

Resources

The following pages include:

- Supporting documents
- Content used on the workstations
- Links to items we purchased
- Instructions on setting up the computers

Bob Hewitt

- <https://www.linkedin.com/in/bobhewitt/>
- <https://twitter.com/infosecbobh>

Security “Escape Room” Scenario Game Master Sheet

Objective

Begin: Log into Notebook at simulated “workstation”

Goal: Email Credit Card capture information to securityawareness@<yourcompany.com>

You have 60 minutes of game time

General Rules

Notebooks are locked to desks – they cannot be moved

Workstation partitions cannot be moved

Documents attached to partitions cannot be removed

Penalties

Hints can be provided at the group’s request – 5 minute penalty per hint provided

Security protocol failures – 5 minute penalty per infraction

Breaking of a general rule – 5 minute penalty per infraction

Game Master Score and Hint Sheet

Date:

Team Name:

Team Captain:

Team Members:

Check off objectives as they are successfully completed.

___ Objective 1. Demonstrate passwords can easily be guessed or cracked.

Hint: Year of the Dog

___ Objective 2. Identify improperly stored PII

Hint: 9k

___ Objective 3. The level of protection should be proportionate to what we are protecting

Hint: PII

___ Objective 4. Demonstrate compliance of physical access control policies and procedures.

Hint: New doors are open

___ Objective 5: Recognize risk of password reuse.

Hint: Haven't we been here before?

___ Objective 6: Identify Phishing attempt e-mails

Hint: BeeGees

___ Objective 7. Perform a manual cipher decryption.

Hint: Hail Caesar!

___ Objective 8. Perform a file decryption using 7zip.

Hint: Look up golf in the dictionary.

___ Objective 9. Crack a hash using an online resource.

Hint: Read the instructions from the 7zip archive.

___ Objective 10. Demonstrate methods to send sensitive information securely.

Hint: Remember your training.

Time Remaining:

Penalties:

Time Loss

Time Loss

Notebook Setup

Equipment

Retired notebooks from IT

Software

7-zip (Workstation B)

Firefox or Chrome (Workstation B)

Microsoft Word (Workstation A and B)

Microsoft Excel (Workstation A)

Network

Wireless card

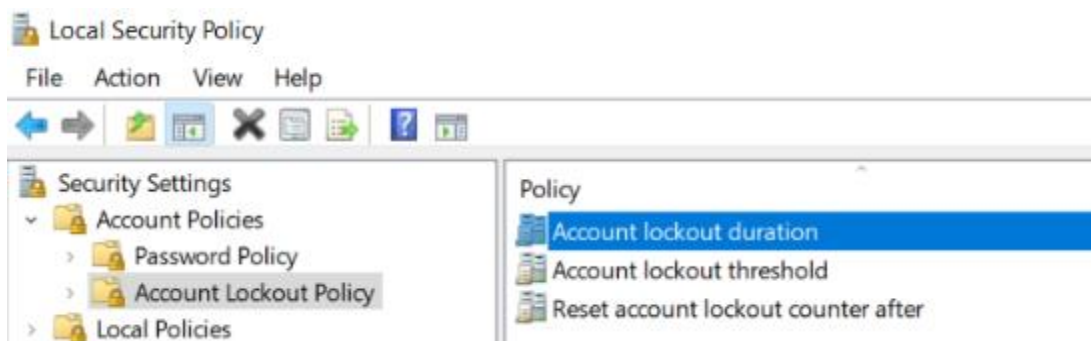
Internet access to crackstation.net and gmail.com

We used AT&T and Verizon Hotspots to avoid any compliance issues

Notebook Setup

Set the Account Lockout Policy




- Start button, “Local Security Policy” and run as an Administrator.
- Under “Security Settings”, browse to “Account Lockout Policy”
 - **Account lockout Duration:** 1 Minute
 - **Account lockout threshold:** 3 invalid login attempts
 - **Reset account lockout counter after:** 10 Minutes



Create Account and Set Password

- Set the password to your liking. Make it so it can be guessed using clues from the user's work area
- Ensure it exceeds your organization's password requirements.
 - We used PrincessLila2018!
 - 17 Characters, mixed case, special character, number

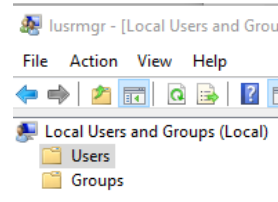
Create Account and Set Password

- Open Control Panel (Click on Start and type "Control Panel")
- Click "User Accounts"  **User Accounts**
Change account type
- Click "User Accounts" again  **User Accounts**
Give other users access to this computer Change account type
- Click "Manage User Accounts"  **Manage User Accounts**
- Select the "Advanced" tab and click "Advanced"



Create Account and Set Password

- Right Click "Users" and select "New User..."
- Complete the form
- Uncheck "User must change password at next login"
- Click "Create"



New User

User name: Aware

Full name: Andy Ware

Description: Activity Account for Awareness training

Password:

Confirm password:

☐ User must change password at next login

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Help Create Close

2018



JANUARY

S	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

FEBRUARY

S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

MARCH

S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

APRIL

S	M	T	W	Th	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

MAY

S	M	T	W	Th	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

JUNE

S	M	T	W	Th	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

JULY

S	M	T	W	Th	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

AUGUST

S	M	T	W	Th	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

SEPTEMBER

S	M	T	W	Th	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

OCTOBER

S	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

NOVEMBER

S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

DECEMBER

S	M	T	W	Th	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Content in Hash.7z file

Recent studies show 45% of passwords are reused. Databases of hashes from various breaches are often distributed and reused as a password found at one site will likely be found on another.

In our next demonstration, the following list of hashes and usernames were found after a Lego related fan site was compromised.

Fortunately, the site only had 8 users, unfortunately one of the users was <yourcompany>awareness@gmail.com.

Find their hash below and crack it at <https://crackstation.net/>, then try to access their gmail (you can access gmail from the Escape Room lab notebook for the purposes of this exercise).

0B20E35DE6FF81A819A7190DC4942C816525BDC915D11947D91E34CAA2469D86::narnia@gmail.com

07862D2A64F3D41C460387BF78160C92886EE5621A1714DC5B3BD8D931D493A5::legomylego@yahoo.com

1D92DAE504A70FBCAE6D3721A55D7EACAF94D3133EA5F0394B7D203D64841110::stillonaol@aol.com

1DA9133AB9DBD11D2937EC8D312E1E2569857059E73CC72DF92E670928983AB5::fullmetaljacket@gmail.com

A88A14ABDAB5DA4BD70E6960B01A6032C661502EA7650A2D853EBE0B3829C146::paulsimon@yahoo.com

BF4FFB1487762665C9B10595337445BB6190D2C60B9DFE85CE68DEA4D1C4C274::masterlegobuilder@yahoo.com

1DA9177AB9BBD11D2937EC8D1925E1E2574957059E73CC72DF92E670928983AB5::<your company>awareness@gmail.com

56093992BC45C1319389321E31880279663A03F5A18C32077BF77002076C1DE3::itwasntme@compuserve.com

Users that reuse passwords run the risk of having their credentials found in other breaches and reused.

Content in Gmail Message

Simulated Credit Card Capture

POST /lego_refill.aspx HTTP/1.0

Referrer: http://test.legobrewing.com:80/index.asp?

Content-Length: 48

Content-Type: application/x-www-form-urlencoded

Connection: Close

Host: legobrewing.com

User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)

Pragma: no-cache

Cookie: ASPSESSIONIDASDFDF=ASDFASDFSDFSADFDFFDFDFASDFOJDG

user=darb&password=reebemoswerb

Content-Disposition: form-data; name="\$cardNumber\$textField"

401288888888

Content-Disposition: form-data; name="\$card\$ccv\$textField"

123

Content-Disposition: form-data; name="card\$expiration\$months\$input"

12

Content-Disposition: form-data; name="card\$expiration\$years\$input"

2018

Shopping List

LED 395nm Ultra Violet Blacklight

https://www.amazon.com/gp/product/B001Q70A0G/ref=ppx_yo_dt_b_search_asin_title?ie=UTF8&psc=1

\$11.88

Set of 3 Invisible UV Blacklight Ink Marker Blue Red Yellow

https://www.amazon.com/gp/product/B004C89M9Q/ref=ppx_yo_dt_b_asin_title_o03_s01?ie=UTF8&psc=1

\$6.25

Book Safe with Combination Lock

https://www.amazon.com/dp/B072PT6XP3/ref=cm_sw_em_r_mt_dp_U_E-wkDbEKP1DWQ

\$12.95

BAZIC Tri-Fold Corrugated Presentation Board, 36 x 48 Inch (3-Pack)

https://www.amazon.com/dp/B01E4J6S4O/ref=cm_sw_em_r_mt_dp_U_K-wkDbQWQD8XT

\$22.93

Vintiquewise(TM) Decorative Treasure Box - Wooden Trunk Chest

https://www.amazon.com/gp/product/B004VG9LHW/ref=ppx_yo_dt_b_asin_title_o01_s01?ie=UTF8&psc=1

\$30.85

Retroworks Classic Caesar Cipher Medallion Silver Decoder Ring

https://www.amazon.com/dp/B004D1L0B0/ref=cm_sw_em_r_mt_dp_U_1.wkDbE3FFXDW

\$18.99