of 199 GB

Data Collection & Staging

- As we collect your data…
- Stage in prep for exfil
  - dedupe, filter, compress, obfuscate
- Note: testers attempt to:
  - minimize data collected
  - change to synthetic data at this point

Data Collection & Staging

Blue Team / Defenders

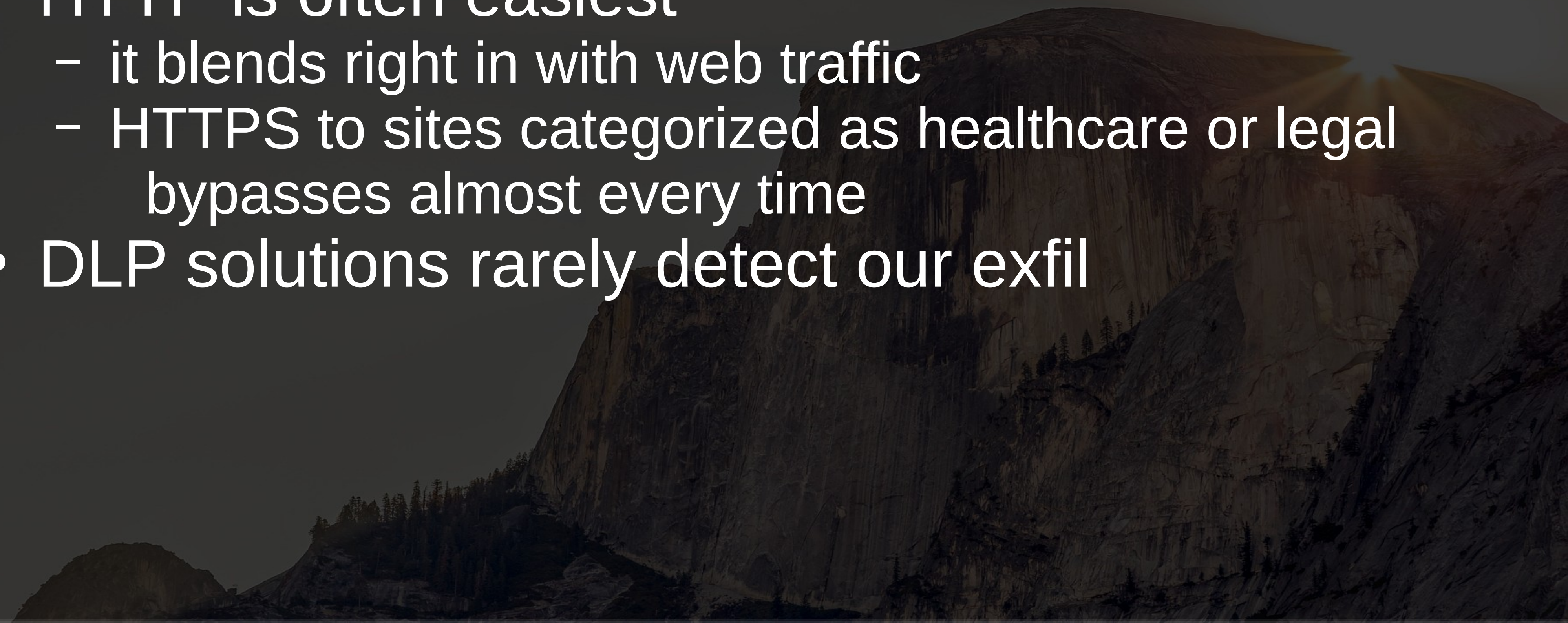
- All the things mentioned so far
- Large anomalous data transfers
  - from network shares
  - to the disk
- Endpoint Detection & Response (EDR)
  - detect tooling and behavior
  - assuming attacker is on a managed device
- Endpoint Data loss prevention (DLP) - maybe
  - assuming no real-time obfuscation

Exfil / Avoid DLP

Exfil / Avoid DLP

Get the data out, and avoid detection

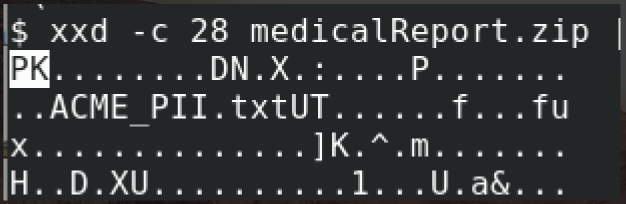
- HTTP is often easiest
  - it blends right in with web traffic
  - HTTPS to sites categorized as healthcare or legal bypasses almost every time
- DLP solutions rarely detect our exfil



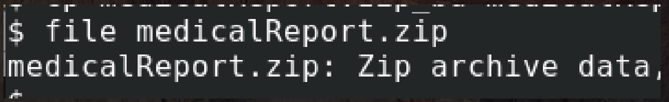
Exfil / Avoid DLP

Get the data out / avoid detection

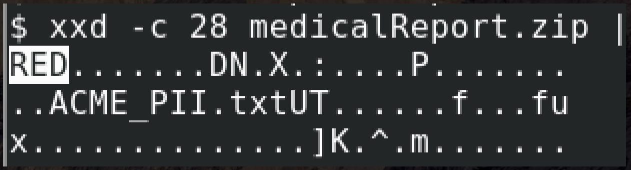
- Worst case scenario
  - zip the payload
    - change the first 2 bytes - the magic bytes
    - decompression will fail
    - data cannot be analyzed
  - this fools nearly every pricey DLP solution
- Avoid large data transfer detections
  - Or: Do it quick before caught



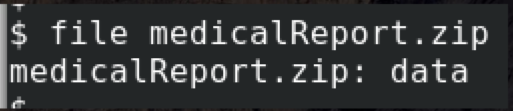
```
$ xxd -c 28 medicalReport.zip |
PK........DN.X.:....P.......
..ACME_PII.txtUT......f...fu
x..............]K.^.m.......
H..D.XU..........1...U.a&...
```



```
$ file medicalReport.zip
medicalReport.zip: Zip archive data,
```



```
$ xxd -c 28 medicalReport.zip |
RED.......DN.X.:....P.......
..ACME_PII.txtUT......f...fu
x..............]K.^.m.......
```

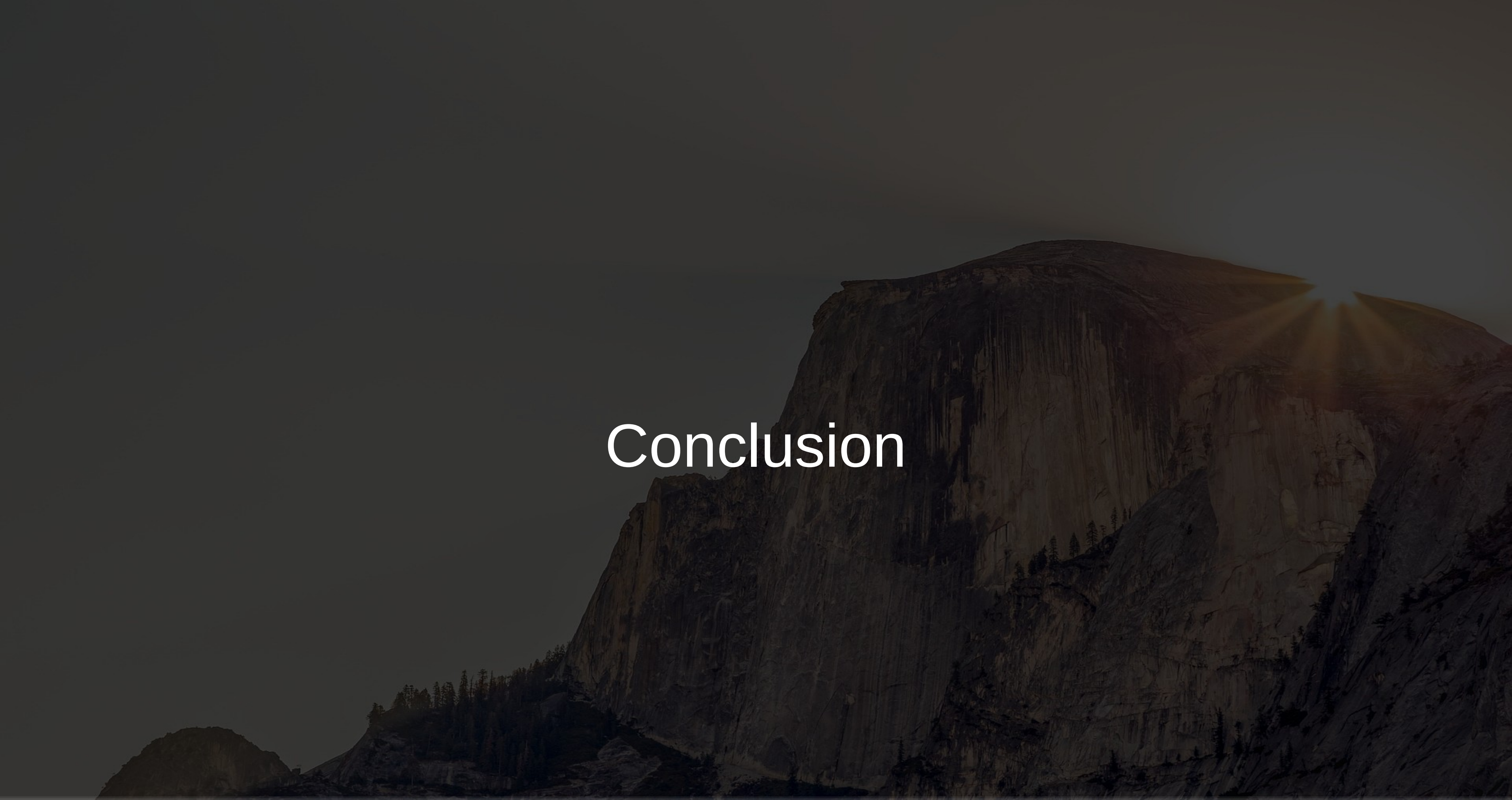


```
$ file medicalReport.zip
medicalReport.zip: data
```

Exfil / Avoid DLP

Blue Team / Defenders

- Alert on large and anomalous data transfers
  - Internal & Outbound
  - Start incident response
- Tune and baseline DLP solutions
  - These are usually configured to ignore…
  - file types it does not recognize
  - large files
  - and so on
- Limit exceptions in DLP, SSL Inspection, etc.
  - when able



Conclusion

Conclusion

- This attack chain used
  - multiple, often risk-accepted, or not considered vulnerabilities
- Doesn’t include many other common ways
- Bottom Line: Get a penetration test!
  - full white box
  - don’t waste your time on black box, time-limited testing - very low ROI
  - from a reputable firm
    - https://penconsultants.com/choosing
    - key metric to look for: dozens of actionable findings

Questions?

Robert Neel

- Email: robert.neel@PENConsultants.com
- X: @redeemedHacker
- LinkedIn: RNeel

PEN Consultants

- Email: info@PENConsultants.com
- Web: https://PENConsultants.com
- X: @PENConsultants_
- LinkedIn: PENConsultants

Credits / References

- Image: https://owasp.org/www-pdf-archive/OWASP_FFM_41_OffensiveActiveDirectory_101_MichaelRitter.pdf
-