KnowBe4
Human error. Conquered.

A Master Class on Cybersecurity: Roger Grimes Teaches Password Best Practices

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

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

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

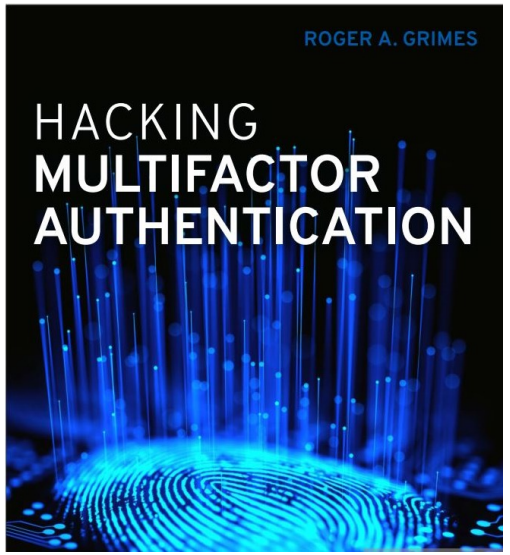
About Roger

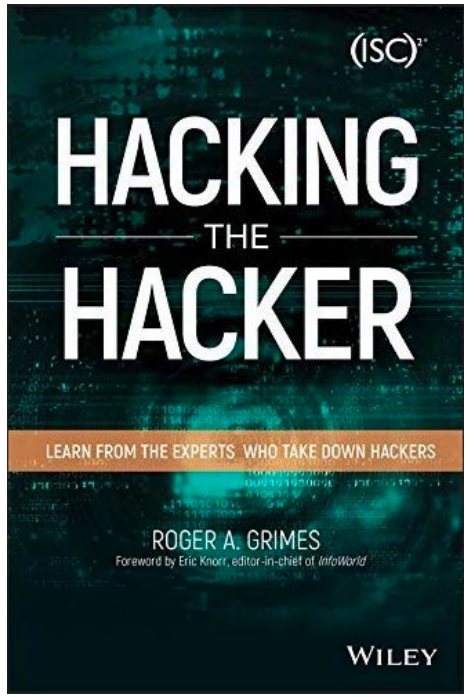
- 34 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,200 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)

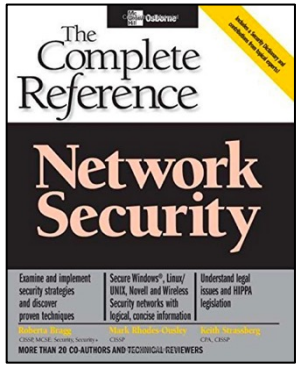
Certification exams passed include:

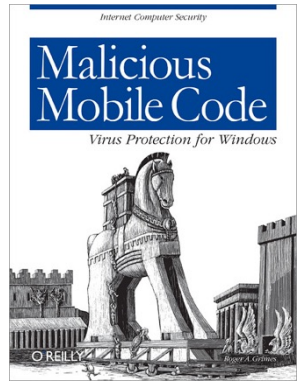
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

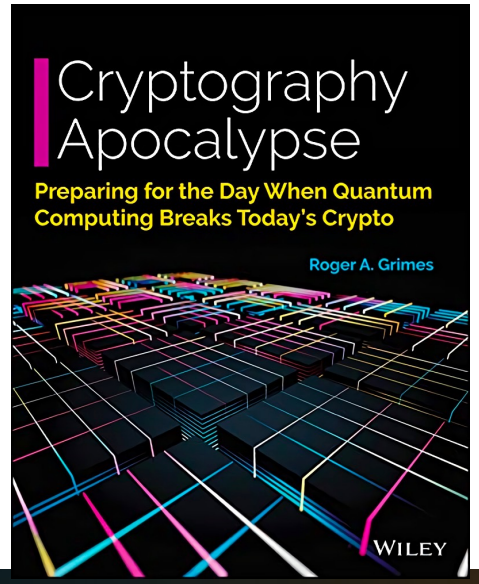
Roger's Books

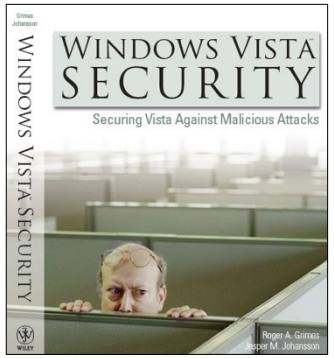


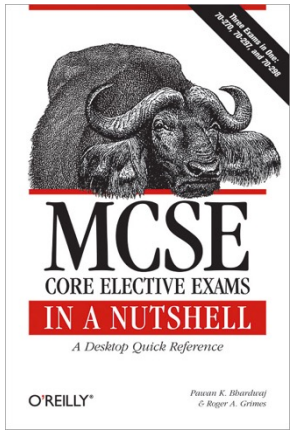


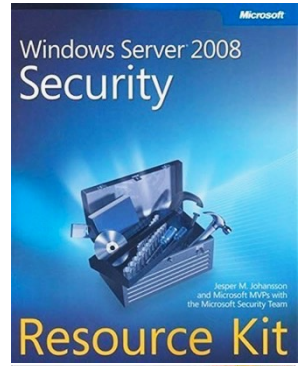


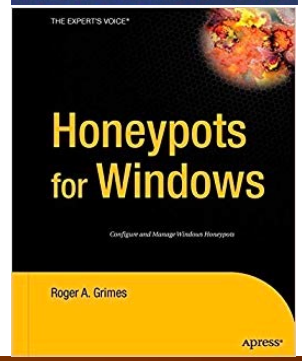












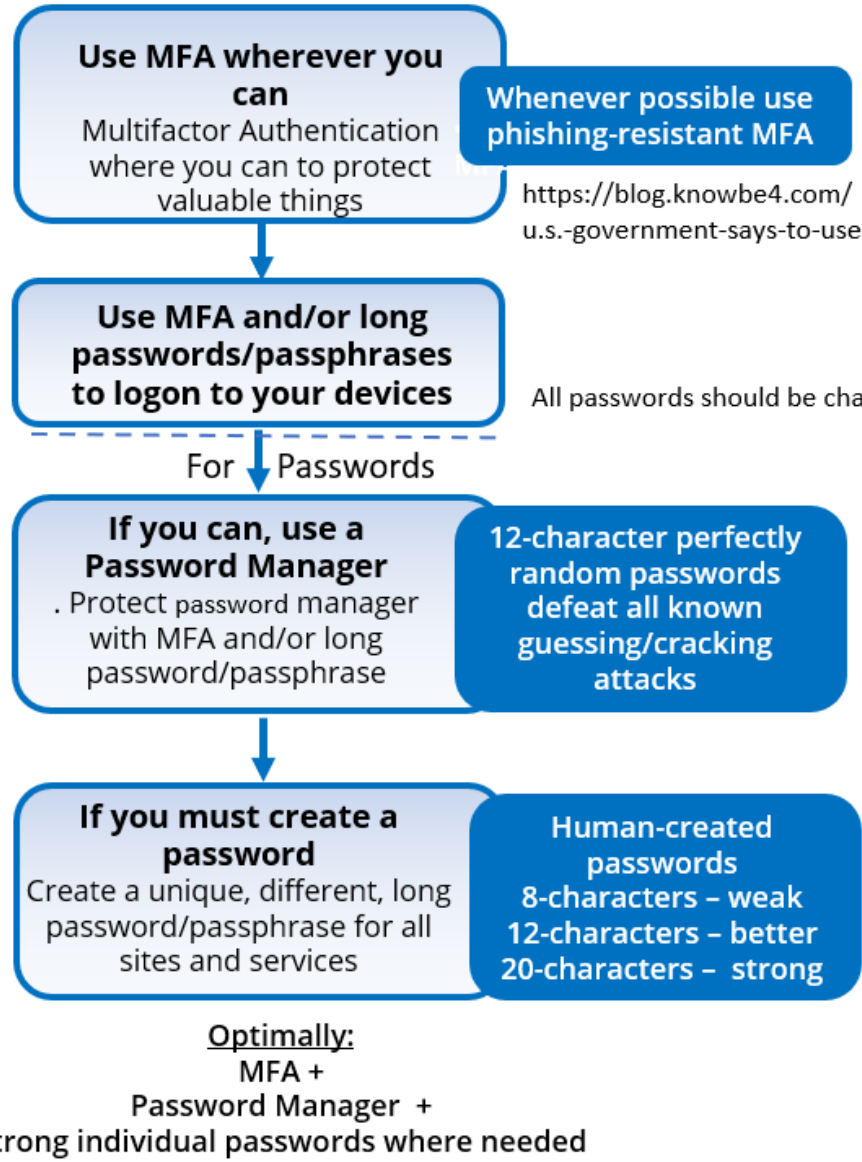
About Us

- Provider of the world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

Agenda

- Types of Password Attacks and Defenses
- Password Policy Recommendations

Password Policy
Practical Implementation



Optimally:
MFA +
Password Manager +
Strong individual passwords where needed

For more detail: https://info.knowbe4.com/wp-password-policy-should-be

Problems with Passwords

- Biggest password problem and risk today
- The average person has to logon to 170+ websites and only has 3 to 19 passwords
- This means one compromise able to leverage other compromises more easily

Passwords Will Be With Us For a Long Time

- If you added up all the password alternatives in the world they don't work on 2% of the world's sites and services
- Average person has more than ever
- Passwords are used in many scenarios beyond user use:
  - Networks
  - Computers/Devices
  - Services/daemons
  - Applications
  - Interfaces

https://www.linkedin.com/pulse/passwords-still-us-decades-roger-grimes

Agenda

- Types of Password Attacks and Defenses
- Password Policy Recommendations

Password Attacks

In General, They Can Be Categorized Into

- Password theft
- Password guessing
- Password hash theft and cracking
- Unauthorized password resetting or bypass

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 accessible “beta” code (e.g., GitHub, etc.)
- Stolen from other compromised site/service
- Shoulder surfing

Password Attacks

Popular Password Attack Types

Social Engineering

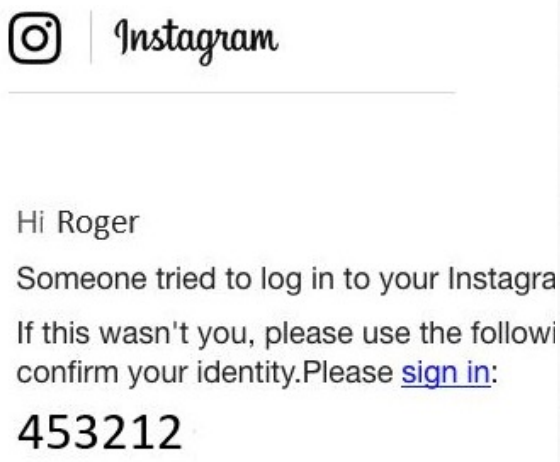
- One of the most common ways to get passwords
- Email, websites, SMS, IM, social media, phone call, etc.

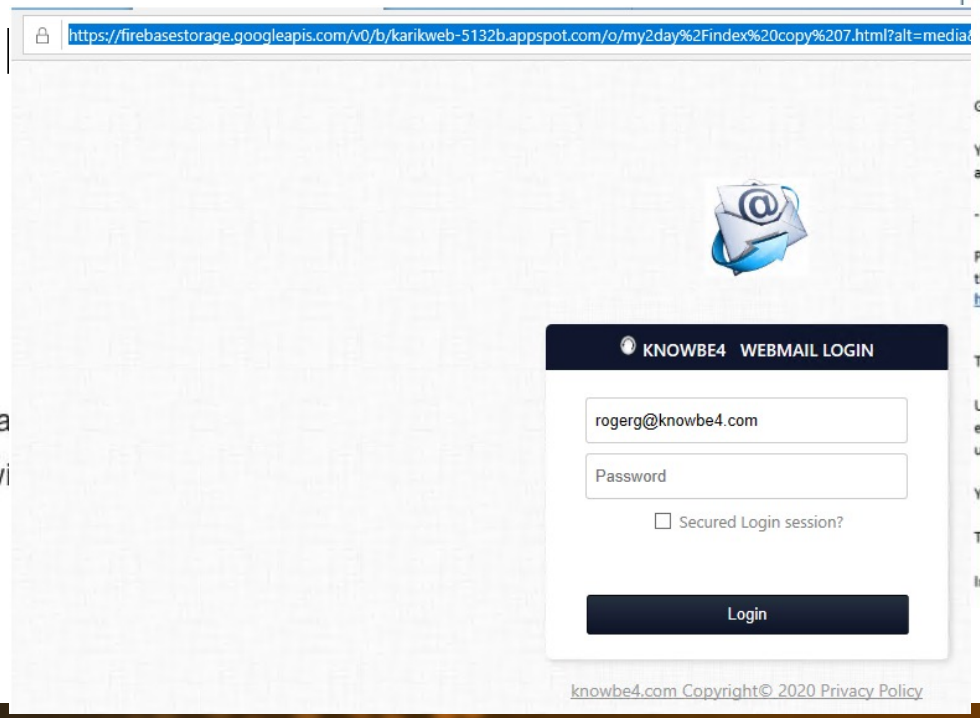
Password Attacks

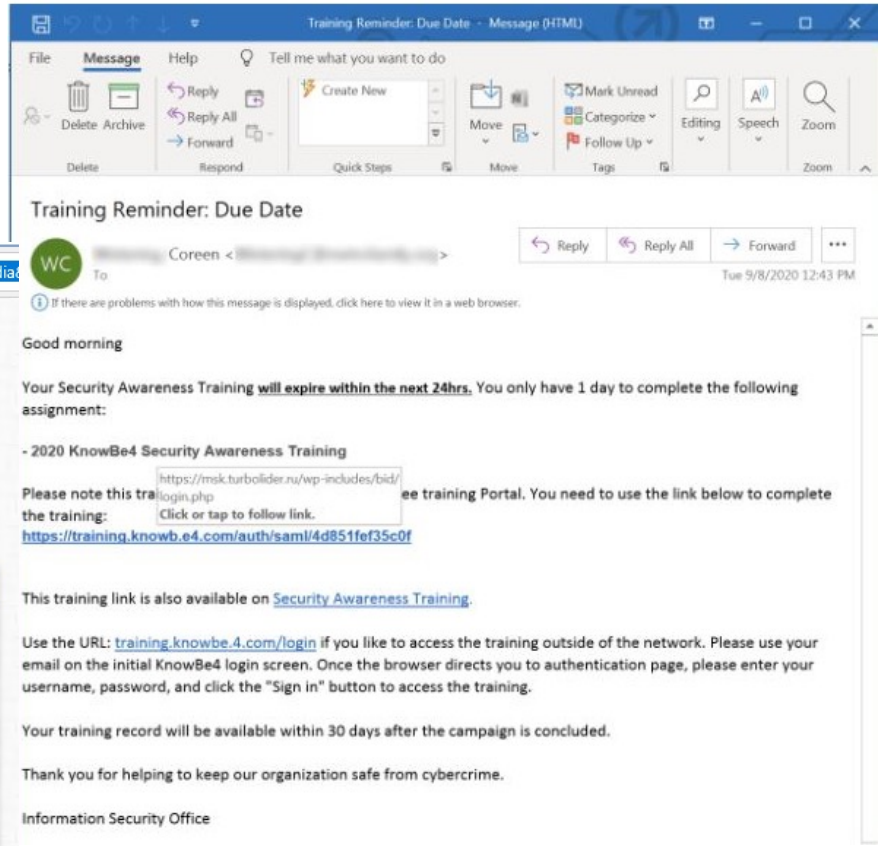
Popular Password Attack Types

Social Engineering

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







Password Attacks

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:

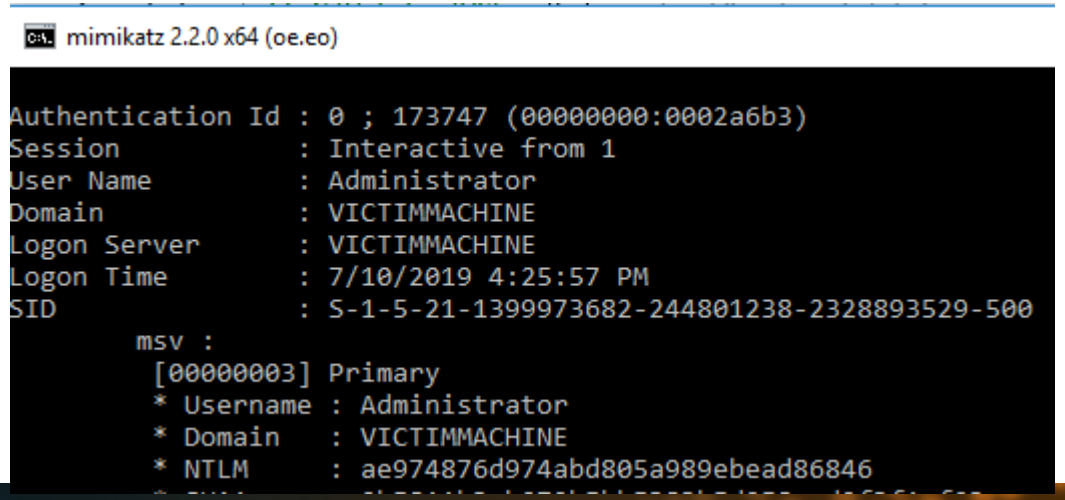
-Identity and password management platforms Autho and LastPass
-Multiple personal and business banking portals;
-Microsoft Office365 accounts
-Direct deposit and Medicaid billing portals
-Cloud-based health insurance management portals
-Numerous online payment processing services
-Cloud-based payroll 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

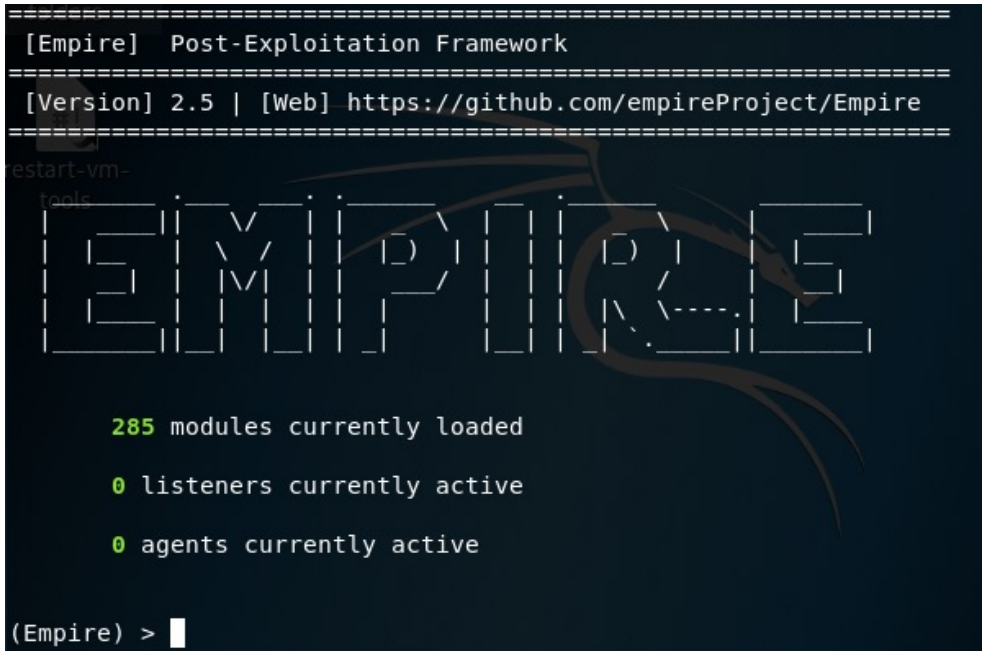
Password Attacks

Popular Password Attack Types

Stealing

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



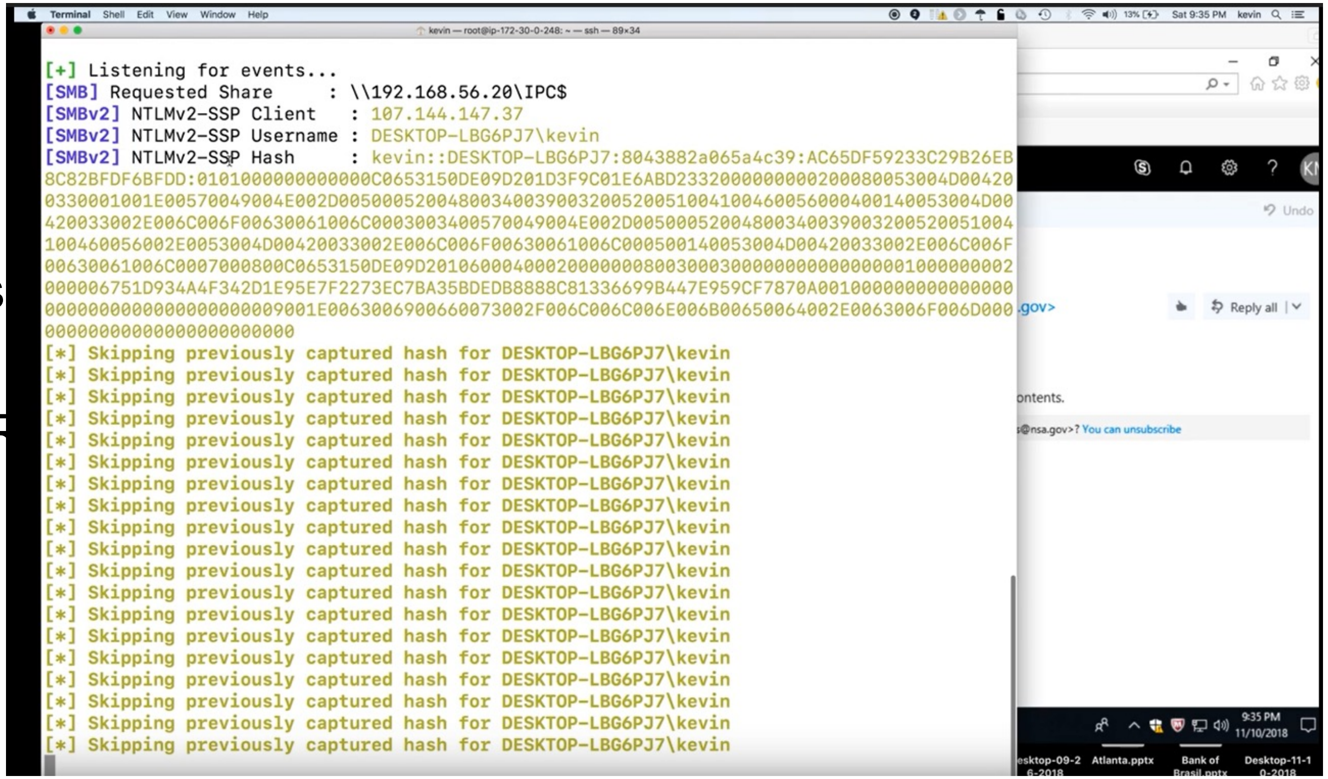


Password Attacks

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



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

Password Attacks

Popular Password Attack Types

GitHub Attacks

How corporate data and secrets leak from GitHub repositories

Attackers constantly search public code repositories like GitHub for secrets developers might inadvertently leave behind, and any tiny mistake can be exploited.

repository for work projects. According to the State of Secrets Sprawl on GitHub report, 85% of the leaks occur on developers' personal repositories

One boring day during the pandemic, security researcher Craig Hays decided to do an experiment. He wanted to leak an SSH username and password into a GitHub repository and see if any attacker might find it. Hays thought he'd have to wait a few days, maybe a week, before anyone noticed it. Reality proved more brutal. The first unauthorized login happened within 34 minutes. "The biggest eye-opener for me was how quickly it was exploited," he tells CSO.

Over the first 24 hours, six different IP addresses connected to his honeypot a total of nine times. One attacker tried to install a botnet client, while another one attempted to use the server to launch a denial-of-service attack. Hays also saw someone who wanted to steal sensitive information from the server and someone else who was just looking around.

https://www.csoonline.com/article/3634784/how-corporate-data-and-secrets-leak-from-github-repositories.html

Password Attacks

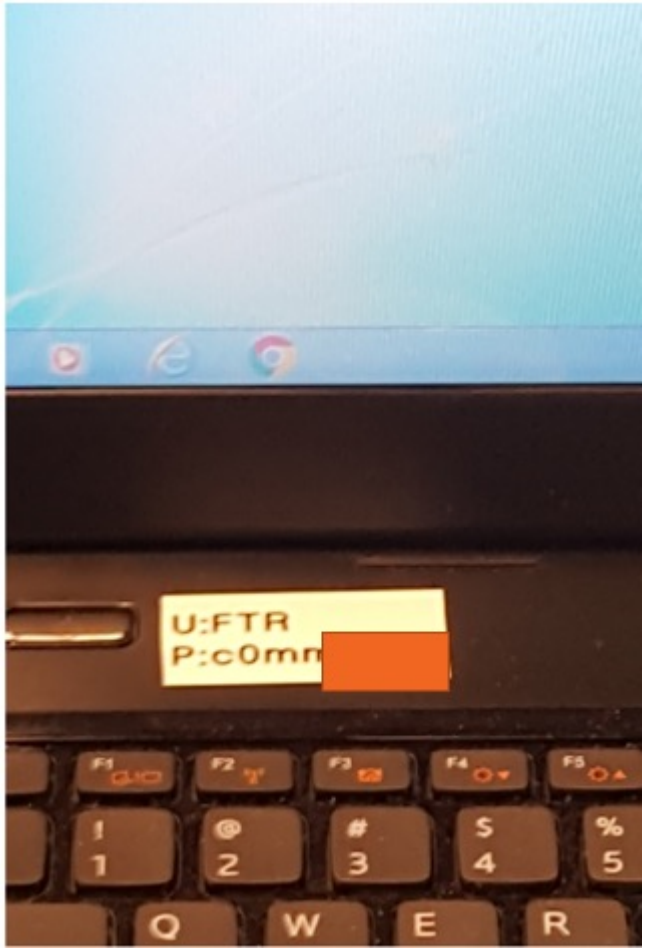
Popular Password Attack Types

Physical Attacks

Examples

- On wall behind everyone
- Watch person type it in
- Password is on a Post-It note
- Taped to a laptop

- This was on a laptop in a gov’t building



Password Attacks

Popular Password Attack Types

Because of all the password theft:

- 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/

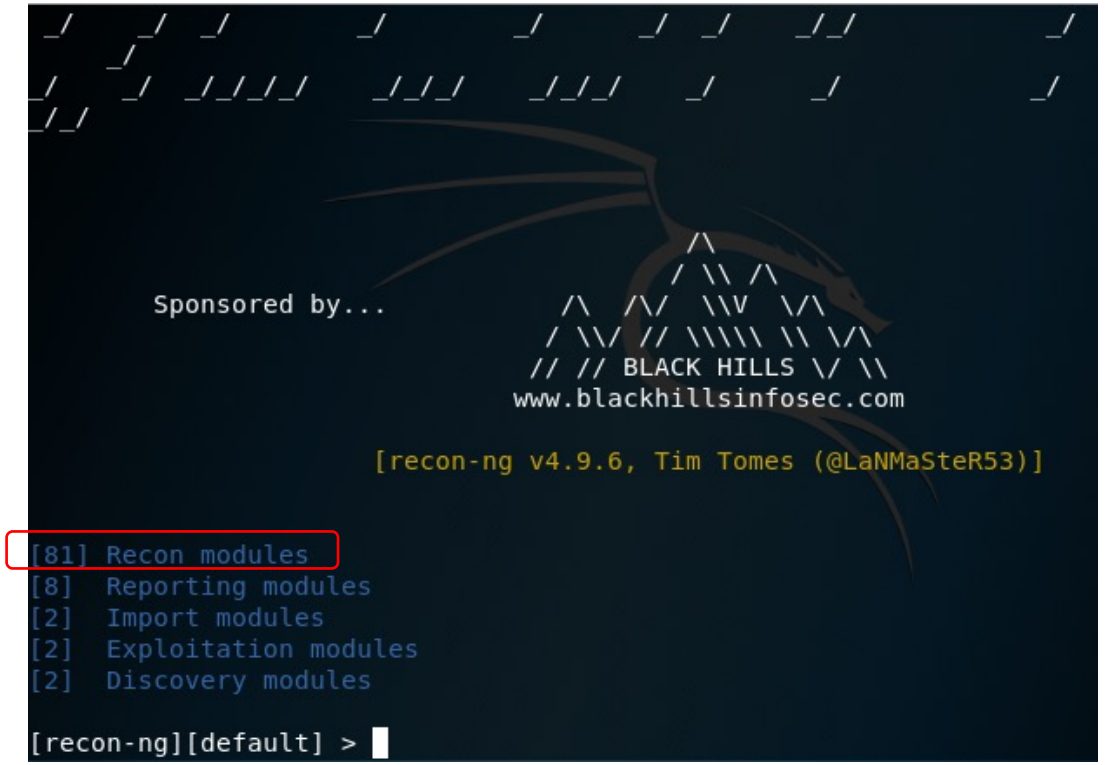
Getting Password Dump Info

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 free or for sale on the Internet and darkweb

> Bill said he's not sure where the passwords are coming from, but he assumes they are tied to various databases for compromised websites that get posted to password cracking and hacking forums on a regular basis. Bill said this criminal group averages between five and ten million email authentication attempts daily, and comes away with anywhere from 50,000 to 100,000 of working inbox credentials.
>
> In a December 2020 blog post about how Microsoft is moving away from passwords to more robust authentication approaches, the software giant said *an average of one in every 250 corporate accounts is compromised each month*. As of last year, Microsoft had nearly 240 million active users, according to this analysis.

From: https://krebsonsecurity.com/2021/09/gift-card-gang-extracts-cash-from-100k-inboxes-daily/

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

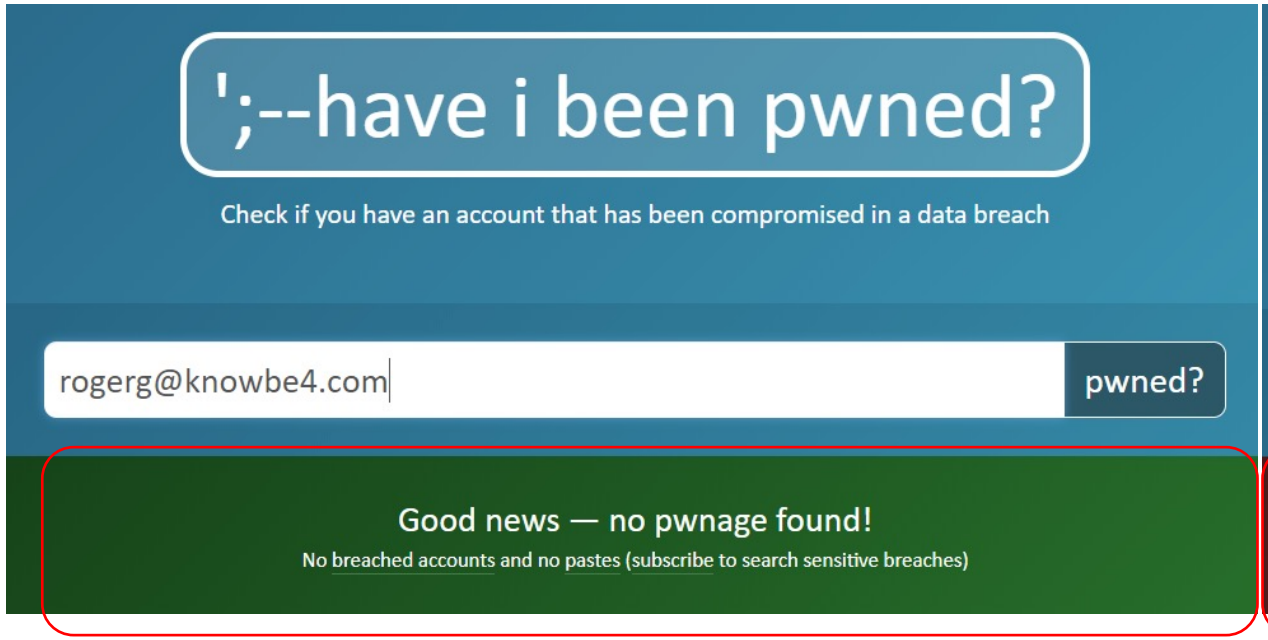
Password Exposure Test

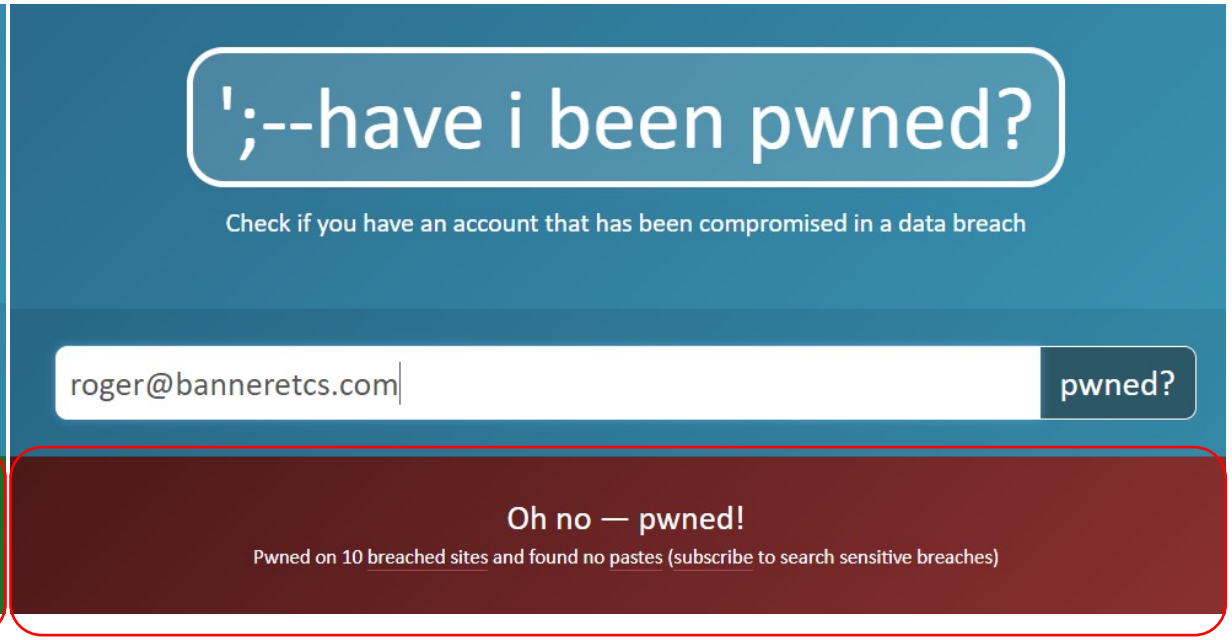
Checking to See if Your Password Has Been Stolen

Attackers Can Buy/Get It:

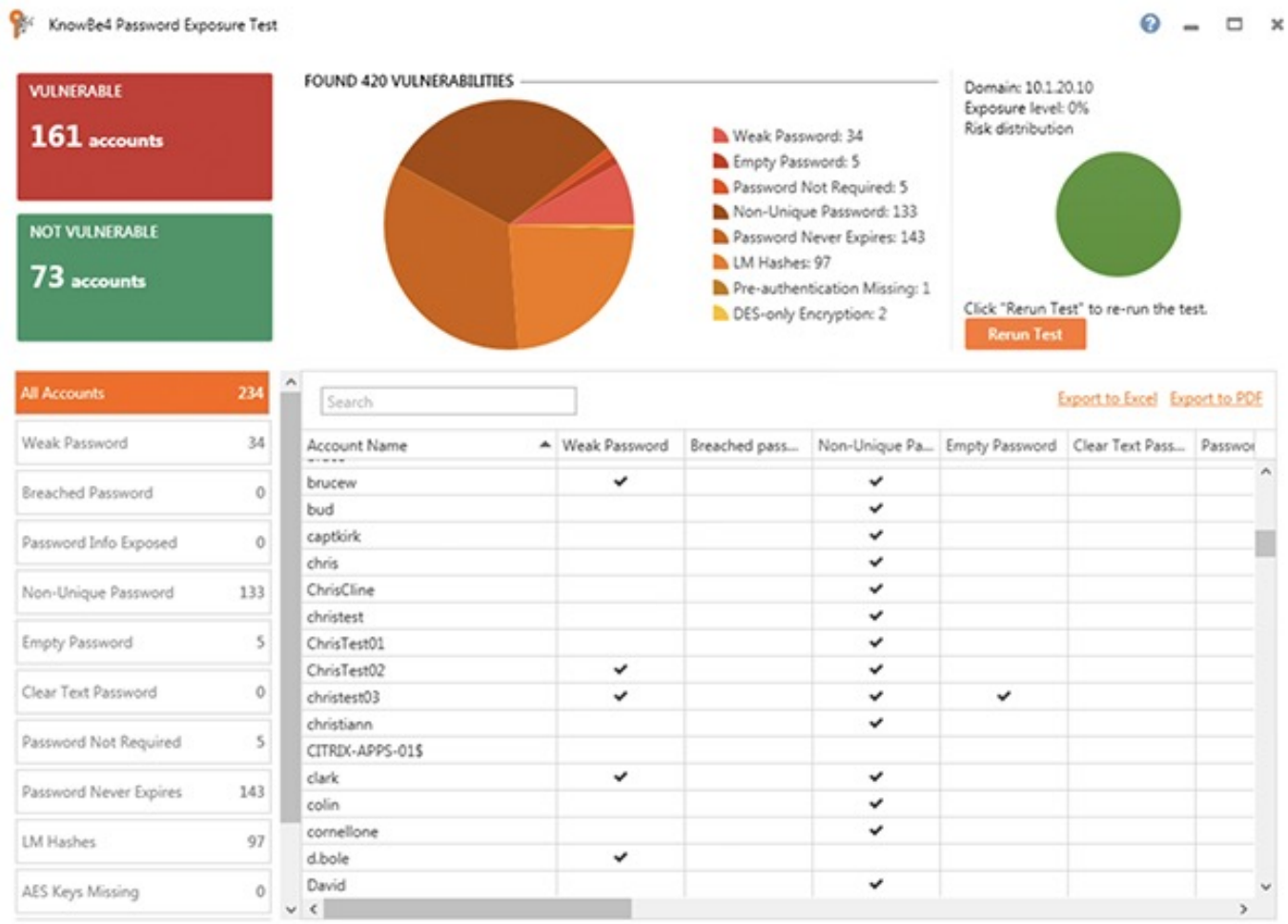
Protecting Yourself/Org

- 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 https://www.knowbe4.com/password-exposure-test

Password Attacks

Popular Password Attack Types

Guessing – Online Logon Prompt

- Guess using one logon name, many guesses
  - Maximum guessing speed limited by application, server response time, network speed and latency, etc.
  - If account lockout or rate throttling ISN'T enabled, attacker can guess from 1 – 100 or so times a minute per guessing instance
  - Far slower than password hash cracking (cover soon)

Password Attacks

Popular Password Attack Types

Guessing Attack Methods

- Worst: Brute force (e.g. a, aa, ab, abc…etc.)
- Better: Dictionary Attack
  - People like to use “root” words for their passwords, in their own language
  - So start with words in dictionary (max. 170K words in Oxford English dictionary)
- Best - 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
  - So most password hacking dictionaries contain less than 10,000 words
- Then add “complexity” to the root word (e.g. frog, frog1, fr0g, etc.)

Password Attacks

Popular Password Attack Types

Guessing

- Only works with weak passwords or when guessing is allowed to be unlimited
  - *password* is the most common password (also *Password2*, *123456*, *admin*, *qwerty*, etc.)

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]	2019[11]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou

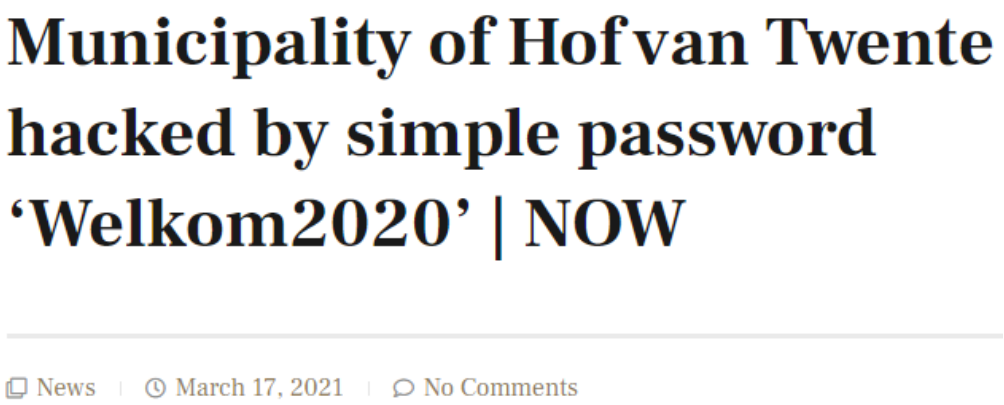
  - 75% of organizations have at least 1 user with a password on a list of 1000 passwords
  - Most “complex” passwords aren’t really that complex

Password Attacks

Popular Password Attack Types

Guessing – Online Logon Prompt

- Example of “long” password guessed, 10-characters
- Attacker was able to guess over a 100,000 times a day for over a year without interruption



Municipality of Hof van Twente hacked by simple password ‘Welkom2020’ | NOW

News | March 17, 2021 | No Comments

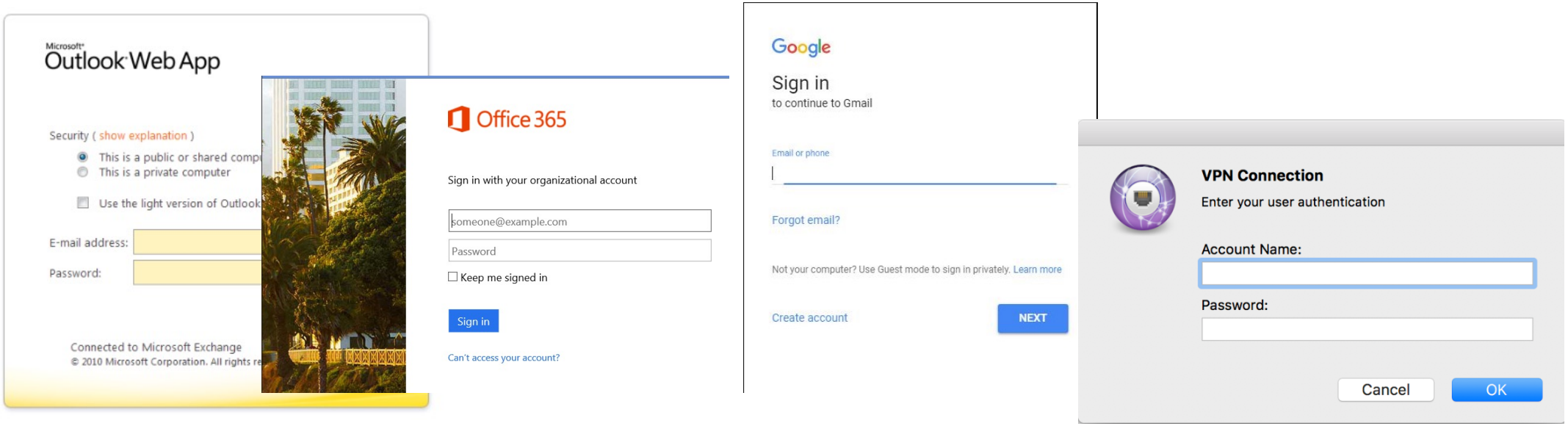
https://www.world-today-news.com/municipality-of-hof-van-twente-hacked-by-simple-password-welkom2020-now/

Password Attacks

Popular Password Attack Types

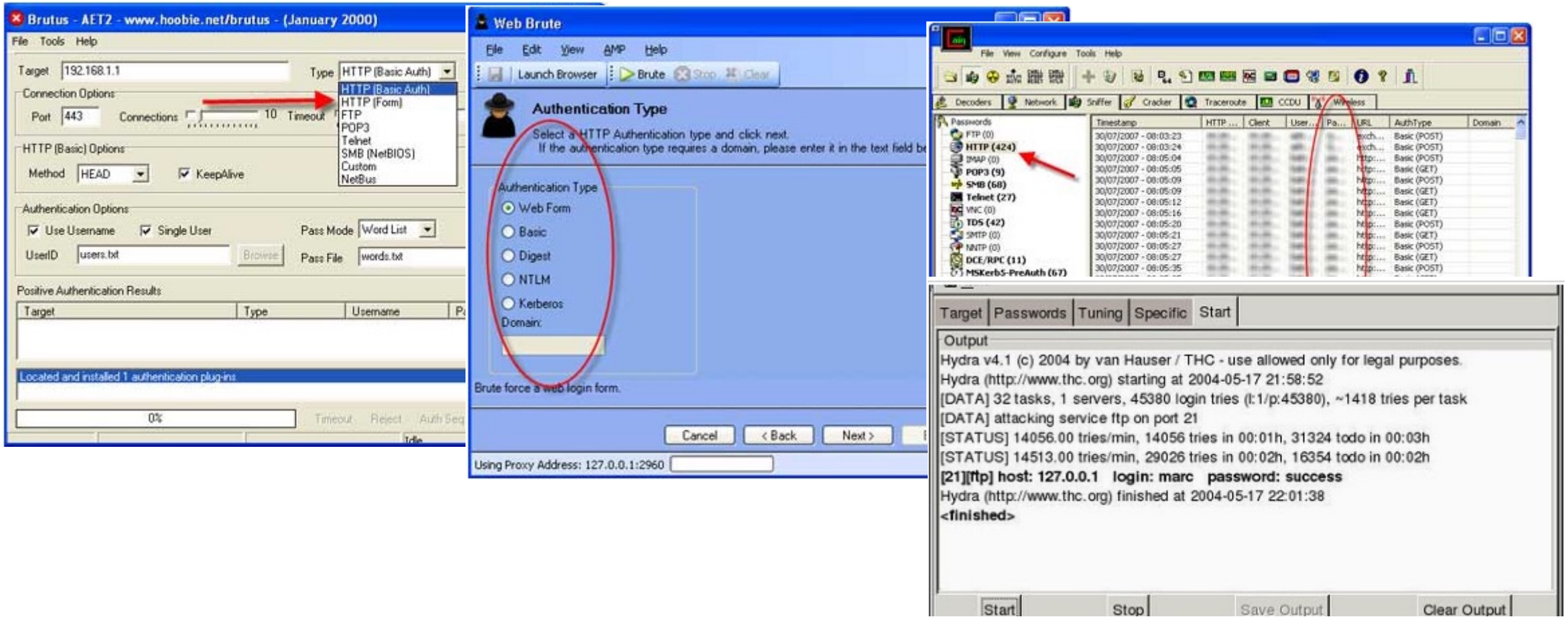
Guessing

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



Password Attacks

Hacker Tools to Guess At Passwords



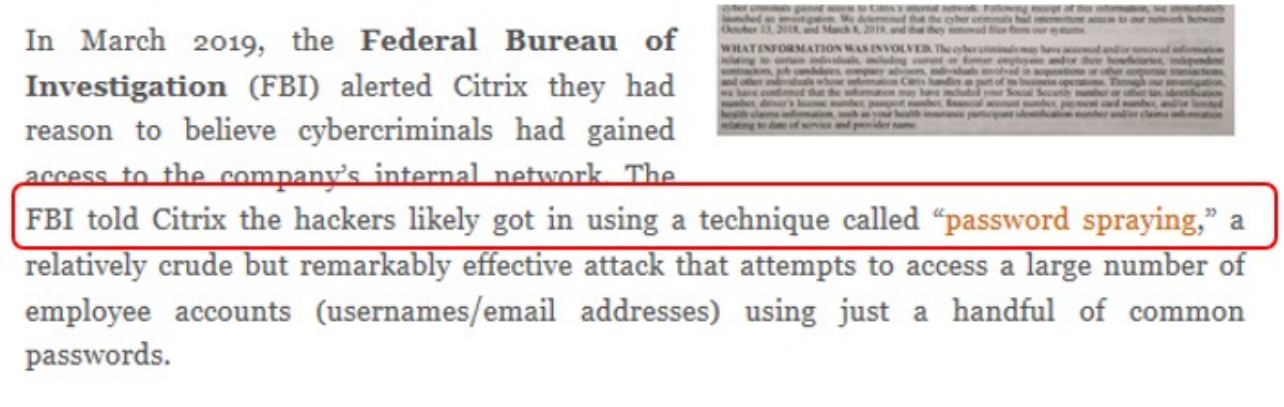
Password Attacks

Popular Password Attack Types

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

Hackers Love Finding Unprotected Open API to Guess Against

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

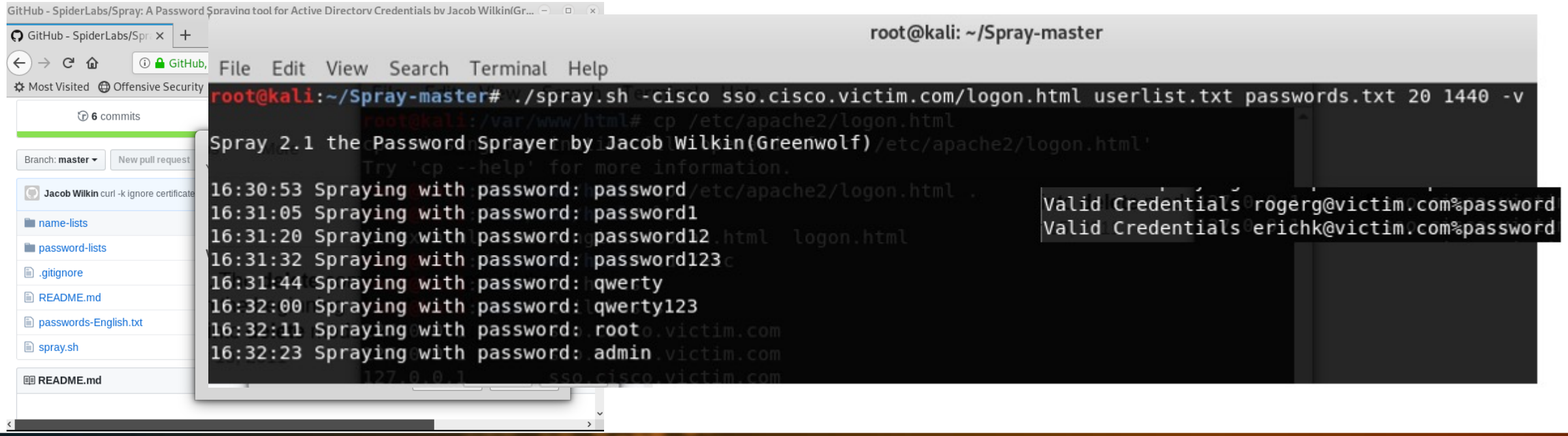
Password Attacks

Password Spray Attack Tools

Tool – Spray

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

<AttemptsPerLockoutPeriod> <LockoutPeriodInMinutes> <DOMAIN>



Password Sprays

Step 3 – Use Tool to Guess At Passwords

Tool - **CredMaster**

```
root@echo:/opt/CredMaster# python3 credmaster.py --plugin o365 -u users.txt -p passwords.txt -a useragents.txt --config aws.config
[2021-03-03 20:52:01.876] Loading AWS configuration details from file: aws.config
[2021-03-03 20:52:01.876] Execution started at: 2021-03-03 20:52:01.876686
[2021-03-03 20:52:01.876] Creating 1 API Gateways for https://outlook.office365.com
[2021-03-03 20:52:02.966] Created API - Region: us-east-2 ID: (tmyrqvswoj) - https://tmyrqvswoj.execute-api.us-east-2.amazonaws.com
[2021-03-03 20:52:02.967] Total Regions Available: 15
[2021-03-03 20:52:02.967] Total API Gateways: 1
[2021-03-03 20:52:02.967] Starting Spray...
```

Benefits & Features

- Rotates the requesting IP address for every request
- Automatically generates APIs for proxy passthru
- Spoofs API tracking numbers, forwarded-for IPs, and other proxy tracking headers
- Multi-threaded processing
- Password delay counters & configuration for lockout policy evasion
- Easily add new plugins
- WeekdayWarrior setting for timed spraying and SOC evasion
- Fully anonymous

The following plugins are currently supported:

- OWA - Outlook Web Access
- EWS - Exchange Web Services
- O365 - Office365
- O365Enum - Office365 User Enum (No Authentication Request)
- MSOL - Microsoft Online
- Okta - Okta Authentication Portal
- FortinetVPN - Fortinet VPN Client
- HTTPBrute - Generic HTTP Brute Methods (Basic/Digest/NTLM)
- ADFS - Active Directory Federation Services
- AzureSSO - Azure AD Seamless SSO Endpoint
- GmailEnum - Gmail User Enumeration (No Authentication Request)

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
- Malware often takes advantage of this
- Becoming a much bigger problem with IoT

Password Attacks

Password Guessing Defenses

- Change any default passwords immediately
- Use strong passwords
- Enable Account Lockout policies
- Enable failed logon monitoring/alerting
- Secure and monitor APIs
- Use phishing-resistant Multifactor Authentication (MFA) where you can

Password Hash Cracking

General Steps

1. Attacker somehow gets your password hashes
   - Normally takes elevated access and total compromise of a device and/or network to get, but not always
2. "Cracks" hashes back to plaintext passwords they represent

   Requires:
   - Password hash cracking "rig" with lots of computational power and memory
   - Cracking software (i.e., hashcat, John the Ripper, etc.)
3. Hacker uses or sells cracked plaintext passwords

- Can often reuse hashes without cracking to attack exploited site

Password Hash Cracking

Password Hash Basics

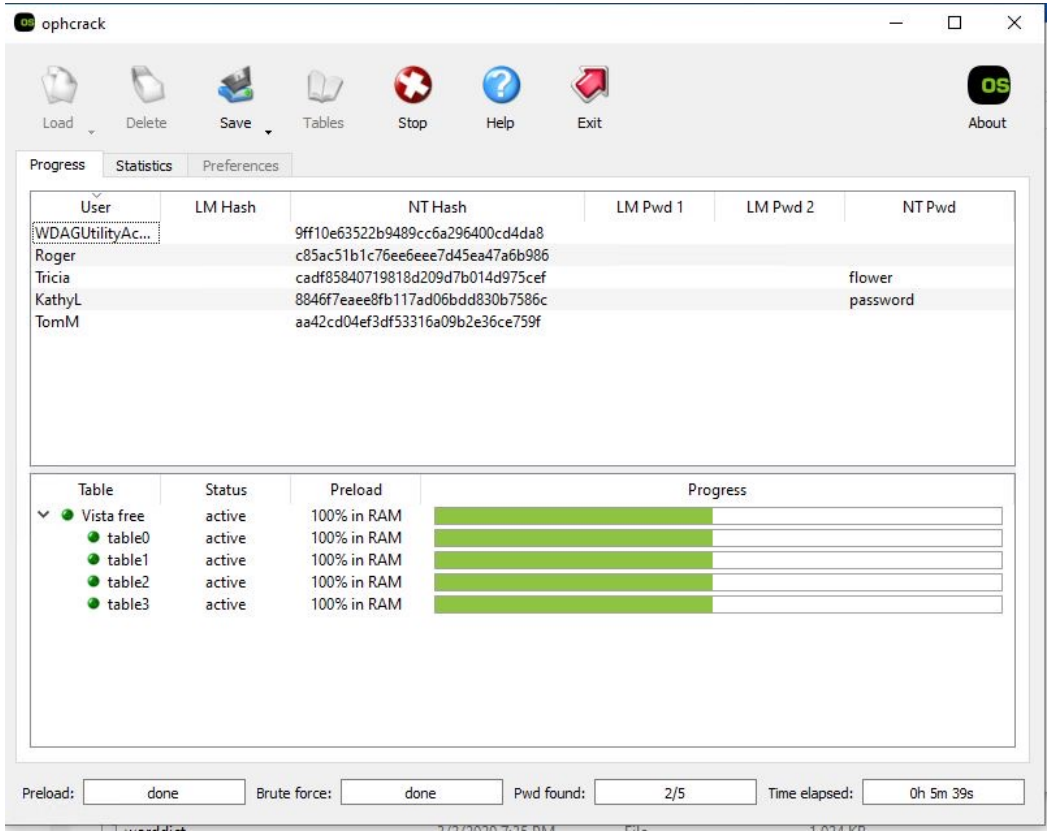
- In most authentication systems, passwords are stored and transmitted as cryptographic hashes (MD5, LM, NT, SHA1, SHA2, BCRYPT, etc.)

Hash Algorithm	Hash Result for frog
Message Digest5 (MD5)	938c2cc0dcc05f2b68c4287040cfcf71
LANManager (LM)	71CF7241255BBEB4AAD3B435B51404EE
Windows NT (NT)	E3EBB26FE8A631171D218D084C76C982
SHA1	b3e0f62fa1046ac6a8559c68d231b6bd11345f36
SHA2-256	74fa5327cc0f4e947789dd5e989a61a8242986a596f170640ac90337b1da1ee4
BCrypt	$2y$10$5lSoGVbVHgmVVvV2J5Cxt.RFJyjVA38InpRbIP/GZo5vQAetjnv9S

Password Hash Cracking

Password Hash Cracking Tools

- Once obtained, password hashes can be “cracked” back to their plaintext equivalents
- Big lists of passwords and their hashes are compared to stolen hashes
- Hash table – 1:1 lookup
- Rainbow table – converts passwords to an intermediate form for much faster hash comparisons



Password Hash Cracking

Stealing Password Hashes

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

Password Hash Cracking

Special Cases That Changes Everything

When attacker doesn’t need elevated access to get hashes

- Password logons transmitted in plaintext across network
- Kerberoasting
- Email password hash theft trick

Password Hash Cracking

Special Case That Changes Everything

Kerberoasting

- Works on Active Directory-connected Microsoft Windows computers
- Attacker first compromises computer using any normal user account
- That account can be used to extract the NT hash from any Windows account with a **Kerberos Service Principal Name (SPN)**
- So, any non-admin user can get hashes of the most privileged accounts
- NT hash can then be guessed against

*This changes my previous, “weaker”, password policy recommendations to be stronger

Phishing Password Hash Theft

Email Phishing Password Hash Capture Steps

1. Hacker creates/has a malicious web server on Internet
2. Creates a malicious URL address that links to object on web server
3. Sends link to victim (e.g., using email, etc.)
4. Victim clicks on URL link
5. Email program/browser attempts to retrieve object
6. Server says it requires an authenticated logon to access object
7. Email program/browser attempts authenticated logon
8. Sends remote logon attempt from which attacker can derive password hash

Phishing Password Hash Theft Demo

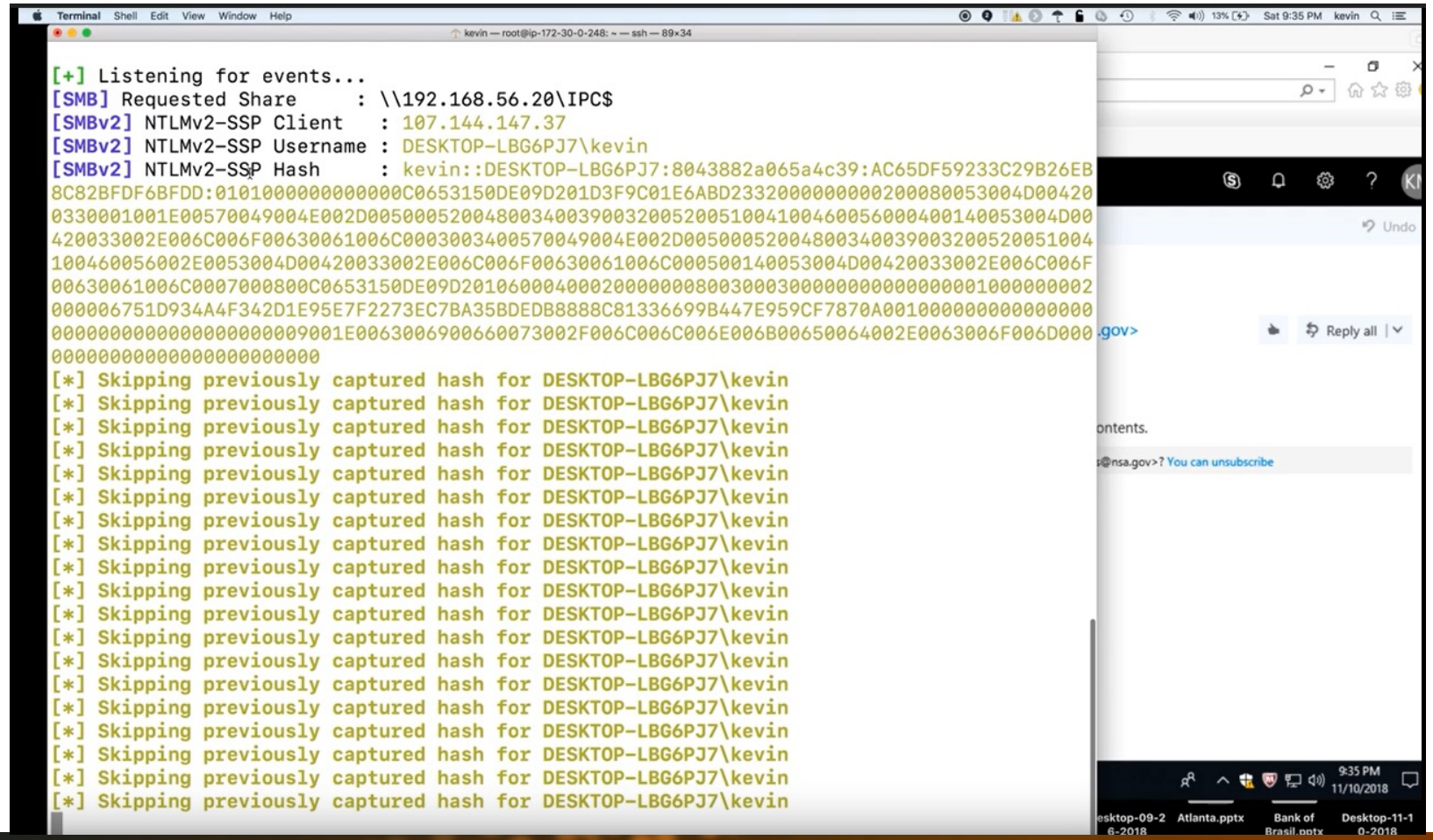
URL Click sends Your Password Hash

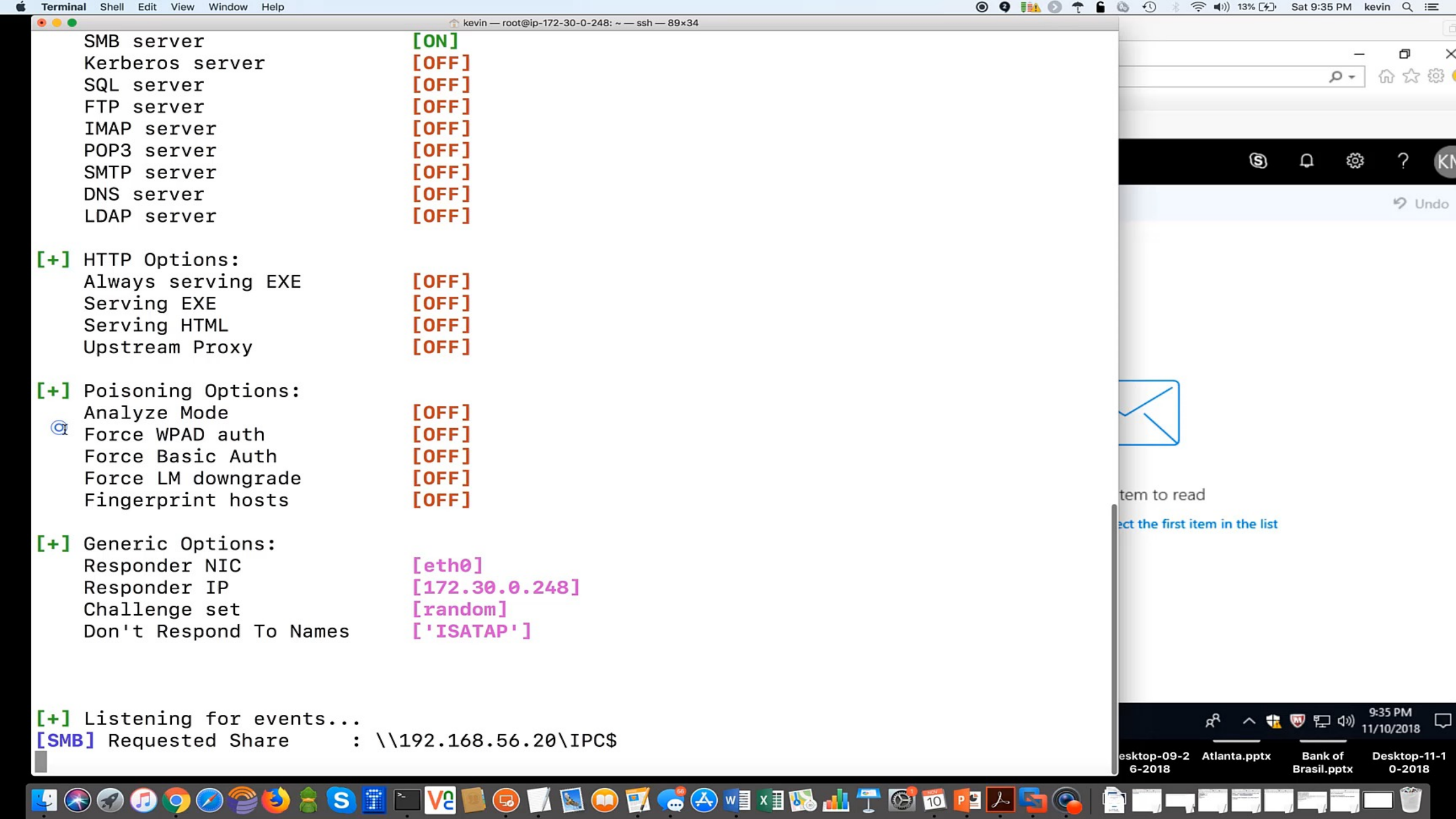
Kevin Mitnick demo

- Uses **file:////** trick
- https://blog.knowbe4.com/kevin-mitnick-demos-password-hack-no-link-click-or-attachments-necessary
- **I Can Get and Hack Your Password Hashes From Email**
  - https://www.csoonline.com/article/3333916/windows-security/i-can-get-and-crack-your-password-hashes-from-email.html

Phishing Password Hash Theft Demo

Password Hash Capture - Kevin Mitnick Demo




Terminal Shell Edit View Window Help
Sat 9:35 PM kevin
kevin — root@ip-172-30-0-248: ~ — ssh — 89×34
SMB server [ON]
Kerberos server [OFF]
SQL server [OFF]
FTP server [OFF]
IMAP server [OFF]
POP3 server [OFF]
SMTP server [OFF]
DNS server [OFF]
LDAP server [OFF]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Fingerprint hosts [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [172.30.0.248]
Challenge set [random]
Don't Respond To Names ['ISATAP']
[+] Listening for events...
[SMB] Requested Share : \\192.168.56.20\IPC$
Undo
tem to read
ct the first item in the list
9:35 PM
11/10/2018
esktop-09-2 6-2018
Atlanta.pptx
Bank of Brasil.pptx
Desktop-11-1 0-2018

Phishing Password Hash Theft

Defenses

- Require passwords with enough entropy to withstand cracking attempts
- Block unauthorized outbound authentication logons at perimeter and/or host
  - Port blocking: **NetBIOS: UDP 137 & 138, TCP 139 & 445; LLMNR: UDP & TCP 5535**; LDAP: UDP/TCP 389 & 636; SQL: TCP 1433; TCP 21; SMTP: TCP 25 & 587; POP: TCP 110 & 995; IMAP: TCP 143 & 993
  - Can you block on portable devices wherever the connect?
- Filter out inbound file:/// links
- Optional Microsoft patch and registry configuration settings:

  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170014

Password Hash Cracking

How Fast Can Password Hashes Be Cracked?

Hash types 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 (often called NTLM, but NTLM is a network protocol not a type of hash)

Easy to Hard Crack

- NT hashes are moderately hard to crack (used unsalted in Microsoft Windows)
- SHA1/SHA2 harder to crack (salted SHA2-256 bit used in most Apple/Linux/Unix OSes)
- PBKDF2 used in Windows 10/Apple/Linux for some operations is fairly hard
- BCRYPT harder to crack (but loses to PBKDF2 after 55-characters)

Password Hash Cracking

- Hashes + Software + CPU cycles + RAM
- Most common cracking tool is **hashcat**
- Graphics Processing Units (GPUs)
- “Rigs” full of GPUs
- Appliances
  - Ex. Terahash - $25,499, 375+ GPUs
- Clouds, Clusters, Parallel Processing

Password Hash Cracking

How Fast Can Password Hashes Be Cracked?

- Many rigs can crack NT password hashes at 2TH/s (2 trillion tries a second)
  - This would be considered the top tier performance level of “normal” password hash cracking rigs
- Some elite top rigs can crack at 10’s of TH/s
- Top bitcoin miners have 100’s of TH/s which is probably what nation-states have
- 100’s of TH/s can be bought for $50-$100/hr in clouds

Password Hash Cracking

How Fast Can Password Hashes Be Cracked?

Password hash cracking speed on 45TH/s rig on perfect random passwords

		Password Length						
Hash	Eff. Speed	6	7	8	9	10	11	12
LM	15.81 TH/s	instant	instant	instant	instant	instant	instant	instant
NT	31.82 TH/s	instant	instant	3.5 min	5.5 hrs	3 wks	5.6 yrs	538 yrs
MD5	17.77 TH/s	instant	instant	6 min	10 hrs	9 wks	10.1 yrs	963 yrs
SHA1	5.89 TH/s	instant	instant	19 min	29 hrs	15 wks	30.6 yrs	2.9M yrs
SHA2-256	2.42 TH/s	instant	instant	45.5 min	3 days	37 wks	74.25 yrs	7.1M yrs
SHA2-512	801.9 GH/s	instant	instant	2.25 hrs	9 days	28 mon	225 yrs	21.4M yrs
BCRYPT	11.37 MH/s	18 hrs	9 wks	59 yrs	5.6M yrs	534M yrs	50744M	4820555M

Data from: https://t.co/NKYIrKwUDb

This is why you need 12-character perfectly random passwords

Password Hash Cracking

How Long Should Your Password Be To Be Considered Uncrackable?

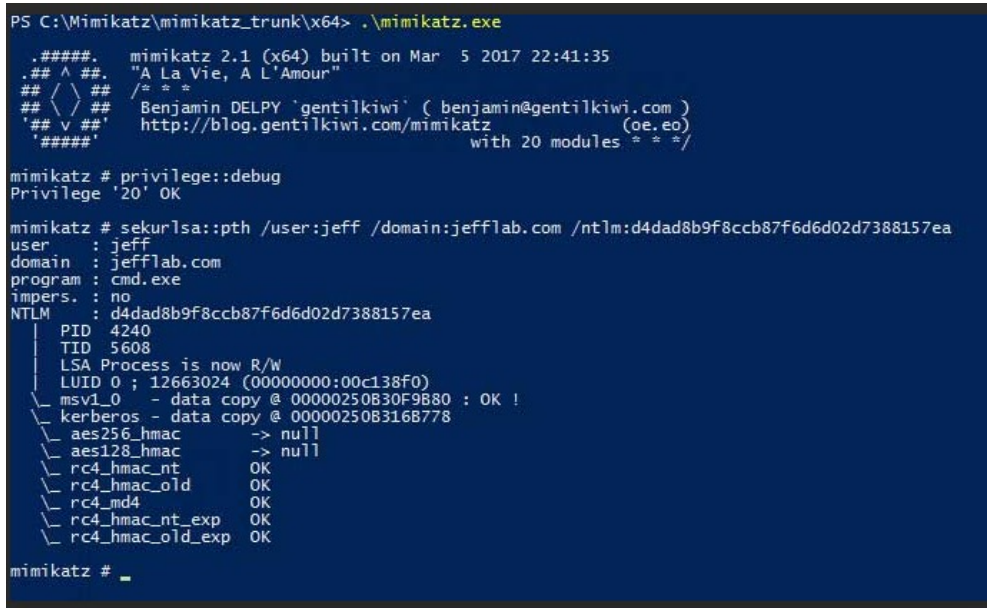
- NT hash from perfectly random password: At least 12-characters
  - SHA2-256-bit: At least 11-chars Bcrypt: 8-9 chars
- NT hash from “normal” complexity passphrase: At least 20-characters
  - At least 30-characters to prevent theoretical or future attacks
- Windows passwords should be 15-characters long to disable LM hashes

- That’s why using MFA and/or password manager when possible is preferred, followed by passphrases

Password Hash Theft

Password Hash Basics

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




```
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
- Prevent social engineering best you can
- 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 Attacks

Popular Password Attack Types

Account Takeover Recoveries

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

Microsoft account

Security code

Please use the following security code for the Microsoft account ro*****@hotmail.com.

Security code: **0152772**

If you don't recognize the Microsoft account ro*****@hotmail.com, you can click here to remove your email address from that account.

Thanks,
The Microsoft account team

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.

954327

Sent

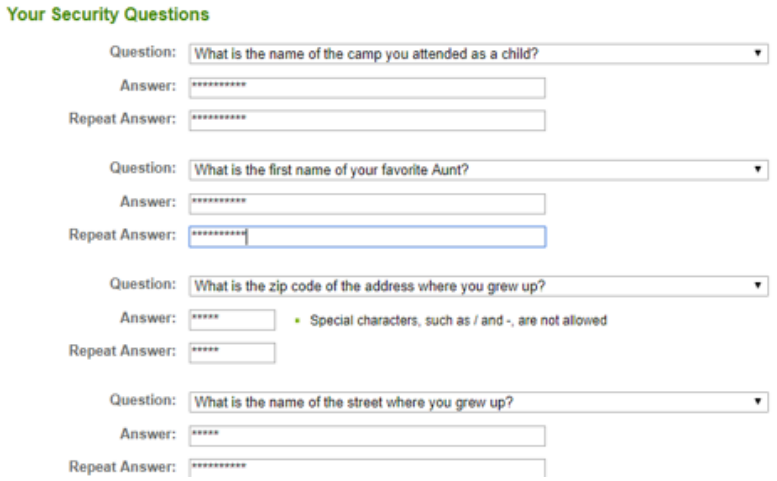
Rogue Recoveries

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

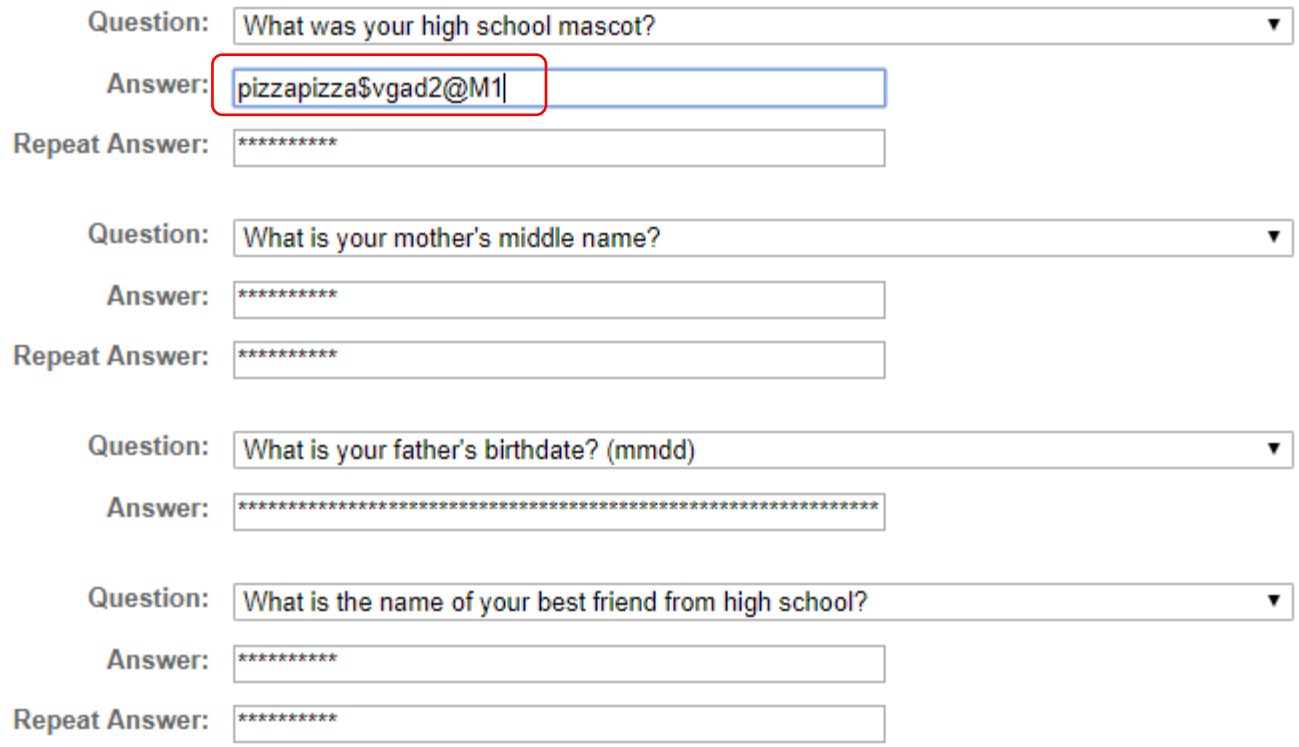
- 20% of some recovery questions can be guessed on first try by hacker
- 40% of people were unable to successfully recall their own recovery answers
- 16% of answers could be found in person's social media profile

- 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!



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

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

- Types of Password Attacks and Defenses
- Password Policy Recommendations

Password Policy

Password Policy Components

- 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 all involved components!!

Password Policy
Practical Implementation

Use MFA wherever you can
Multifactor Authentication where you can to protect valuable things

Whenever possible use phishing-resistant MFA

https://blog.knowbe4.com/u.s.-government-says-to-use-phishing-resistant-mfa

Use MFA and/or long passwords/passphrases to logon to your devices

All passwords should be changed at least annually

For Passwords

If you can, use a Password Manager
. Protect password manager with MFA and/or long password/passphrase

12-character perfectly random passwords defeat all known guessing/cracking attacks

Perfectly Random Password Examples
R#Yv&ZCAojrX
ELv!2MibAb>RC?ru
a!#=dH)vvLykiJhu

If you must create a password
Create a unique, different, long password/passphrase for all sites and services

Human-created passwords
8-characters – weak
12-characters – better
20-characters – strong

Examples of Good Passphrases
I went to 7-11 earlier today.
rogerjumpedoverthepurplefox
2belivingtherockandrolllifeforever

*Hackers are routinely cracking 18-character human-created Windows passwords if they get the hashes

Optimally:
MFA +
Password Manager +
Strong individual passwords where needed

For more detail: https://info.knowbe4.com/wp-password-policy-should-be

Which Password Attack Types…

Don't Care About "Strong" Passwords?

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

Are Impacted by "Strong" Passwords?

- Guessing
- Hash Cracking
  - (but does not stop hash reuse and may be game over anyway)

The vast majority of password attacks are this type

Password Policy

What is password complexity?

- 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

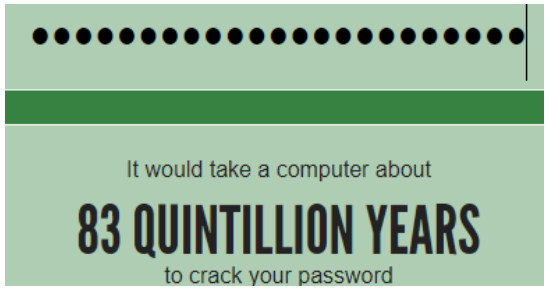
Password Policy

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

Passwords Strength Checkers

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/

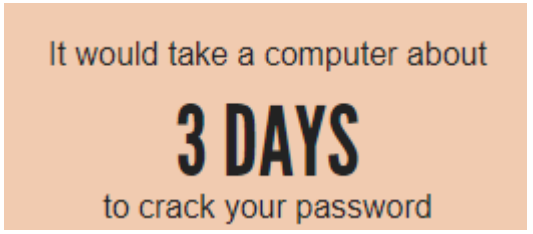
- Caution: Any website asking you to submit your real password to determine strength could be using your submission against your interests
  - Use another similar, but not identical password submission to get the same information.
  - For ex: If your password is Dogdog32 use CatCat23

Password Strength

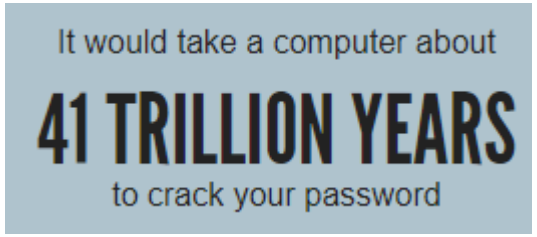
Length vs. Complexity

- How long to crack the hashes of these passwords?

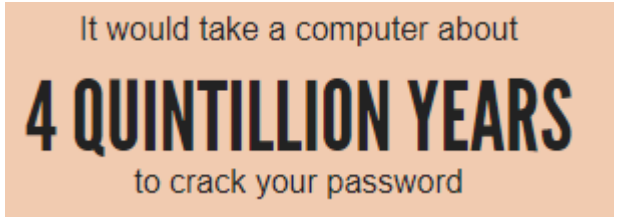
Rogergri2



]}7Y?@w@?)Nmt4h7



rogerjumpedoverthedogandcat



Both are hard to crack, 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

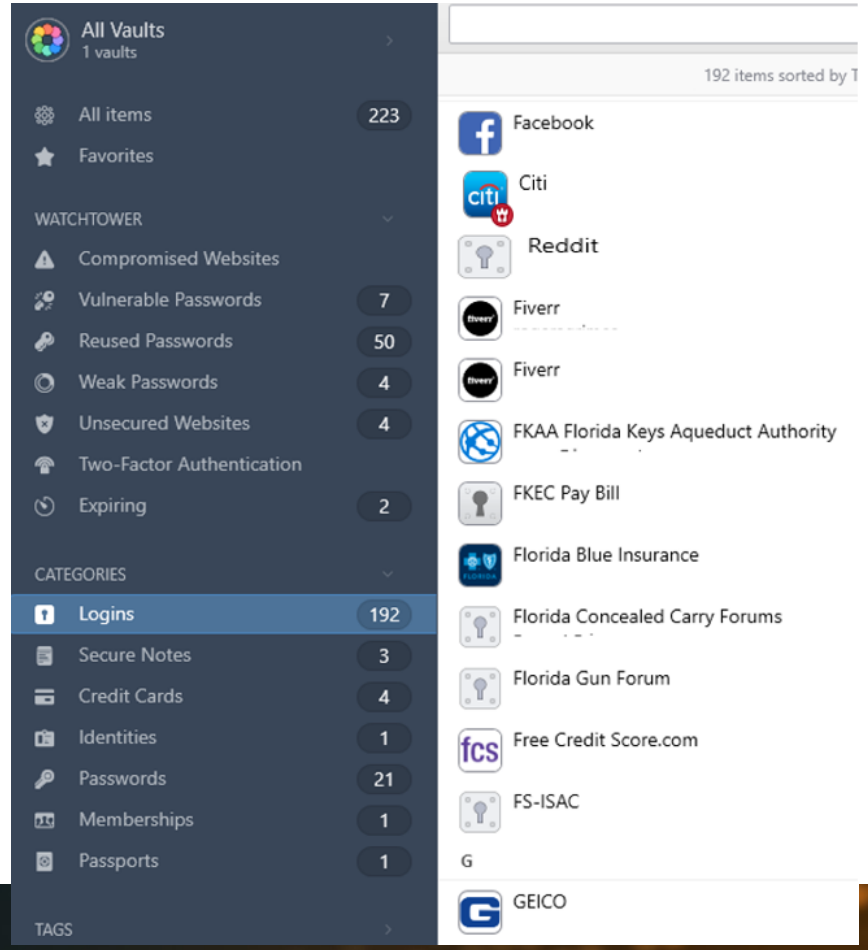
Password Managers

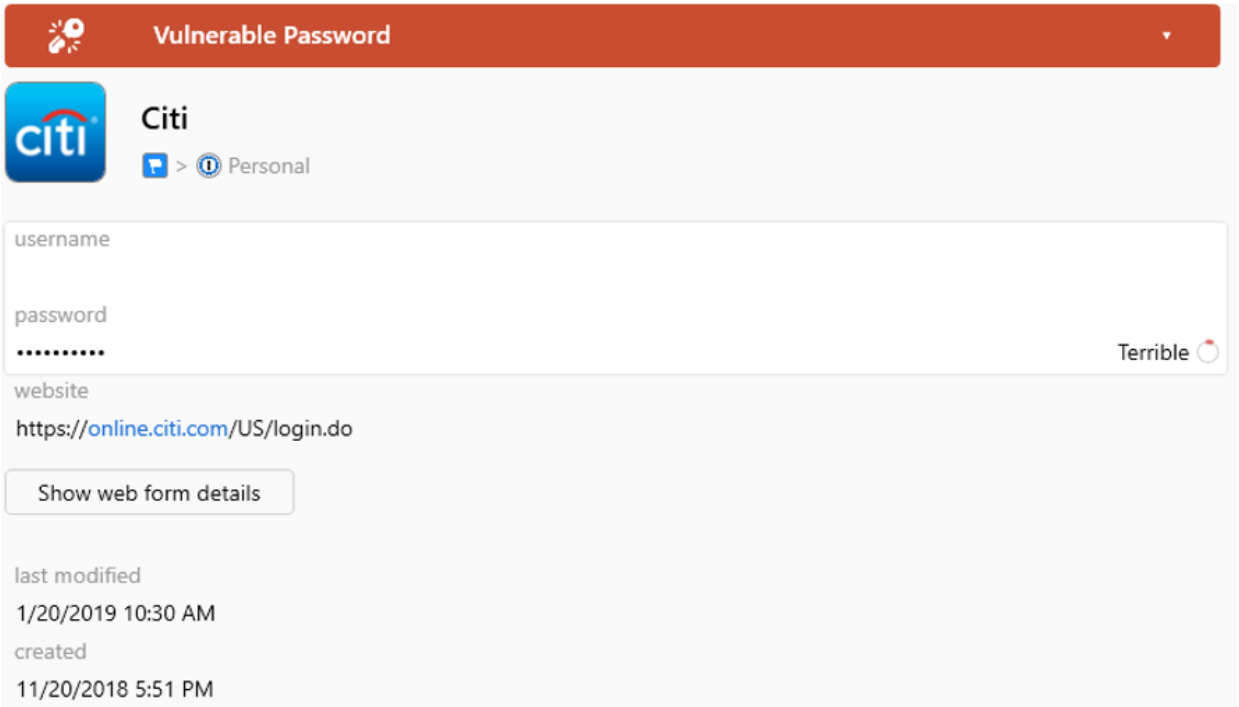
Password Managers

- 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://blog.knowbe4.com/what-about-password-manager-risks

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

Resilient MFA Solutions

My List of Good, Strong MFA

- https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes

Don't Use Easily Phishable MFA and That's Most MFA!

- https://blog.knowbe4.com/do-not-use-easily-phishable-mfa

US Government Says to Avoid Phishing-Resistant MFA and Why Is the Majority of Our MFA So Phishable?

- https://blog.knowbe4.com/u.s.-government-says-to-avoid-phishing-resistant-mfa

Monitoring Recommendations

Monitoring and Alerting

- 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

Other Recommendations

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

Password Policy ebook

https://info.knowbe4.com/wp-password-policy-should-be

KnowBe4 Security Awareness Training

Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

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, thousands of templates with unlimited usage, and community phishing templates.

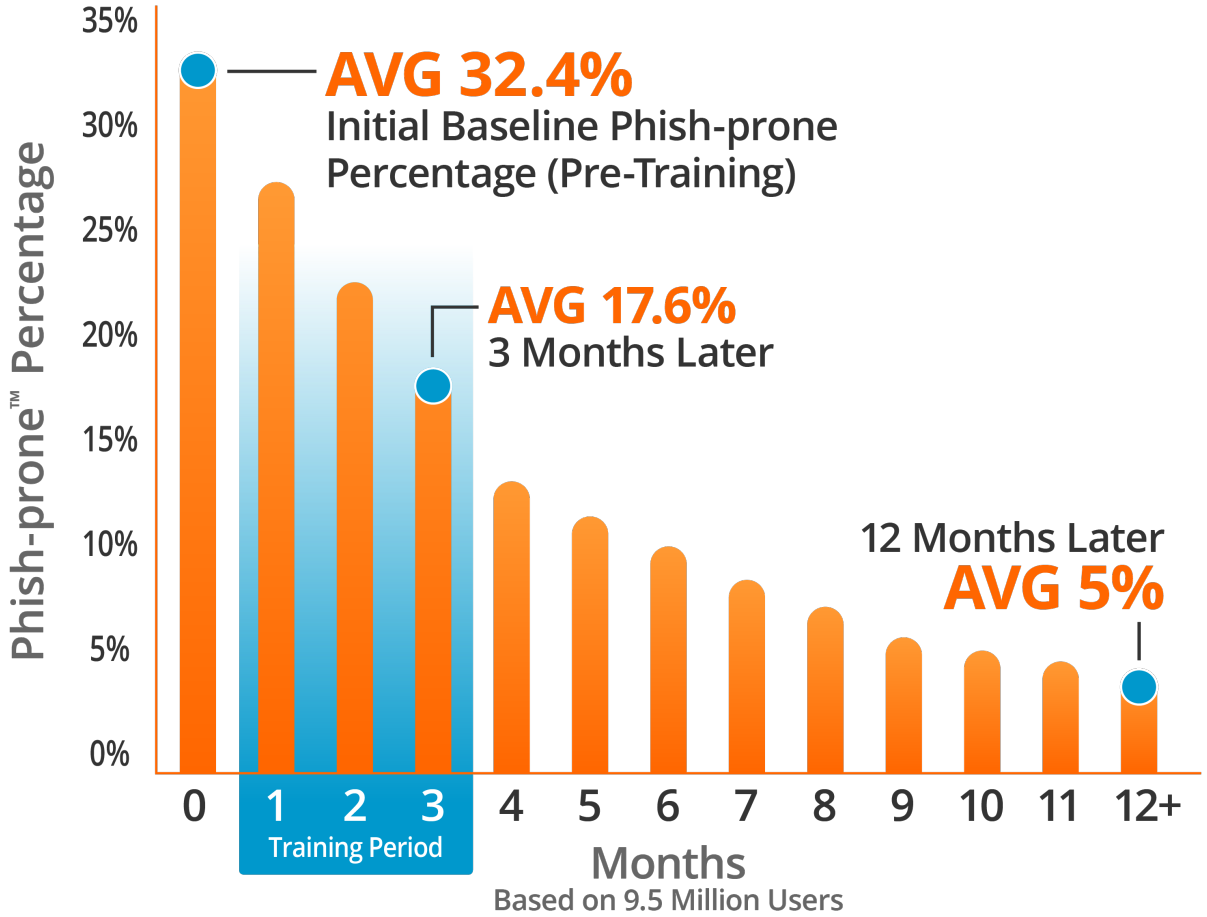
See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

85% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

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