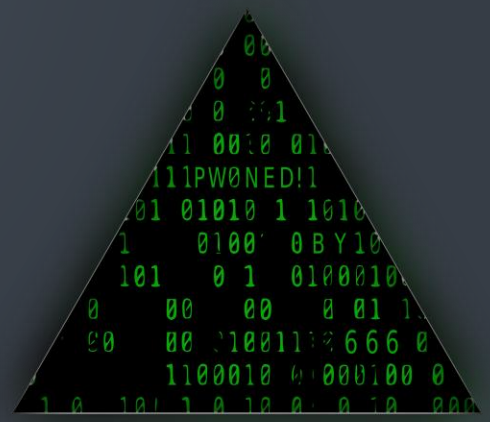
CRACKING PASWORD 101

@INFRN0

INFOSEC, LINUX LOVER, REDTEAMER,
RESEARCHER, SECURITY ANALYST,
DIGITAL FORENSICS, RF ENTHUSIAST

Is your company safe?



AGENDA

- Diccionario
- Fuerza bruta
- Combinado
  - Híbrido
    - Máscaras + Dic
    - Dic + Máscaras
  - Rules

ATAQUE DE DICCIONARIOS COMBINADOS

- El ataque de diccionarios combinados, como su nombre lo dice solo es combinar dos dicconarios.
- Dic_a.txt
- Dic_b.txt
- hashcat -a 1 -m 1000 hash_NTLM.txt -o res.log rockyou.txt names.txt

ATAQUE CON MÁSCARAS

- LAS MASCARAS ES UN ATAQUE QUE PRUEBA TODAS LA COMBINACIONES DE DETERMINADO TIPO DE CARACTERES EJEMPLO:

  - ?l = abcdefghijklmnopqrstuvwxyz
  - ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - ?d = 0123456789
  - ?h = 0123456789abcdef
  - ?H = 0123456789ABCDEF
  - ?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
  - ?a = ?l?u?d?s
  - ?b = 0x00 - 0xff

DICCIONARIOS

Mp64.bin

- https://github.com/hashcat/maskprocessor

Crunch

- https://github.com/jim3ma/crunch

Mentalist

- https://github.com/sc0tfree/mentalist

Hashcat Utils

- https://github.com/hashcat/hashcat-utils

1337_SPEAK_DIC

- https://github.com/mustis-tyr/1337_SPEAK_DIC

coronavirus

hashcat -a 3 -m 1000 hash_NTLM.txt -o RES.log -i -1oO0 -2aA4@ -3il1 -45sS C?1r?1n?2v?3ru?4?a?a?a?a?a --increment --increment-min=12 --increment-max=15

diciembre

hashcat -a 3 -m 1000 hash_NTLM.txt -o RES.log -i -1il1 -2eE3WwMm D?1c?1?2mbr?2?a?a?a?a?a --increment --increment-min=12 --increment-max=14

noviembre

hashcat -a 3 -m 1000 hash_NTLM.txt -o RES.log -i -1oO0 -2eE3WwMm -3il1 N?1v?3?2mbr?2?a?a?a?a --increment --increment-min=12 --increment-max=15

septiembre

hashcat -a 3 -m 1000 hash_NTLM.txt -o RES.log -i -1il1 -2eE3WwMm S?2pt?1?2mbr?2?a?a?a?a?a --increment --increment-min=12 --increment-max=15

ATAQUE CON MÁSCARAS

ATAQUE HÍBRIDO

```
hashcat -a 3 -m 1000 hash_NTLM.txt -o RES.log /home/mustis/NO_Trust_Sec/Tools/MASK/Corporate_Masks/corp_14.hcmask
```

```
hashcat -a 7 -m 1000 hash_NTLM.txt -o RES.log ?a?a?a?a names.txt --increment --increment-min=4
```

- ?a?a?a?a+Catalina

```
hashcat -a 6 -m 1000 hash_NTLM.txt -o RES.log names.txt ?a?a?a?a --increment --increment-min=4
```

- Catalina+?a?a?a?a

ATAQUE CON RULES HASHCAT

- Los ataques con Rules de hashcat, son un tipo de reglas las cuales hacen cambios en las palabras que se van procesando.

Name	Func-tion	Description	Example Rule	Input Word	Output Word	Note
Nothing	:	Do nothing (passthrough)	:	p@ssW0rd	p@ssW0rd	
Lowercase	l	Lowercase all letters	l	p@ssW0rd	p@ssw0rd	
Uppercase	u	Uppercase all letters	u	p@ssW0rd	P@SSW0RD	
Capitalize	c	Capitalize the first letter and lower the rest	c	p@ssW0rd	P@ssw0rd	
Invert Capitalize	C	Lowercase first found character, uppercase the rest	C	p@ssW0rd	p@SSW0RD	
Toggle Case	t	Toggle the case of all characters in word.	t	p@ssW0rd	P@SSw0RD	
Toggle @	TN	Toggle the case of characters at position N	T3	p@ssW0rd	p@sSW0rd	*
Reverse	r	Reverse the entire word	r	p@ssW0rd	dr0Wss@p	
Duplicate	d	Duplicate entire word	d	p@ssW0rd	p@ssW0rdp@ssW0rd	
Duplicate N	pN	Append duplicated word N times	p2	p@ssW0rd	p@ssW0rdp@ssW0rdp@ssW0rd	
Reflect	f	Duplicate word reversed	f	p@ssW0rd	p@ssW0rddr0Wss@p	
Rotate Left	{	Rotate the word left.	{	p@ssW0rd	@ssW0rdp	
Rotate Right	}	Rotate the word right	}	p@ssW0rd	dp@ssW0r	
Append Character	$X	Append character X to end	$1	p@ssW0rd	p@ssW0rd1	
Prepend Character	^X	Prepend character X to front	^1	p@ssW0rd	1p@ssW0rd	
Truncate left	[	Delete first character	[	p@ssW0rd	@ssW0rd	
Trucate right	]	Delete last character	]	p@ssW0rd	p@assW0r	
Delete @ N	DN	Delete character at position N	D3	p@ssW0rd	p@sW0rd	*
Extract range	xNM	Extract M characters, starting at position N	x04	p@ssW0rd	p@ss	* #
Omit range	ONM	Delete M characters, starting at position N	O12	p@ssW0rd	psW0rd	*
Insert @ N	iNX	Insert character X at position N	i4!	p@ssW0rd	p@ss!W0rd	*
Overwrite @ N	oNX	Overwrite character at position N with X	o3$	p@ssW0rd	p@s$W0rd	*
Truncate @ N	'N	Truncate word at position N	'6	p@ssW0rd	p@ssW0	*
Replace	sXY	Replace all instances of X with Y	ss$	p@ssW0rd	p@$$W0rd	
Purge	@X	Purge all instances of X	@s	p@ssW0rd	p@W0rd	
Duplicate first N	zN	Duplicate first character N times	z2	p@ssW0rd	ppp@ssW0rd	
Duplicate last N	ZN	Duplicate last character N times	Z2	p@ssW0rd	p@ssW0rddd	
Duplicate all	q	Duplicate every character	q	p@ssW0rd	pp@@ssssWW00rrdd	
Extract memory	XNMI	Insert substring of length M starting from position N of word saved to memory at position I	lMX428	p@ssW0rd	p@ssw0rdw0	+
Append memory	4	Append the word saved to memory to current word	uMl4	p@ssW0rd	p@ssw0rdP@SSW0RD	+
Prepend memory	6	Prepend the word saved to memory to current word	rMr6	p@ssW0rd	dr0Wss@pp@ssW0rd	+
Memorize	M	Memorize current word	lMuX084	p@ssW0rd	P@SSp@ssw0rdW0RD	+

ATAQUE CON RULES HASHCAT

SHOWTIME

Is your company safe?

jsalcedo@roguesecurity.io

https://www.roguesecurity.io