KnowBe4
Human error. Conquered.

The Pesky Password Problem: Policies That Help You Gain the Upper Hand on the Bad Guys

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

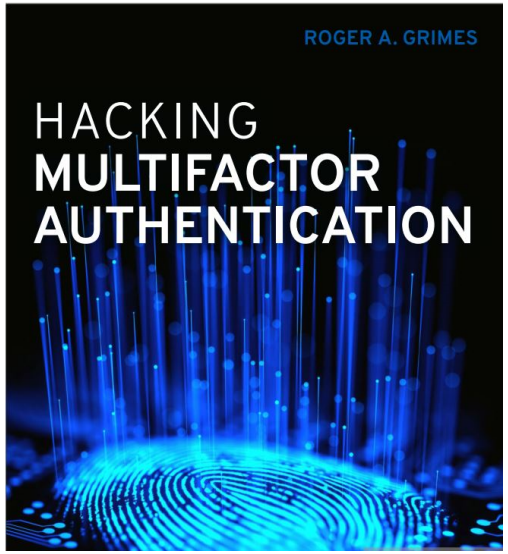
About Roger

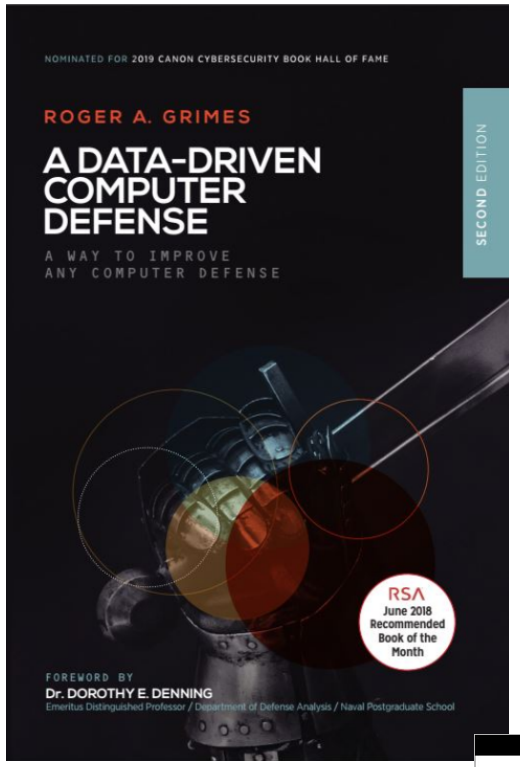
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

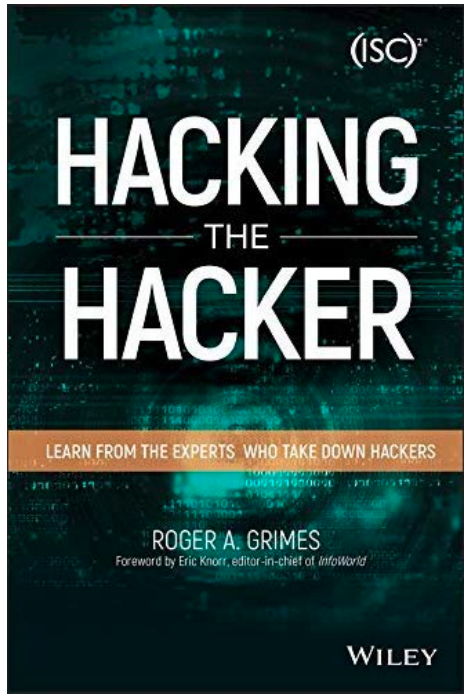
Certification exams passed include:

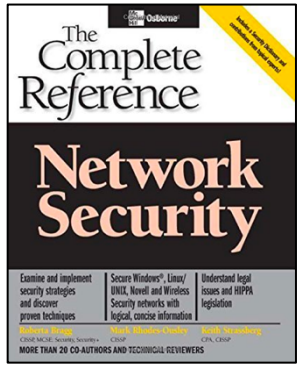
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

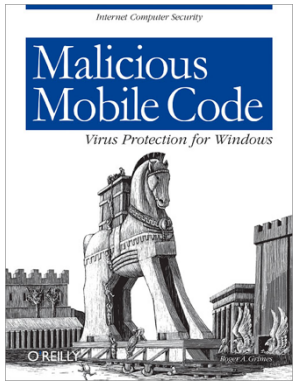
Roger's Books

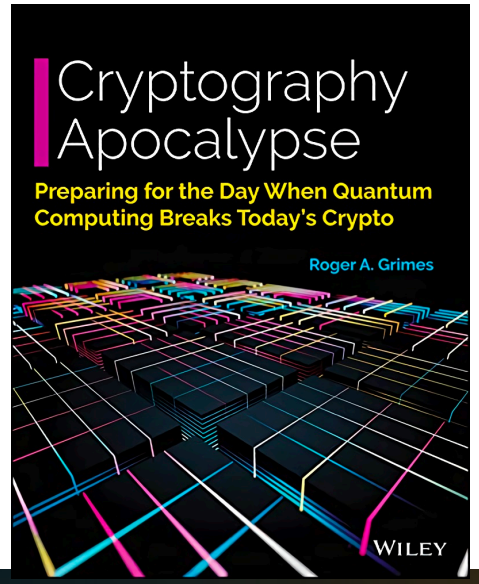


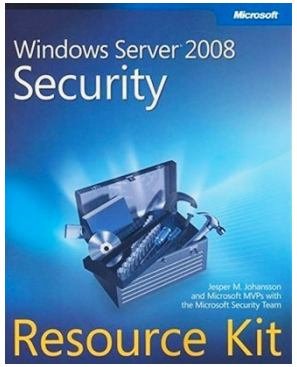


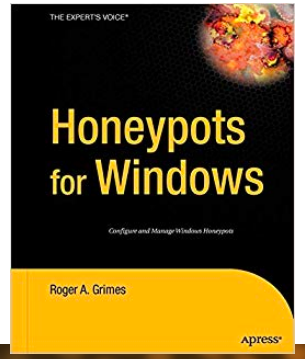


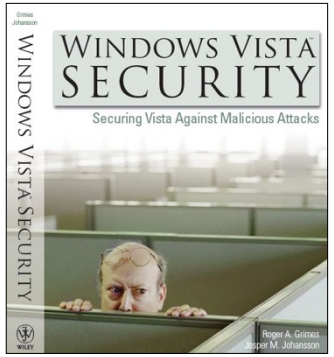


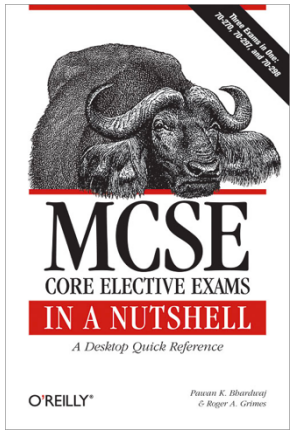












Agenda

- Problems with Passwords
- Types of Password Attacks
- Password Policy Recommendations

Agenda

- Problems with Passwords
- Types of Password Attacks
- Password Policy Recommendations

Passwords Basics

- Earliest and most common digital authentication method by far
- User/Subject supplies an identity label (i.e. logon name) and supposedly a password only known by them and the authentication verifier
- 94-characters is average US keyboard
- Can take a lot of guesses to guess right
- If truly random, and that usually isn't the case

Password Length	94 Character-Set Passwords	
1	94	
2	8,930	
3	839,608	
4	78,914,598	tens of millions
5	7,417,954,916	billions
6	697,287,736,066	
7	65,545,047,155,424	tens of trillions
8	6,161,234,432,566,330	quadrillions
9	579,156,036,661,183,000	
10	54,440,667,446,151,200,000	
11	5,117,422,739,938,210,000,000	
12	481,037,737,554,192,000,000,000	
13	45,217,547,330,094,000,000,000,000	
14	4,250,449,449,028,840,000,000,000,000	
15	399,542,248,208,711,000,000,000,000,000	

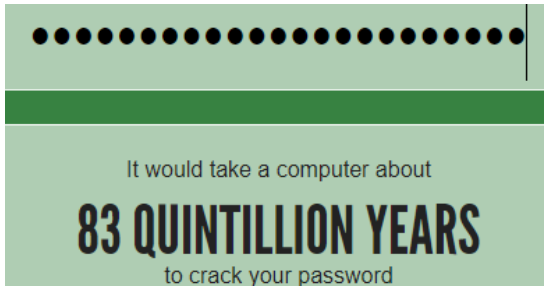
Passwords Basics

- On a Microsoft Windows system you can use over 65,000 characters for your password, although most people use the same 23 - 32 characters
- Lots of free password hacking/cracking calculators to determine if your password policy can withstand sustained guessing/cracking attacks

Max. # of Characters/Symbols Size Allowed in Passwords**	94
Password Length (max. of 15 for this calculator)	8
Complexity Enabled? (Input Yes or No)	YES
# of attacker Password Guesses per Minute	184.00
Max. # of days between password change	90
y Model Selection in radio button)	
Entropy Model Selected (displayed only to confirm)	NIST
Bits of entropy based on password length*	24
Equivalent number of possible passwords based on entropy bits*	16,777,216
Equivalent password length based on entropy bits	4
DO NOT CHANGE VALUES OR FORMULAS BELOW THIS LINE	DO NOT CHANGE VALUES OR FORMULA
Max. number of possible passwords with perfect randomness	6,161,234,432,566,330
Max. number of "likely" passwords (using entropy assumptions*)	16,777,216
Max. Time (days) to guess "likely" password	63
Avg. Time (days) to guess "likely" password	32
Will guessing be successful vs. password policy?	YES
# of password guesses/min. to break existing password policy	64.7

- Email me at rogerg@knowbe4.com to get password “hacking” spreadsheets

Passwords Basics



Online Password Strength Checking Sites

- https://howsecureismypassword.net/
- https://password.kaspersky.com/
- https://thycotic.com/resources/password-strength-checker
- http://www.passwordmeter.com
- https://www.howsecureismypassword.io/

- Caution: Any website asking you to submit your real password to determine strength could be using your submission against your interests
  - Use another similar, but not identical password submission to get the same information.

Are Passwords Going Away Anytime Soon?

- No!
- The average person has 3 to 19 different active passwords
- Passwords used by users, devices, services, networks, etc.
- The things that replace them (e.g. MFA, biometrics, behavioral analytics, etc.) don't work on even 2% of the world's web sites and services
- The most popular non-password solutions in the world don't work on 1% of the world's websites
  - So, you would have multiple types/instances of them to cover the 2% that does accept MFA much less the world
- The articles claiming "passwords' days are numbered" have been coming out for 3 decades

Are Passwords Going Away?

- Even the things that replace passwords (e.g. MFA, biometrics, etc.) are routinely hacked and have been for decades
- But big password problem: The average person has to logon to 170+ websites and only has 3 to 19 passwords
- This makes one compromise able to leverage other compromises more easily

Problems with Passwords

General Password Problems

- Easy to Hack
- Easy to Forget
- Hard to Forget
- Easy to Share/Reuse

Good Things About Passwords

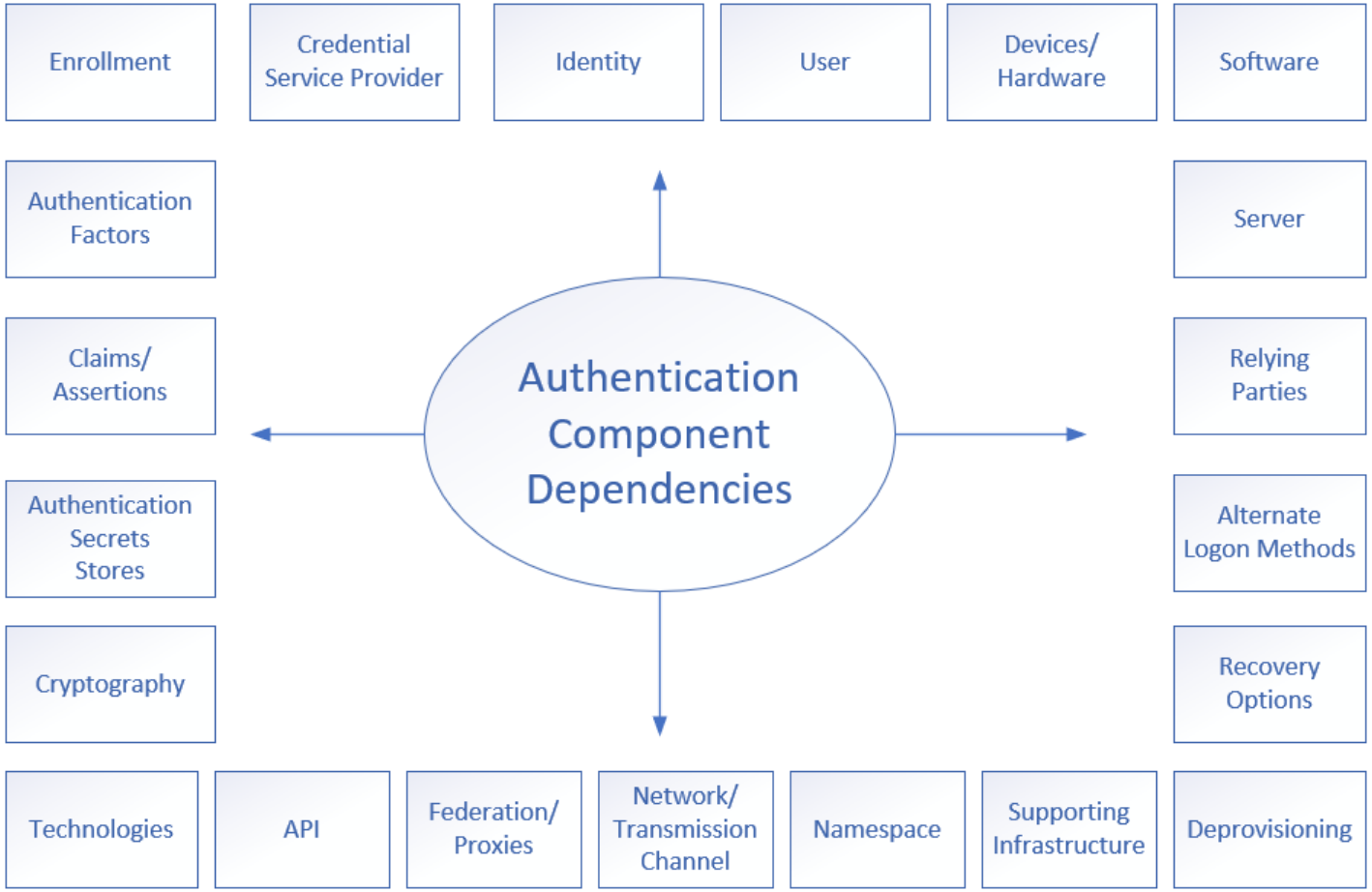
- Easy to Generate a New One When Needed
- Works With Nearly Everything
- Can Be Secure If Used and Protected Correctly

Agenda

- Problems with Passwords
- Types of Password Attacks
- Password Policy Recommendations

Password Attacks

Any of these dependencies can be attacked



Password Attacks

Most Popular Password Attack Types

- Social Engineering
- Guessing
- Hash Cracking
- Stealing
- Lookups
- Account Takeover (ATO) Recoveries

Password Attacks

<u>Popular Password Attack Types</u>

Social Engineering

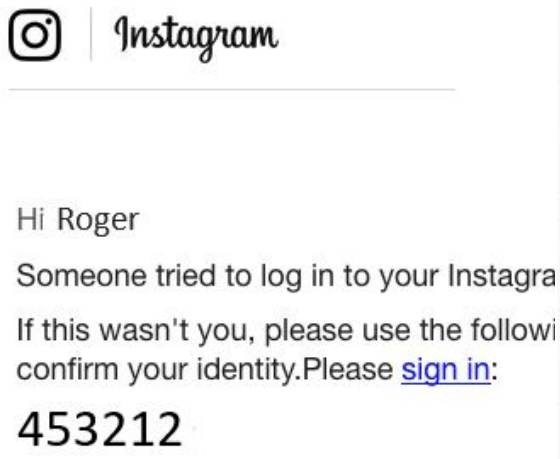
- One of the most common ways to get passwords
- Email, websites, SMS, IM, social media, phone call, etc.

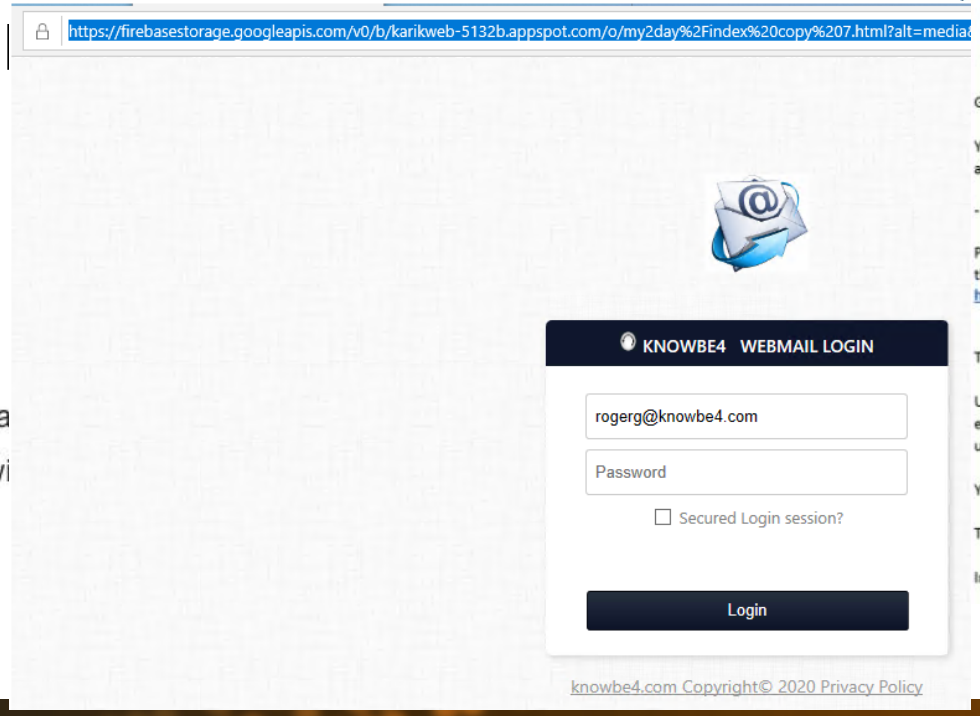
Password Attacks

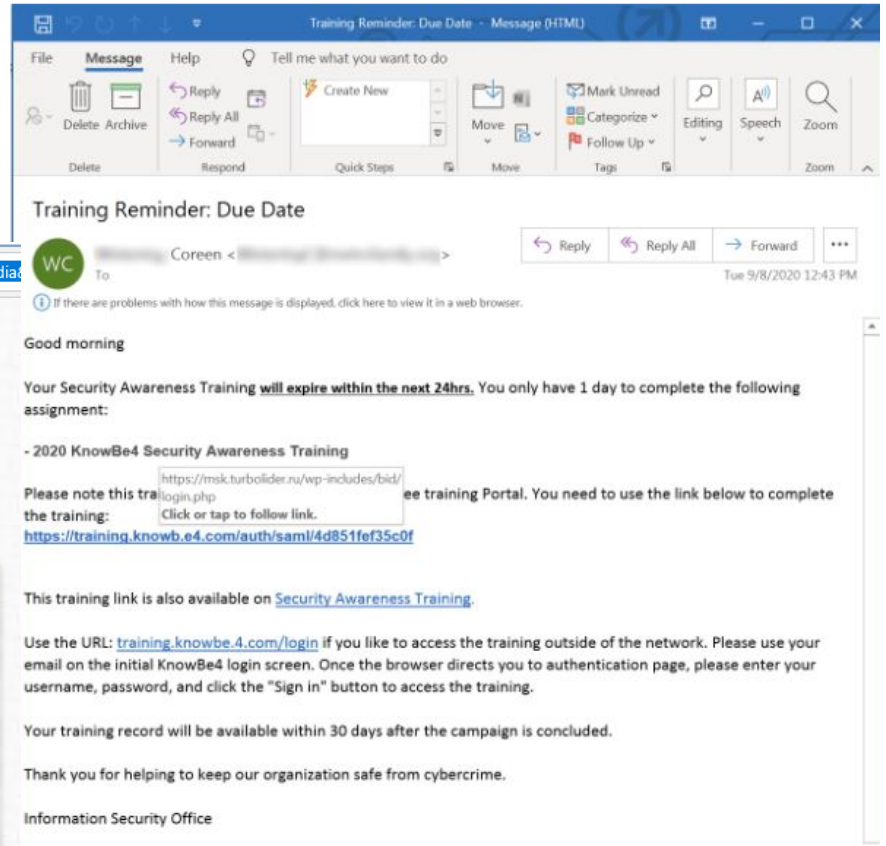
Popular Password Attack Types

Social Engineering

- One of the most common ways to get passwords
- Email, websites, S







Password Attacks

<u>Popular Password Attack Types</u>

Guessing Attack Methods

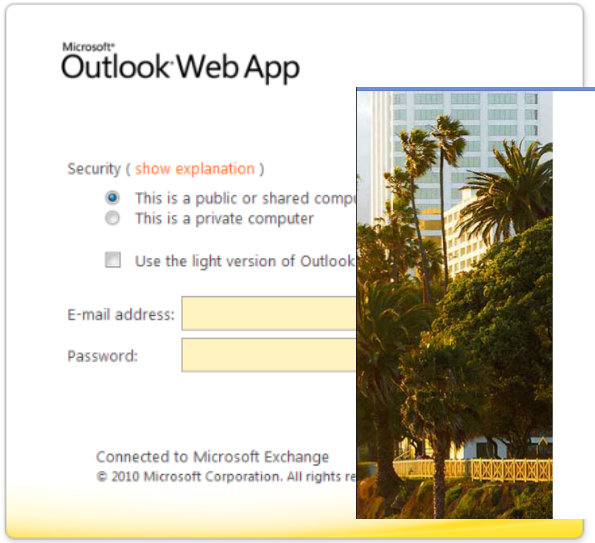
- Bruteforce (e.g. a, aa, ab, abc…etc.)
- Dictionary Attack
  - People like to use “root” words for their passwords, in their own language
  - So use dictionary (170K words in Oxford English dictionary)
  - And add “complexity” to the root word (e.g. frog, frog1, fr0g, etc.)
- Use logic based on human behaviors
  - Most people have a “working vocabulary” of 3000 – 4000, max. 10,000 words
  - Start with the most popular words and passwords first

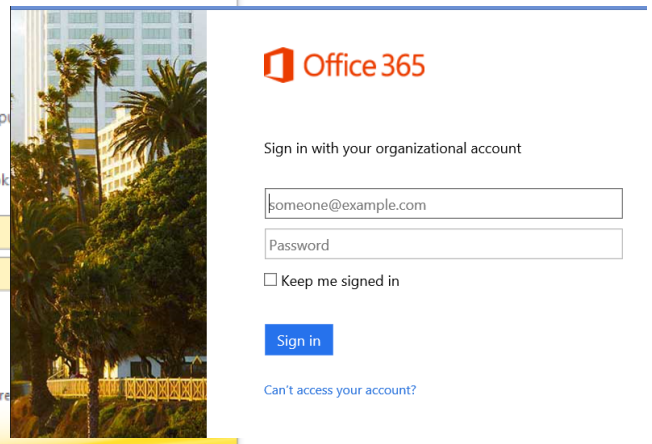
Password Attacks

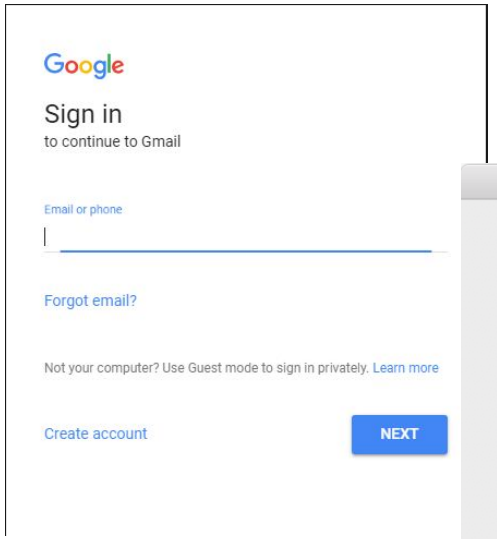
Popular Password Attack Types

Guessing

- Attackers will just guess at accessible logon prompts
  - RDP, OWA, O365, Gmail, VPNs, etc.

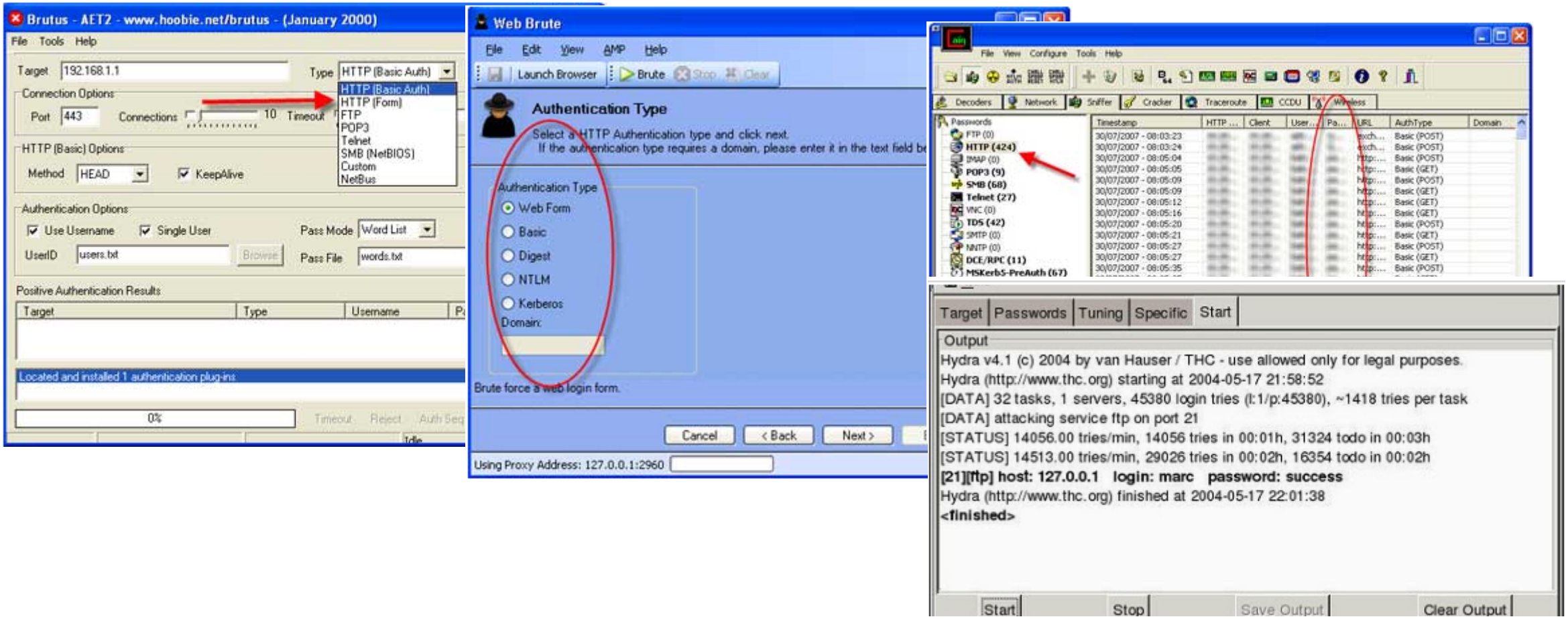






Password Attacks

Hacker Tools to Guess At Passwords



Password Attacks

<u>Popular Password Attack Types</u>

Guessing

- Password Credential Stuffing/Spray Attacks
  - Will guess a 100 to 1000 passwords, one-at-a-time, slowly, against many accounts

Akamai: We Saw 61 Billion Credential Stuffing Attacks in 18 Months

In March 2019, the **Federal Bureau of Investigation** (FBI) alerted Citrix they had reason to believe cybercriminals had gained access to the company's internal network. The FBI told Citrix the hackers likely got in using a technique called "password spraying," a relatively crude but remarkably effective attack that attempts to access a large number of employee accounts (usernames/email addresses) using just a handful of common passwords.

Password Attacks

<u>Hackers Love Finding Unprotected Open API to Guess Against</u>

Application Programming Interfaces (APIs) connection points are often accessible over the Internet

- Many require/allow logon authentication
- Can be used for password spray attacks
- May bypass MFA requirements, not have acct lockout, not well monitored
- Akamai said 75% of password spray attacks were against APIs
  - https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

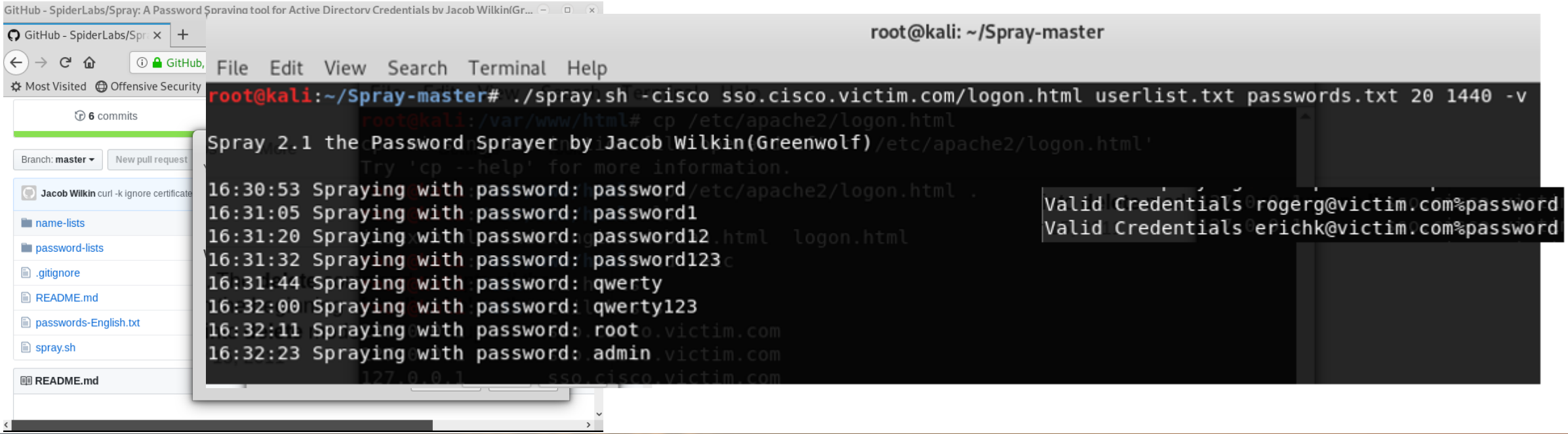
Password Attacks

Password Spray Attack Tools

Tool – Spray

Useage: spray.sh –<typeoflogon> <targetIP> <usernameList> <passwordList>

<AttemptsPerLockoutPeriod> <LockoutPeriodInMinutes> <DOMAIN>



Password Attacks

<u>Popular Password Attack Types</u>

Guessing

- Only works with truly weak passwords
  - *password* is the most common password (also *Password2*, *123456*, *admin*, *qwerty*, etc.)
  - Most organizations have at least 1 user with a password on a list of the 1000 most popular passwords
  - 70% of organizations have at least 1 user with a password on a list of 100 passwords
  - Most “complex” passwords aren’t that complex

Password Attacks

Popular Password Attack Types

Guessing – Sometimes it's not really fair to call it "guessing"

- Hard-coded and Default Passwords
  - Many devices come with well-known default passwords
  - Many people never change the well-known default passwords
  - Just google/bing for 'default password lists' and have fun
  - Many built-in passwords cannot be changed
- Has been one of the most popular ways people and devices are successfully attacked for decades
- Becoming a much bigger problem with IoT

Password Attacks

Password Guessing Malware

- Many malware programs will guess against devices, logon portals, and network shares
- Usually guess using 100 or so common passwords
- Examples: Conficker, Emotet, Kobot

Once Trojan.Emotet has infected a networked machine, it will propagate by enumerating network resources and write to share drives, as well as brute force user accounts. Infected machines attempt to spread Emotet laterally via brute forcing of domain credentials, as well as externally via its built-in spam module. As a result, the Emotet botnet is quite active and responsible for much of the malspam we encounter.

Description:
This worm propagates through network shares. It uses NetBEUI functions to get available lists of user names and passwords. It then lists down the available network shares. It uses the obtained user names and passwords to drop a copy itself into the said shares. It also uses a list of user names and passwords, apart from those it gathers, to access machines.

Password Attacks

<u>Popular Password Attack Types</u>

Password Guessing Defenses:

- Change any default passwords immediately
- Use strong passwords
- Enable Account Lockout polices
- Enable failed logon monitoring/alerting
- Restrict connections to APIs
- Use Multifactor Authentication (MFA) where you can

Password Hash Theft

Password Hash Basics

- In most authentication systems, passwords are stored and transmitted as cryptographic hashes (LM, NT, MD5, Bcrypt, SHA1, SHA2, SHA-3, etc.)

Hash Algorithm	Hash result for "frog"
MD5	938C2CC0DCC05F2B68C4287040CFCF71
SHA-1	B3E0F62FA1046AC6A8559C68D231B6BD11345F36
SHA-2	74FA5327CC0F4E947789DD5E989A61A8242986A596F170640AC9033 7B1DA1EE4
SHA-3 (512)	6EB693784D6128476291A3BBBF799d287F77E1816b05C611CE114AF 239BE2DEE734B5Df71B21AC74A36BE12CD629890CE63EE87E0F53BE987 D938D39E8D52B62

Password Hash Theft

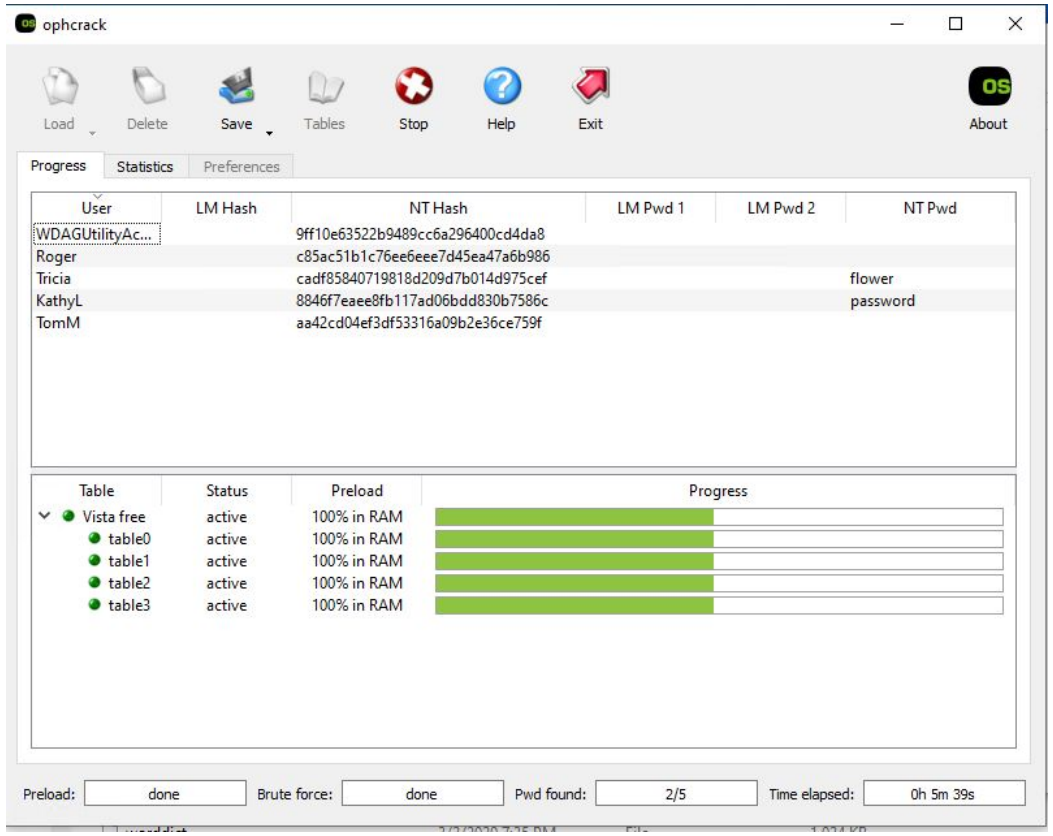
<u>Stealing Password Hashess</u>

- Can be stolen from password storage files, databases, from memory, or from eavesdropping on network connections
- On a device, normally an attacker needs elevated access (i.e. administrator, root, etc.; plus a password hash theft tool
- On an Active Directory domain controller, attacker needs domain administrator or better
- Man-in-the-middle (MitM) network attacks can steal password hashes or derive hashes from challenge/response sessions

Password Hash Cracking

Password Hash Cracking Tools

- Once obtained, password hashes can be "cracked" back to their plaintext equivalents using brute force, hash tables, rainbow tables, etc.



Password Hash Cracking

How Fast Can Password Hashes Be Cracked?

Note: Hashes are not equal. Cracking speed depends on type of hash being cracked

- When you hear of “cracking speed” usually people are talking about Windows NT hashes (also NTLM is a network protocol not a hash)
- NT hashes are only moderately hard to crack
- LM hashes are very easy (but disabled with 17+ char passwords)
- PBKDF2 used in Windows 10 for some operations is fairly hard
- BCRYPT harder to crack
- SHA2 hard to crack
- MD5, SHA1, RC4, RC5, not so hard to crack

Password Hash Cracking

<u>How Fast Can Passwords Be Cracked?</u>

- Common cracking tools are Optcrack, Jack the Ripper, **Hashcat**…
- Graphics Processing Units (GPUs)
- “Rigs” full of GPUs
- Appliances (Terahash, etc.)
- Clouds, Clusters
- At least 102.8/350 billion password tries/second on a single cracking “rig”
- Any 8-character NT hash password can be cracked in under 2 hours on a “rig” or 12-minutes using $25 of cloud processing power

Password Hash Cracking

How Fast Can Passwords Be Cracked?

- At least 108.2 billion tries/second on a single cracking “rig”

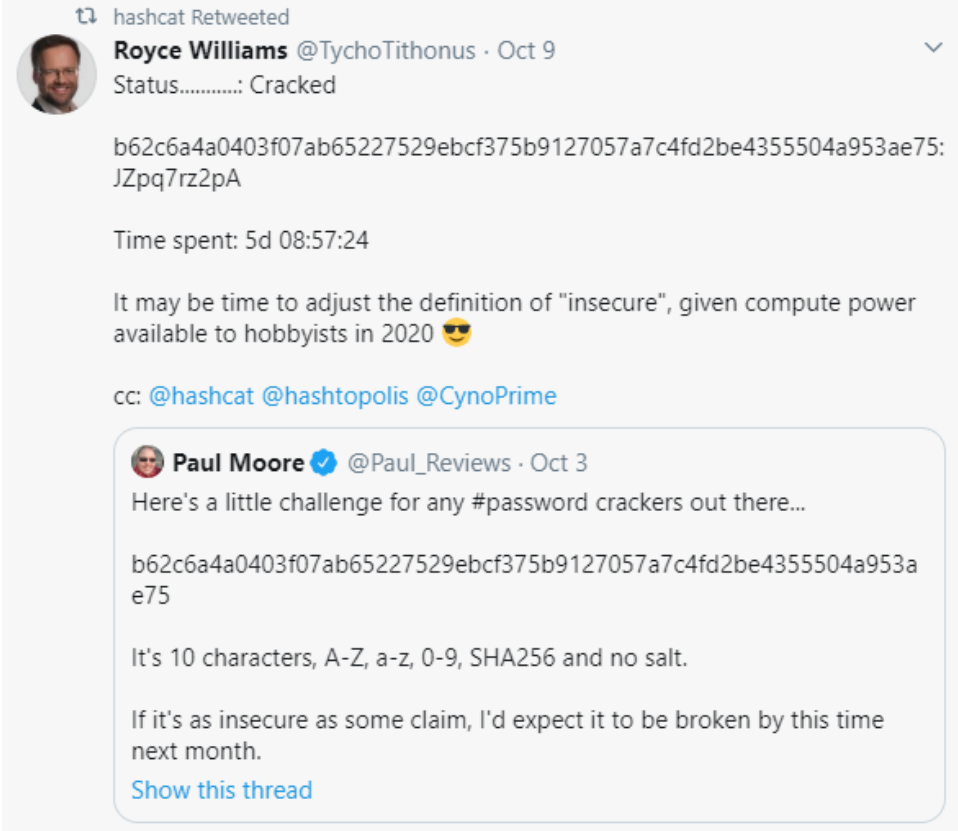
```
C:\Windows\System32\cmd.exe

d:\tools\hashcat-6.0.0>hashcat64 -b -m 1000 -u 1024 -n 512 --opencl-vector-width 8 --force -O

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce RTX 2080 Ti, 2816/11264 MB allocatable, 68MCU

Benchmark relevant options:
===========================
* --force
* --optimized-kernel-enable
* --opencl-vector-width=8
* --kernel-accel=512

Hashmode: 1000 - NTLM

Speed.#1.........:   102.8 GH/s (10.48ms) @ Accel:512 Loops:1024 Thr:32 Vec:8

Started: Wed Feb 13 22:57:19 2019
Stopped: Wed Feb 13 22:57:26 2019

d:\tools\hashcat-6.0.0>_
```

Password Hash Cracking

How Fast Can Passwords Be Cracked?

- 10-character password was cracked in 5 days

https://twitter.com/hashcat


hashcat Retweeted

Royce Williams @TychoTithonus · Oct 9

Status.....: Cracked

b62c6a4a0403f07ab65227529ebcf375b9127057a7c4fd2be4355504a953ae75:JZpq7rz2pA

Time spent: 5d 08:57:24

It may be time to adjust the definition of "insecure", given compute power available to hobbyists in 2020 😎

cc: @hashcat @hashtopolis @CynoPrime

Paul Moore @Paul_Reviews · Oct 3

Here's a little challenge for any #password crackers out there...

b62c6a4a0403f07ab65227529ebcf375b9127057a7c4fd2be4355504a953ae75

It's 10 characters, A-Z, a-z, 0-9, SHA256 and no salt.

If it's as insecure as some claim, I'd expect it to be broken by this time next month.

Show this thread

You need 16-character passwords before you get any cracking "safety" and that's just for now

May already be "broken" by nation state

Password Hash Theft

Password Hash Basics

- Hashes can be used without cracking in many systems, including Microsoft Windows and Active Directory
  - Pass-the-Hash attack tools
    - Mimikatz
    - WinCe
    - NTLMRelay

```
PS C:\Mimikatz\mimikatz_trunk\x64> .\mimikatz.exe

  .#####.   mimikatz 2.1 (x64) built on Mar  5 2017 22:41:35
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:jeff /domain:jefflab.com /ntlm:d4dad8b9f8ccb87f6d6d02d7388157ea
user    : jeff
domain  : jefflab.com
program : cmd.exe
impers. : no
NTLM    : d4dad8b9f8ccb87f6d6d02d7388157ea
  |  PID  4240
  |  TID  5608
  |  LSA Process is now R/W
  |  LUID 0 ; 12663024 (00000000:00c138f0)
  \_ msv1_0   - data copy @ 00000250B30F9B80 : OK !
  \_ kerberos - data copy @ 00000250B316B778
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK

mimikatz # _
```

```
root@kali:~# ntmlrelayx.py -tf victims.txt -c <shellcodehere>
```

Password Hash Theft

Password Hash Basics – Stolen Hashes

Defenses:

- **Prevent attackers from getting the hashes in the first place!!**
- Very long (and complex) passwords can prevent successful cracking
- Use AV/EDR to prevent hacker tools from being used to steal hashes
- Check with individual vendors for their own solutions
  - i.e. Microsoft (e.g. Protected LSASS, etc.)

Password Hash Theft

Password Hash Basics – Stolen Hashes

Defenses: **LET ME SAY IT AGAIN**

- **Prevent attackers from getting the hashes in the first place!!**
- If the attackers have your hashes, they already have the keys to the kingdom
- They already have admin, root, or domain admin access to your environment
- There is nothing they can't do. There is very little you can to do to stop them

Password Attacks

Popular Password Attack Types

Stealing – Lots of Ways:

- Social engineering
- Malware on the endpoint
- Hackers on the endpoint or network
- Network eavesdropping
- Stolen credential databases
- Accidentally left in publicly accessibe “beta” code (e.g. github, etc.)
- Stolen from other compromised site/service where same password is used
- Shoulder surfing

Password Attacks

Popular Password Attack Types

Stealing

- Malware on the endpoint
  - Trickbot is the most common right now

Indeed, Holden shared records of communications from VCPI's tormentors suggesting they'd unleashed Trickbot to steal passwords from infected VCPI endpoints that the company used to log in at *more than 300 Web sites and services*, including:

-Identity and password management platforms Autho and LastPass
-Multiple personal and business banking portals;
-Microsoft Office365 accounts
-Direct deposit and Medicaid billing portals
-Cloud-based health insurance management portals
-Numerous online payment processing services
-Cloud-based payroll management services
-Prescription management services
-Commercial phone, Internet and power services
-Medical supply services
-State and local government competitive bidding portals
-Online content distribution networks
-Shipping and postage accounts
-Amazon, Facebook, LinkedIn, Microsoft, Twitter accounts

Password Attacks

Popular Password Attack Types

Stealing

- Hackers on the endpoint or network
  - Empire PowerShell Toolkit
  - Mimikatz
  - Metasploit

mimikatz 2.2.0 x64 (oe.eo)

```
Authentication Id : 0 ; 173747 (00000000:0002a6b3)
Session           : Interactive from 1
User Name         : Administrator
Domain            : VICTIMMACHINE
Logon Server      : VICTIMMACHINE
Logon Time        : 7/10/2019 4:25:57 PM
SID               : S-1-5-21-1399973682-244801238-2328893529-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : VICTIMMACHINE
         * NTLM     : ae974876d974abd805a989ebead86846
```

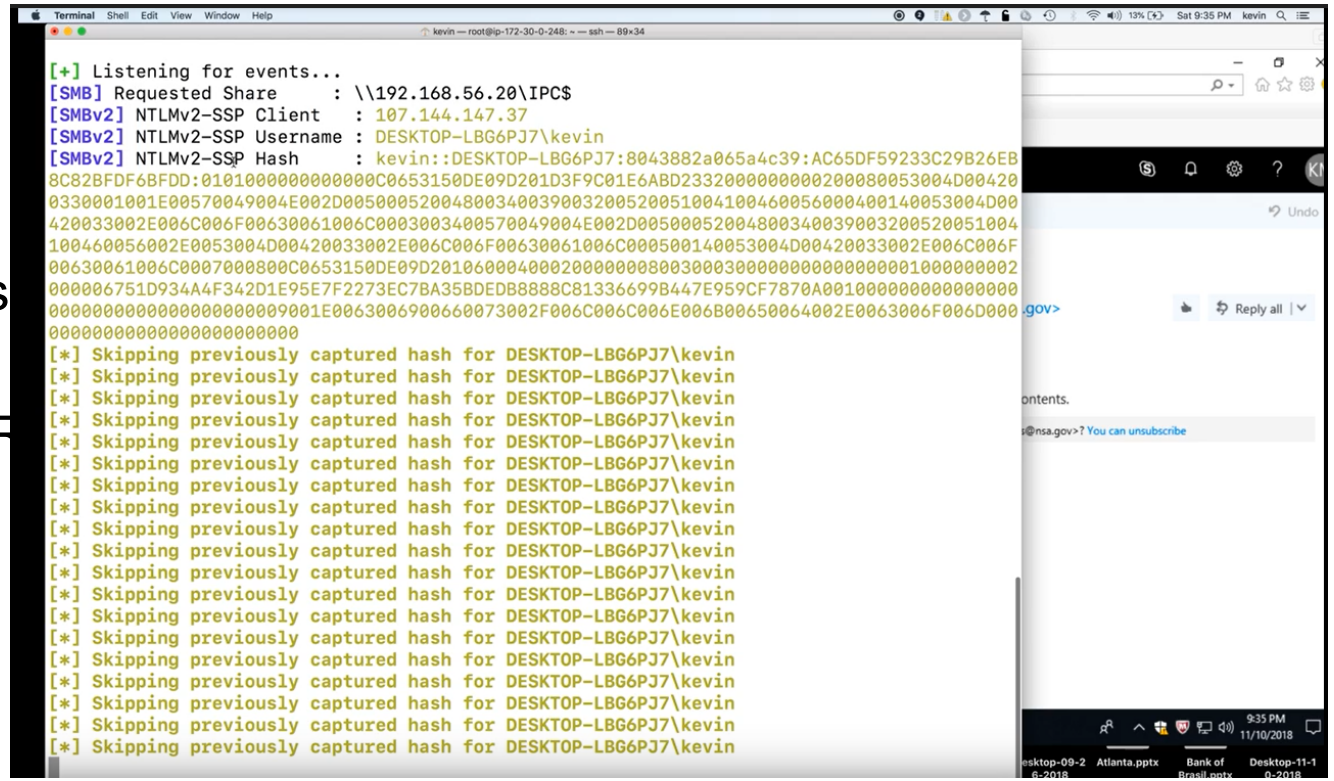
```
=================================================================
 [Empire]  Post-Exploitation Framework
=================================================================
 [Version] 2.5 | [Web] https://github.com/empireProject/Empire
=================================================================

      285 modules currently loaded

      0 listeners currently active

      0 agents currently active

(Empire) >
```

Password Attacks

Popular Password Attack Types

Stealing

- Network eavesdropping
  - Man-the-middle attacks
  - Capturing challenge-response sess
  - Responder hacking tool for one
    - https://github.com/SpiderLabs/R



```
[+] Listening for events...
[SMB] Requested Share      : \\192.168.56.20\IPC$
[SMBv2] NTLMv2-SSP Client   : 107.144.147.37
[SMBv2] NTLMv2-SSP Username : DESKTOP-LBG6PJ7\kevin
[SMBv2] NTLMv2-SSP Hash     : kevin::DESKTOP-LBG6PJ7:8043882a065a4c39:AC65DF59233C29B26EB
8C82BFDF6BFDD:0101000000000000C0653150DE09D201D3F9C01E6ABD23320000000002000800530004D00420
0330001001E00570049004E002D0050005200480034003900320052005100410046005600040014005300 4D00
420033002E006C006F00630061006C000300340057004900 4E002D00500052004800340039003200520051004
100460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F
00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000010000000002
000006751D934A4F342D1E95E7F2273EC7BA35BDEDB8888C81336699B447E959CF7870A0010000000000000000
000000000000000000009001E00630069006600730002F006C006C006E006B00650064002E0063006F006D000
000000000000000000000
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
[*] Skipping previously captured hash for DESKTOP-LBG6PJ7\kevin
```

https://blog.knowbe4.com/kevin-mitnick-demos-password-hack-no-link-click-or-attachments-necessary

Password Attacks

Popular Password Attack Types

Lookups

- Your password, my password, is everywhere!
- Well, there's a good chance some of our passwords are somewhere

- There are billions of logon names and passwords all over the Internet

One Example – Just one password dump collection set

- Collection#1: 770 million email addresses/logon names and password
- Collections#2-5: 2.2 billion records
  - https://www.forbes.com/sites/daveywinder/2019/02/01/2-2-billion-accounts-found-in-biggest-ever-data-dump-how-to-check-if-youre-a-victim/

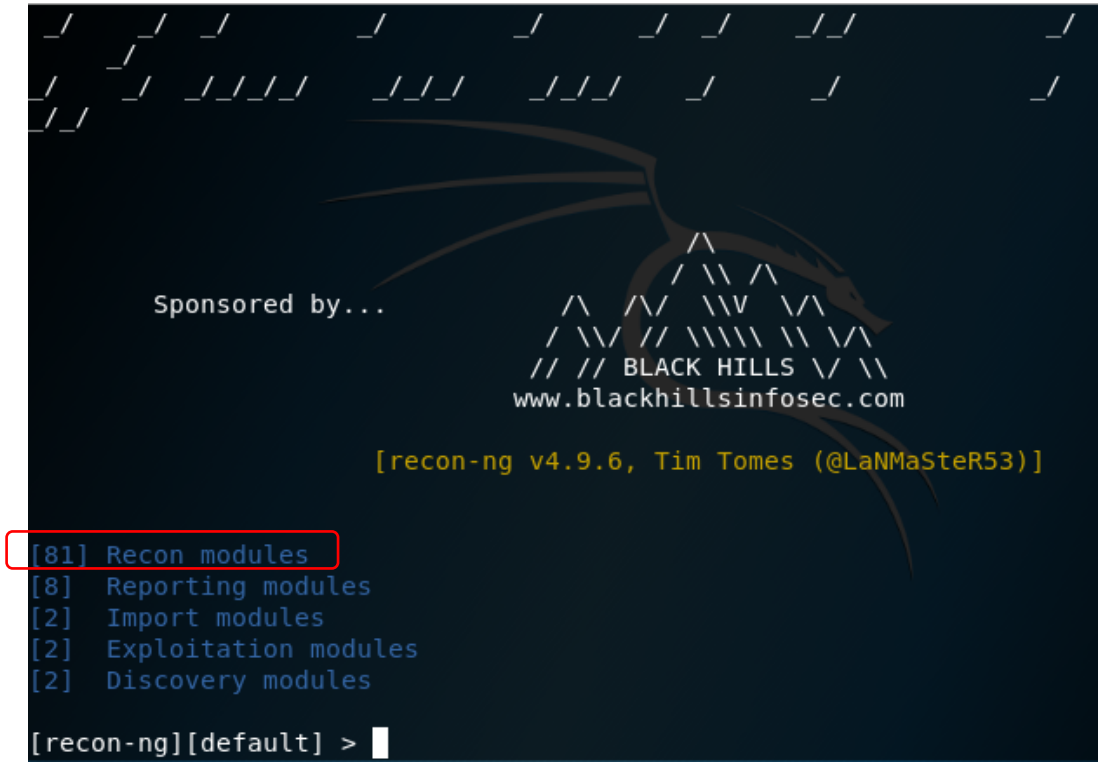
Getting Password Dump Info

Password Dump Retrieval Tools:

- There are dozen of OSINT tools hackers can use to find stolen passwords
- Example: Recon-ng

```
recon/domains-credentials/pwnedlist/account_creds
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_creds
recon/domains-credentials/pwnedlist/domain_ispwned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump
```

```
recon/contacts-credentials/hibp_breach
recon/contacts-credentials/hibp_paste
```



Checking to See if Your Password Has Been Stolen

Attackers Can Buy/Get It:

- There are hundreds of databases with your email address (and password) for sale on the Internet and darkweb

Defenses:

Research your own passwords availability on the Internet and dark web

- www.knowbe4.com/resources - Password Exposure Test
- Sites like: https://haveibeenpwned.com/
- Password managers like 1Password

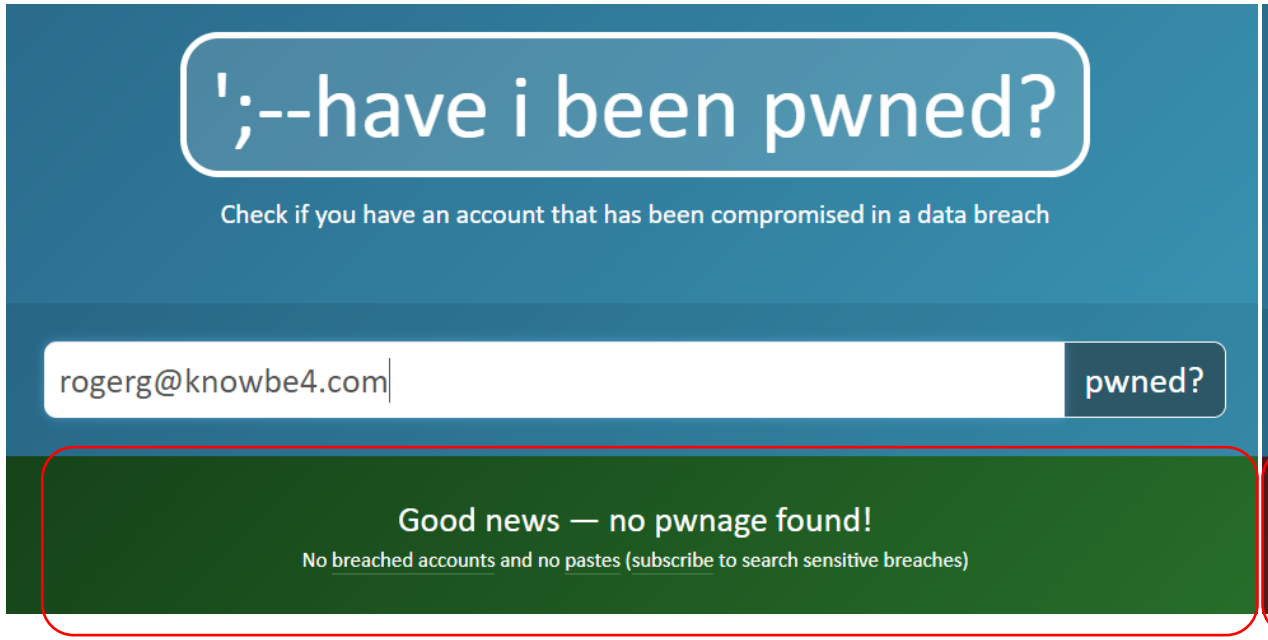
Password Exposure Test

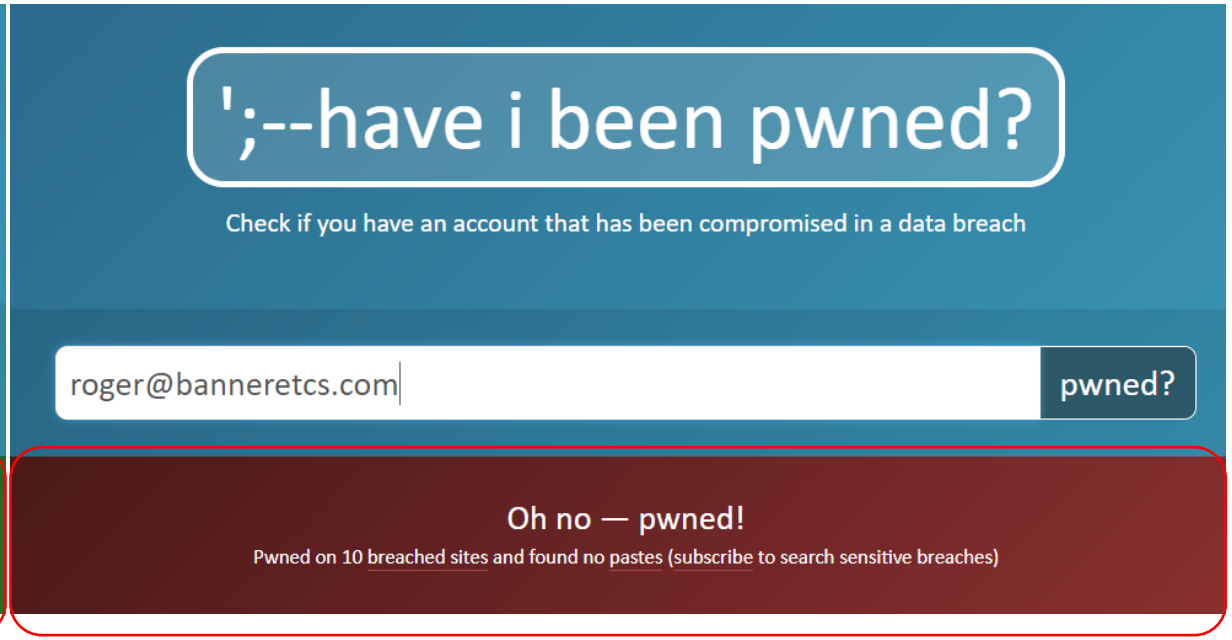
Checking to See if Your Password Has Been Stolen

<u>Attackers Can Buy/Get It:</u>

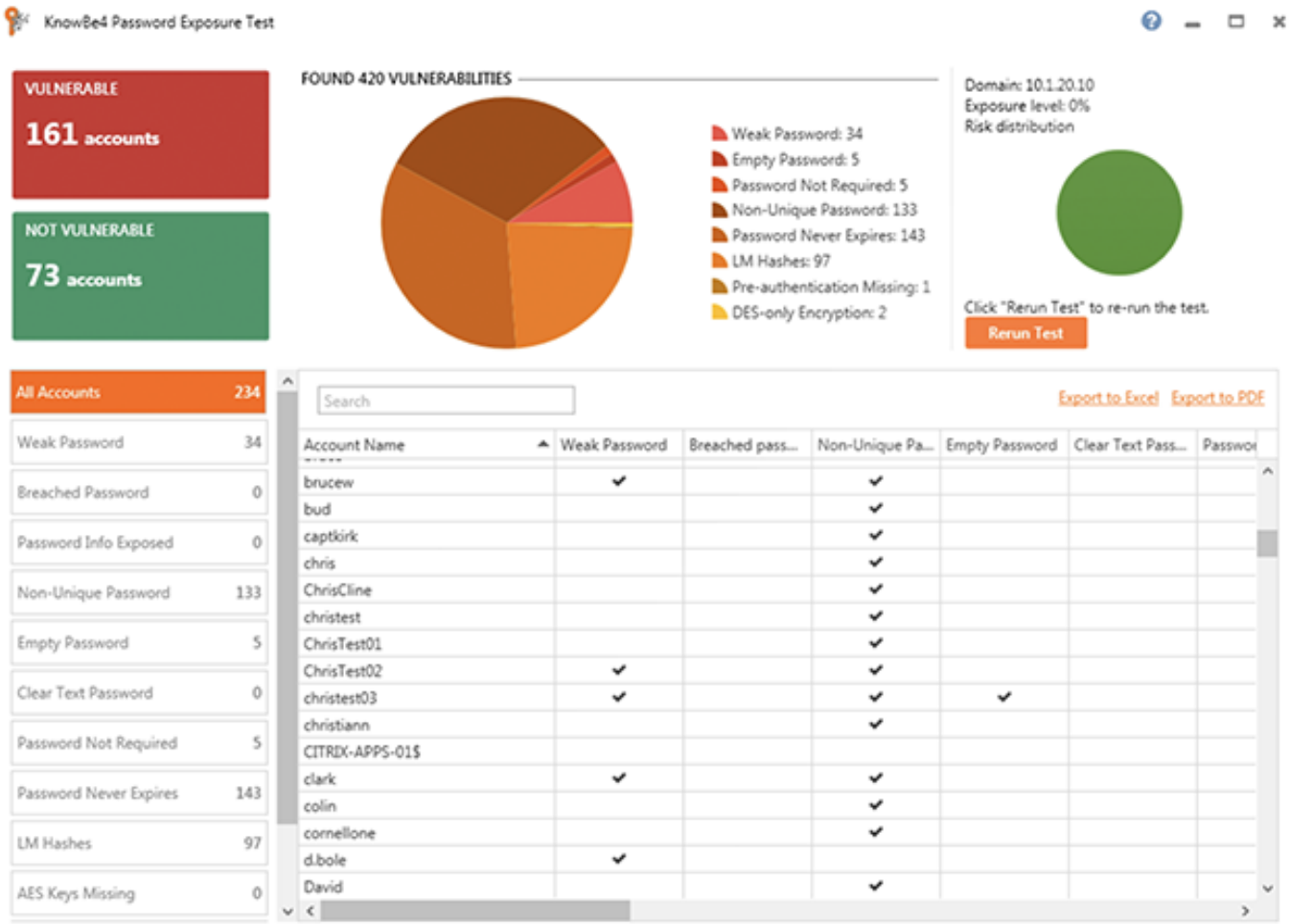
Protecting Yourself/Org

- https://haveibeenpwned.com





Password Exposure Test



Here's How the Password Exposure Test works:

- Checks to see if your company domains have been part of a data breach that included passwords
- Tests against 10 types of weak password related threats
- Checks against breached/weak passwords currently in use in your Active Directory
- Reports on the accounts affected and does not show/report on actual passwords
- Just download the install, run it, with results in minutes!

Requirements: Active Directory, Windows 7 or higher (32 or 64 bit) NOTE: the analysis is done on the workstation you install PET on, no confidential data leaves your network, and actual passwords are never disclosed.

» Learn More at www.KnowBe4.com/Resources «

Password Attacks

<u>Popular Password Attack Types</u>

Account Takeover Recoveries

- Account password reset methods can be used by hackers to take over people's accounts

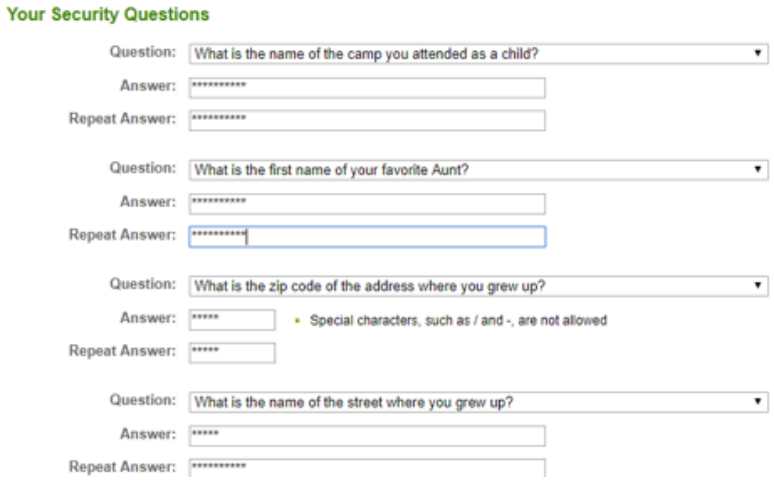
Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

- Password Reset Questions

  The worst recovery method on the planet is password recovery questions

  - Usually REQUIRED by many web sites, you can't create a new account without them



Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

Problem: Answers can often be easily guessed by hackers

Great Google paper called *Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google*

http://www.a51.nl/sites/default/files/pdf/43783.pdf

- 20% of some recovery questions can be guessed on first try by hacker
- 40% of people were unable to successfully recall their own recovery answers
- 16% of answers could be found in person's social media profile

- Attack has been involved in many well known attacks (e.g. Sarah Palin's compromised email)

Rogue Recoveries

Defense

Defense: Never answer the questions with the real answers!

Question: What was your high school mascot?

Answer: pizzapizza$vgad2@M1

Repeat Answer: **********

Question: What is your mother's middle name?

Answer: **********

Repeat Answer: **********

Question: What is your father's birthdate? (mmdd)

Answer: **********

Question: What is the name of your best friend from high school?

Answer: **********

Repeat Answer: **********

Unfortunate that means you have to record them somewhere else just like passwords (password managers help with this)

Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

SMS Recovery Hack - Steps

1. Hacker sends you a text pretending to be from your email provider asking for your forthcoming SMS PIN reset code

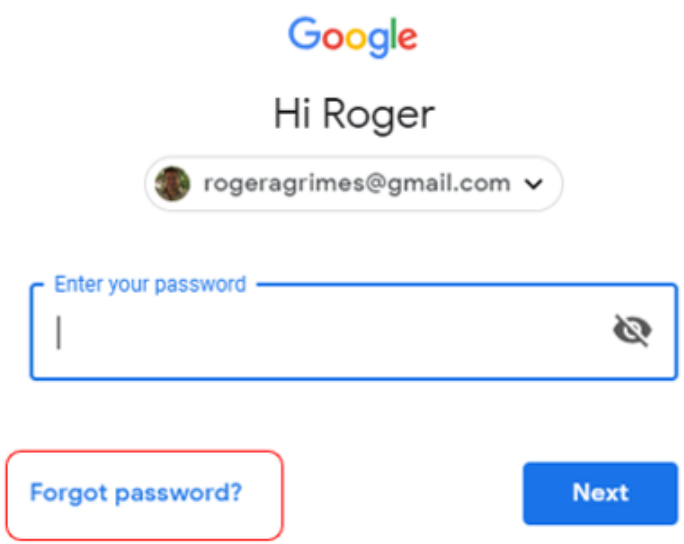
> From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

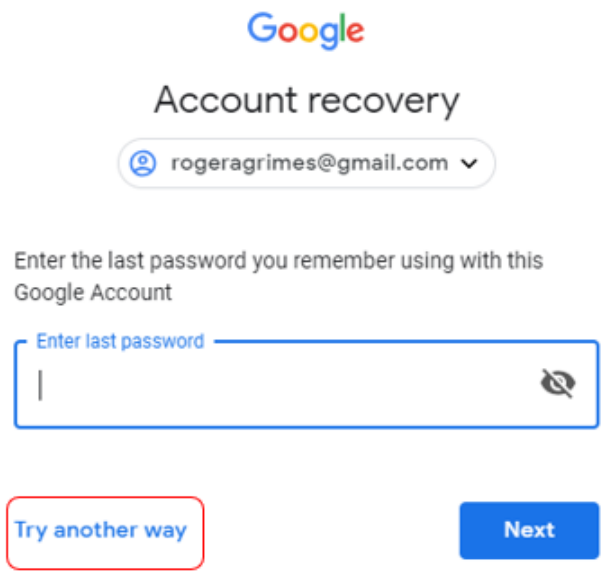
Rogue Recoveries

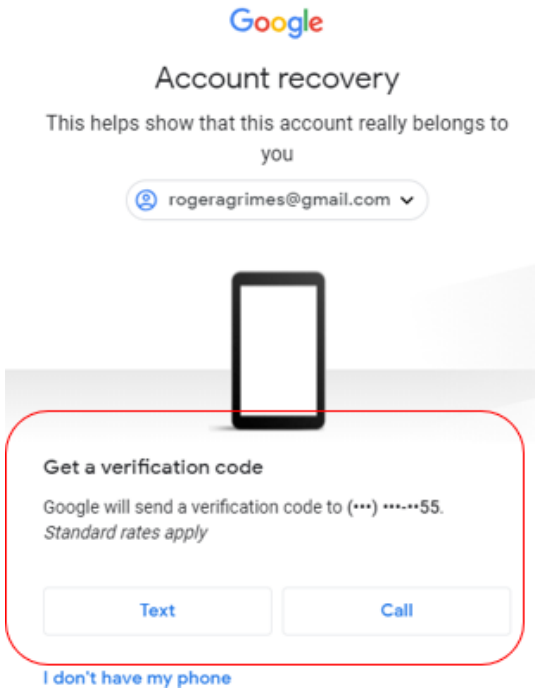
Hacking Into Your Email Using Recovery Methods

SMS Recovery Hack - Steps

2. Hacker forces your email account into SMS PIN recovery mode





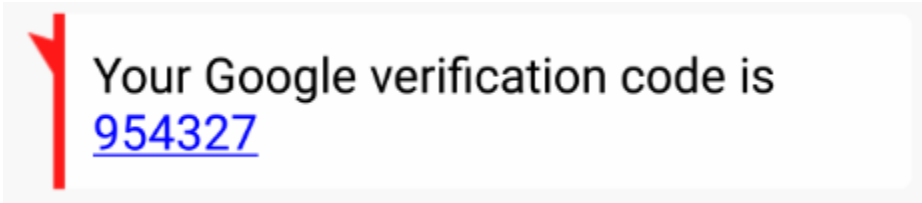


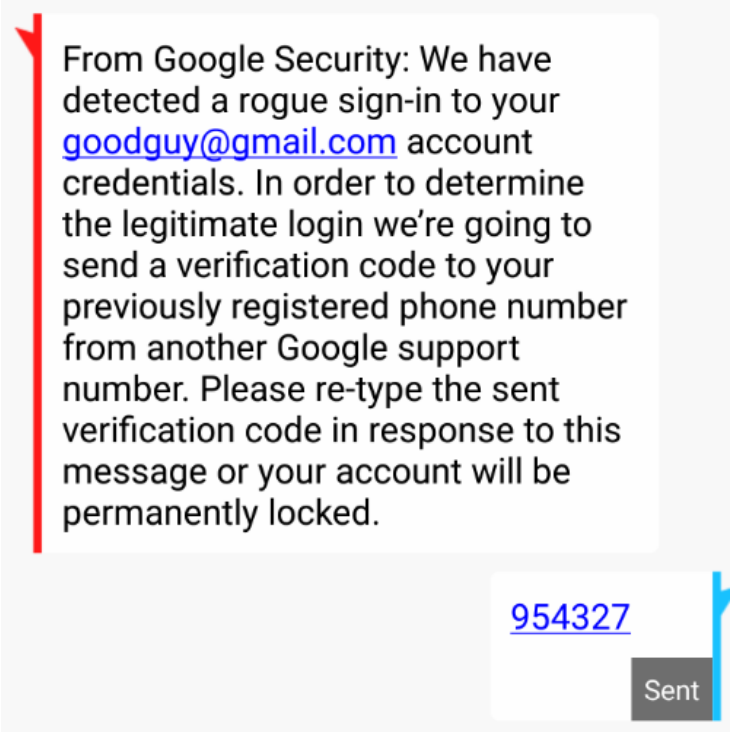
Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

SMS Recovery Hack - Steps

3. You get text from vendor with your reset code, which you then send to other number





Password Attacks

Popular Password Attack Types

Ask For It

- You'd be amazed how many people give up their passwords to strangers who ask for them
- I've often asked people for their passwords
- Jimmy Kimmel password video: https://www.youtube.com/watch?v=opRMrEfAIiI

Agenda

- Problems with Passwords
- Types of Password Attacks
- Password Policy Recommendations

Password Policy

How Effective is a Password Policy?

- Most hacker attacks do not care about your password policy
  - 70-90% of all malicious breaches are due to social engineering
  - 20-40% are due to unpatched software
  - Every other attack type, including password attacks, added up all together, only accounts for 1% - 10% of your risk
  - https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks
- Password policy only impacts authentication attacks
- And even then, only attacks against password guessing and cracking
- Most organizations would be far better off spending more time stopping social engineering and patching better than worried about password policy
- But with that said, yes, a good password policy can only help

Password Policy

<u>Password Guessing vs. Cracking</u>

- Guessing is done usually against an active service
  - Account lockout can be enabled
  - Attackers can't guess that quickly
  - Even in the best attacker scenario, an attacker can only guess thousands to millions of times
  - Monitoring and alerting can help mitigate
- Cracking is usually against already stolen password hashes
  - No "logon defense" is going to stop a hacker from trying billions and trillions of guesses
  - Only defense against cracking a password once it has been stolen is very long and complex passwords

Password Policy

<u>Password Policy Components</u>

- Length
- Complexity (i.e. character types/sets required)
- Useful lifetime/expiration period
- How long till password can be re-used in same system by same person
- Account Lockout enabled/disabled
- Rules (such as “Can’t be a “common” password or can’t be your logon name)

- Don’t forget: You must protect the involved components!!

Password Policy

Password Policy Components

- When people say a password is “strong” they usually mean the password has appropriate length and complexity to withstand most password guessing attacks, but “strength” is really a factor of all involved components
- One weakness and the whole thing falls

NIST Password Policy

National Institute for Standards and Technology (NIST)

- Considered the most respected authority on password policy and recommendations for decades
- What they recommended decades ago is what most organizations and people still follow today for password security

NIST Special Publication 800-63
Version 1.0.2

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Electronic Authentication Guideline

Recommendations of the National Institute of Standards and Technology

William E. Burr
Donna F. Dodson
W. Timothy Polk

Password Policy Debate "Eruption"

NIST SP 800-63

Digital Identify Guidelines

- Special Publication 800-63
- https://www.nist.gov/itl/tig/projects/special-publication-800-63
- Significantly updated in June 2017
- **Said based on two decades of data collection around password attacks, NIST was wrong about previous advice, do the opposite**
- Recommends MFA when it can be used to protect valuable data
- **Recommends not requiring complexity, long length, or regularly forced password changes**
- Recommends "blacklisting" common passwords to stop easy guessing attacks

Ignoring NIST

Industry Response to NIST SP 800-63 Recommendations?

Over three years later:

- Most people and organizations don't know about it
- Almost no one actually uses it
- Almost no one CAN use it!
- Almost no security regulation or guide (e.g. PCI-DSS, HIPAA, NERC, SOX, etc.) follows or allows it
- You will fail an audit check if you follow it
- The most progressive policies (e.g. Microsoft, etc.) simply don't recommend anything and leave it up to you now

Which Password Attack Types…

Don't Care About "Strong" Passwords?

- Social Engineering
- Stealing
- Lookups
- Account Takeover (ATO) Recoveries
- Asking

The vast majority of password attacks are this type

Are Impacted by "Strong" Passwords?

- Guessing
- Hash Cracking
  - (but does not stop hash reuse and it's already game over anyway)

Which Password Attack Types?

Don't Care About "Strong" Passwords

- Social Engineering
- Stealing
- Lookups
- Account Takeover (ATO) Recoveries
- Asking

Are Mitigated by "Strong" Passwords

- **Guessing**
- Hash Cracking
  - (but does not stop hash replays and it's already game over)

IMHO, So it's really just guessing attacks

Which Password Attack Types?

Are Mitigated by “Strong” Passwords

Cracking

- But there are scenarios where real strong passwords are protective:
- If attackers crack your password hash, they can re-use on logons that only accept plaintext logons
- Attacker has captured password hash credentials in one AD forest/website/service and relies on the fact that people often re-use the same passwords in another forest/website/service, and getting the plaintext equivalent allows them to then more easily break into other locations
- **These are not very common scenarios but they do happen**

Password Policy

What is a “Strong” Password?

- Want your passwords to be not easily guessable?
  - 8+ characters and not a commonly used password is usually strong enough
  - Especially if account lockout is enabled
- Want your passwords to be un-crackable?
  - Must resist hundreds of trillions of guesses
  - Requires a much longer and/or complex password
  - Requires 16+ characters and/or complexity and increases every year
- Account lockouts help prevent guessing attacks, but not cracking attacks

- The central risk dilemma is as you strengthen password requirements to prevent successful cracking, it makes it tougher for users to remember and use, and increases risk of attacks from non-guessing/cracking attacks because of password reuse

Password Policy

<u>What is password complexity?</u>

- It's known as *entropy*…randomness of something
  - Traditional password theory follows something called "Shannon entropy" guidelines
- Truly random passwords are hard for humans to make and remember
- What we think is a complex password
  - RogerisaG0on
  - RogerGrimes3
- What truly random, high entropy, passwords look like
  -]}7Y?@w@?)Nmt4h7
  - J.MF.F)RGzHk4y}x
  - CYADB_d},R->Z>C2

Password Policy

Problem with Complexity?

- Really hard to require true randomness/high entropy
- Humans like to use easier to remember patterns and root words
- The average human-generated complex password is:
  - Uppercase first letter
  - Lowercase second letter which is a vowel
  - If number required, 1 or 2 at end
  - If symbol is required, it's likely a @ or ! or # or $ or &
- Ex: Rogerishere2 or R0gerg
- Did I describe some of your passwords?
- Harder to guess but not that hard to crack

Password Policy

Length vs. Complexity

- Simple complexity (Rogergri2) beats password guessers, especially if account lockout is enabled
- Need high entropy to beat password crackers and that is hard for human-derived passwords
- Length adds undeniable entropy
- When humans are involved, consider using longer length over requiring complexity
- Works just as well security-wise, but easier for people to remember
- Passphase (ex. rogerjumpedoverthedogandcat)

Password Policy

Length vs. Complexity

- How long to crack the hashes of these passwords?

Rogergri2

It would take a computer about
3 DAYS
to crack your password

]}7Y?@w@?)Nmt4h7

It would take a computer about
41 TRILLION YEARS
to crack your password

rogerjumpedoverthedogandcat

It would take a computer about
4 QUINTILLION YEARS
to crack your password

Both are hard to hack, but which is easier to remember and use?

Using https://howsecureismypassword.net/

Password Managers

Password Managers

- The best password to fight all attack types is a very long and complex password
- But requiring a human to do it can be self-defeating
  - So says NIST SP 800-63
- Instead, if you need truly long and complex passwords, try to use/require a password manager instead
- Password managers allow a different long and complex password to be used on most web sites and services
  - Just a keystroke combination or few clicks of a mouse to logon
  - Autologon

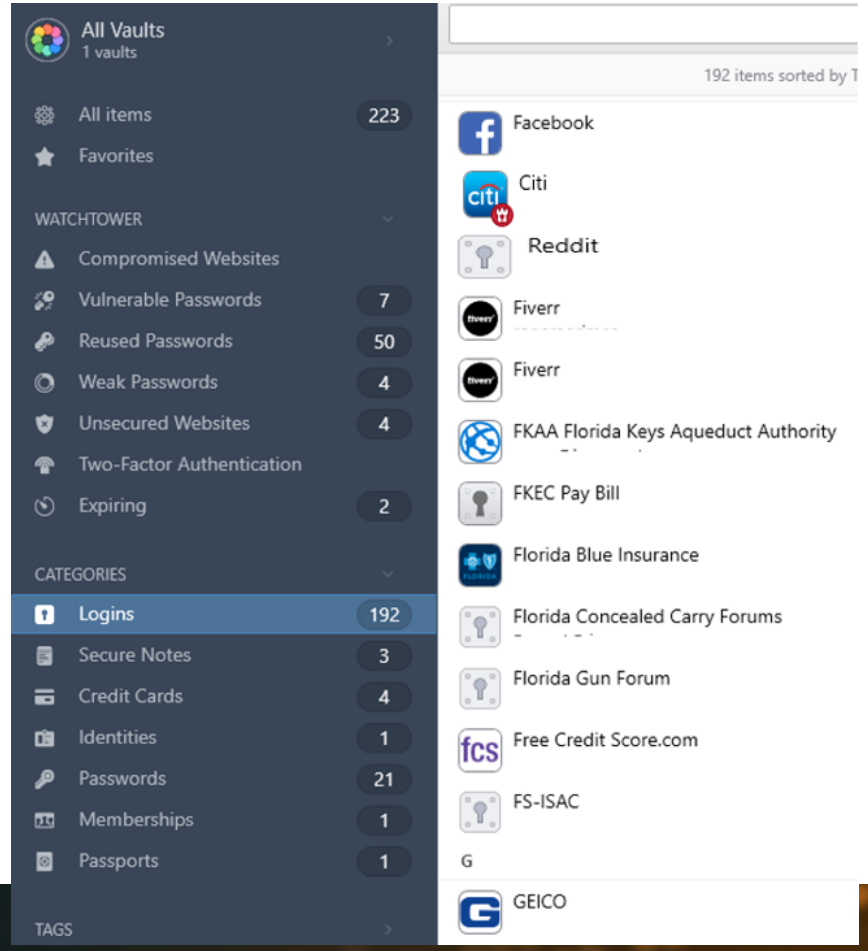
Password Managers

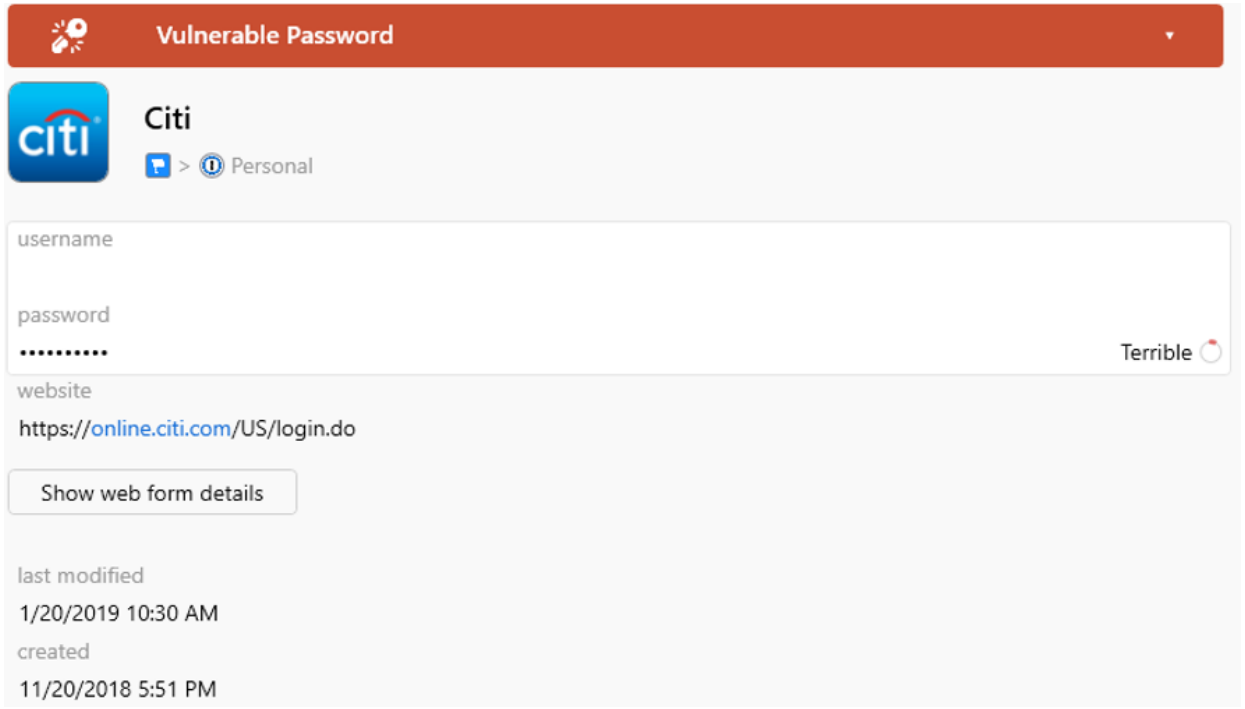
Password Managers

- Create and store and allow easy use of long and complex passwords
- Most have many other features
- Free and commercial
- A few allow enterprise management
- Many very good password manager programs out there
- My recommendation: Use one that has been out for a long time and has many "real" reviews
- Check out: https://www.wired.com/story/best-password-managers/

Password Managers

Password Managers





Password Managers

Password Managers

Negatives

- Don’t work with all devices, browsers, or sites/services
- One stop shop for hackers and malware that are looking to get your passwords
- Can be buggy
- Can be tough to use until you get use to it
- Seems every other website has a different password policy…it’s a pain
- Single point of failure
- https://www.csoonline.com/article/3325326/password-security/using-a-password-manager.html

MFA

Multifactor Authentication

- Significantly mitigates some types of hacker attacks
  - Especially broadcast phishes asking you to logon with a password

Negatives

- Can’t be used on most sites/services
- Can be hacked, sometimes easily so
- If you use MFA, you must train users about how they can still be hacked, including attacks against their type of MFA and how to avoid

Hacking MFA

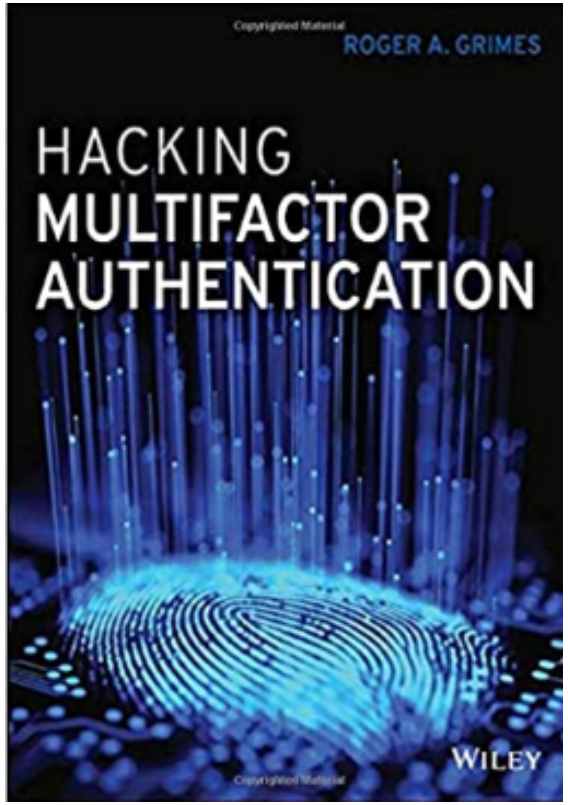
Free Hacking MFA Resources

- Hacking MFA e-book, webinar, whitepaper
- https://www.knowbe4.com/how-to-hack-multi-factor-authentication
- Multifactor Authentication Security Assessment
- https://www.knowbe4.com/multi-factor-authentication-security-assessment

Hacking MFA

Multifactor Authentication

- Covers over 50 ways MFA can be attacked
- Discusses all MFA types, strengthens and weaknesses
- Hundreds of examples
- Picks MFA winners and losers
- Tells you how to pick out the best MFA solution



https://www.amazon.com/Hacking-Multifactor-Authentication-Roger-Grimes/dp/1119650798

Password Policy Advice

Password Policy Recommendations

Everyone's password policy advice is all over the place and most don't agree with each other

- You must decide what your risk tolerance is and what meets requirements
- **Core decision: How much are you worried about password cracking?**
- Most of the other risks can be put down by using non-easily-guessable passwords
- To prevent cracking, you have to go much longer and/complex
  - And when you do that, you risk increasing all the other password attack types risk
- It's often not binary
- You can have different policies for different logins and groups of people (users, admins, etc.)

My Password Policy Advice

My Password Policy Recommendations

- Use MFA when you can and where it makes sense
  - Not all logons need MFA protection
  - Ensure that you educate everyone that MFA can be hacked and how
- If a password manager can be used, use long and very complex passwords
- If a password manager can't be used, use at very least longer passwords (8-12+ characters), maybe a passphrase if concerned about cracking
- Enable account lockout (at any value, but much debate over)
- Don't re-use passwords between any website or service
- Do not use easily guessable passwords (e.g. password2, 12345678, etc.)
- Change passwords at least once a year, possibly more often for corp orgs

My Password Policy Advice

My Password Policy Recommendations

The vast majority of password hacking risk is eliminated by:

- Passwords are 8-characters or longer
- Enable account lockout
- Don't re-use passwords between any website or service
  - How to enforce is the question…education
- Do not use easily guessable passwords (e.g. password2, 12345678, etc.)
- Change passwords at least once a year, possibly more often for corp orgs

- And if you want the extra protection against hash cracking, do all the other stuff

Password Policy

<u>Monitoring and Alerting</u>

- Alert for an abnormal # of failed logins in a given time period
  - For a single account
  - In aggregate
  - For an unusual number of accounts (stops credential stuffing attacks)
- Alert for an abnormal # of account lockout warnings
- Alert on strange network logon pathway flows
  - Logons for devices that don’t normally logon to other devices

Password Policy

Other Checks

- Do account credential hygiene
  - Remove the accounts you don't need
  - Put MFA and/or strong passwords on the ones you do need
  - Reduce permanent memberships of privileged groups to as near zero as you can
  - Enable "check-out" methods and monitoring of elevated accounts
- Secure any remotely accessible APIs
  - They often don't have account lockout, allow MFA, or are monitored as closely
- Do an account audit to ensure that all existing (active) accounts have strong passwords
  - It's easy for older accounts to somehow get bypassed or not follow the newer policies
  - Check those interfaces and legacy systems

The KnowBe4 Security Awareness Program WORKS

Baseline Testing
Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

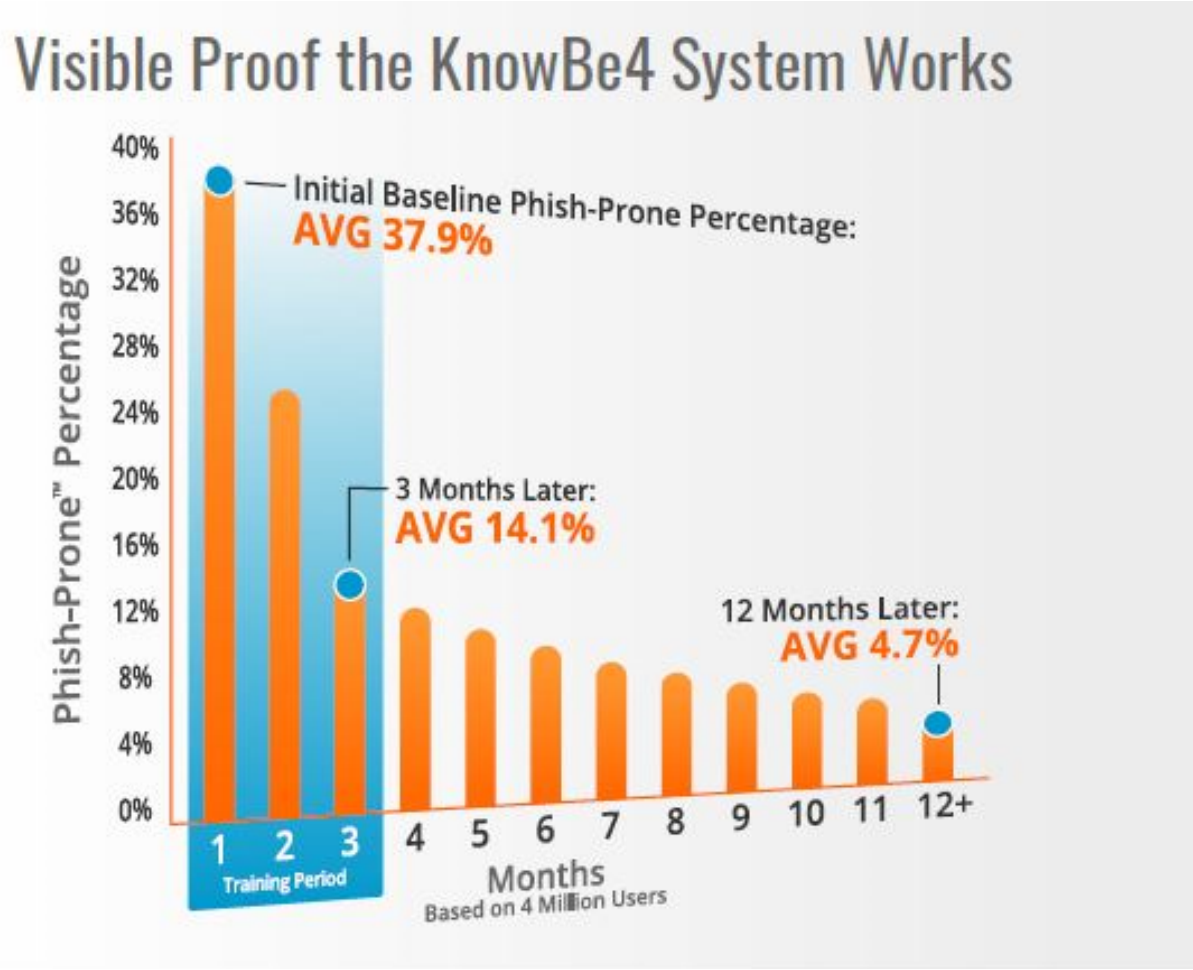
See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

Security Awareness Training Program That Works

- Drawn from a data set of **over four million users**
- Over **17K organizations**
- **Over 9.1M** Simulated Phishing Campaigns

- Segmented **by industry type** and **organization size**

https://info.knowbe4.com/phishing-by-industry-benchmarking-report

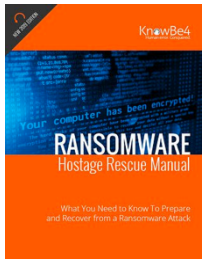


Resources

Free IT Security Tools

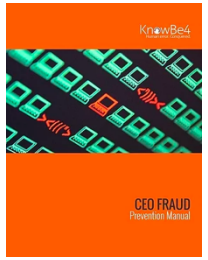
- Domain Doppelgänger
- Awareness Program Builder
- Domain Spoof Tool
- Mailserver Security Assessment
- Phish Alert
- Ransomware Simulator
- Weak Password Test
- Phishing Security Test
- Second Chance
- Email Exposure Check Pro
- Training Preview
- Breached Password Test

Whitepapers



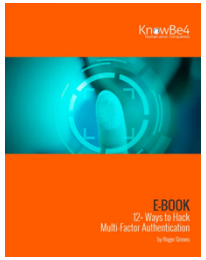
Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.



CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.



12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

» Learn More at www.KnowBe4.com/Resources «

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/