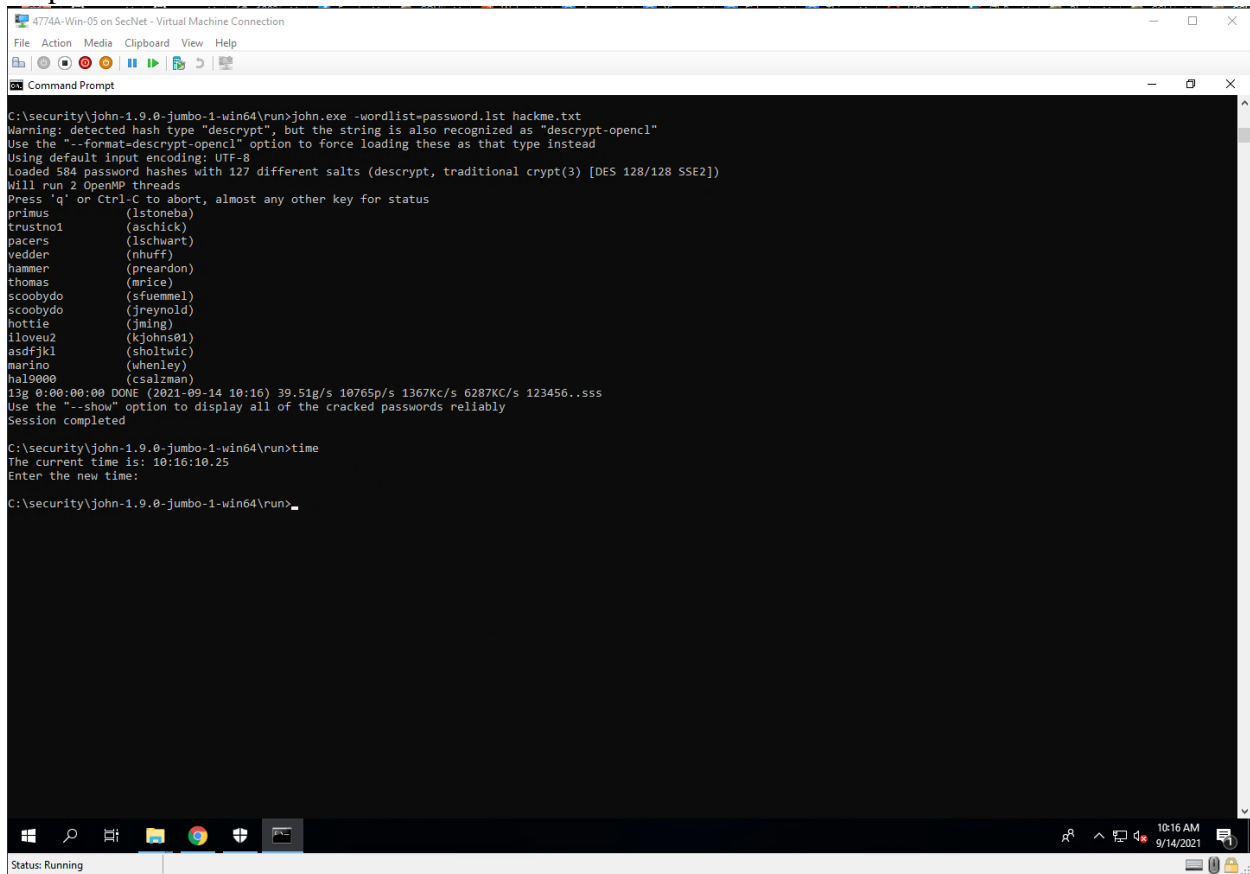


Jamel Douglas
JED18C
Lab 3 – John the Ripper
9/14/2021

6.1 John The Ripper

Screenshots

Step 32

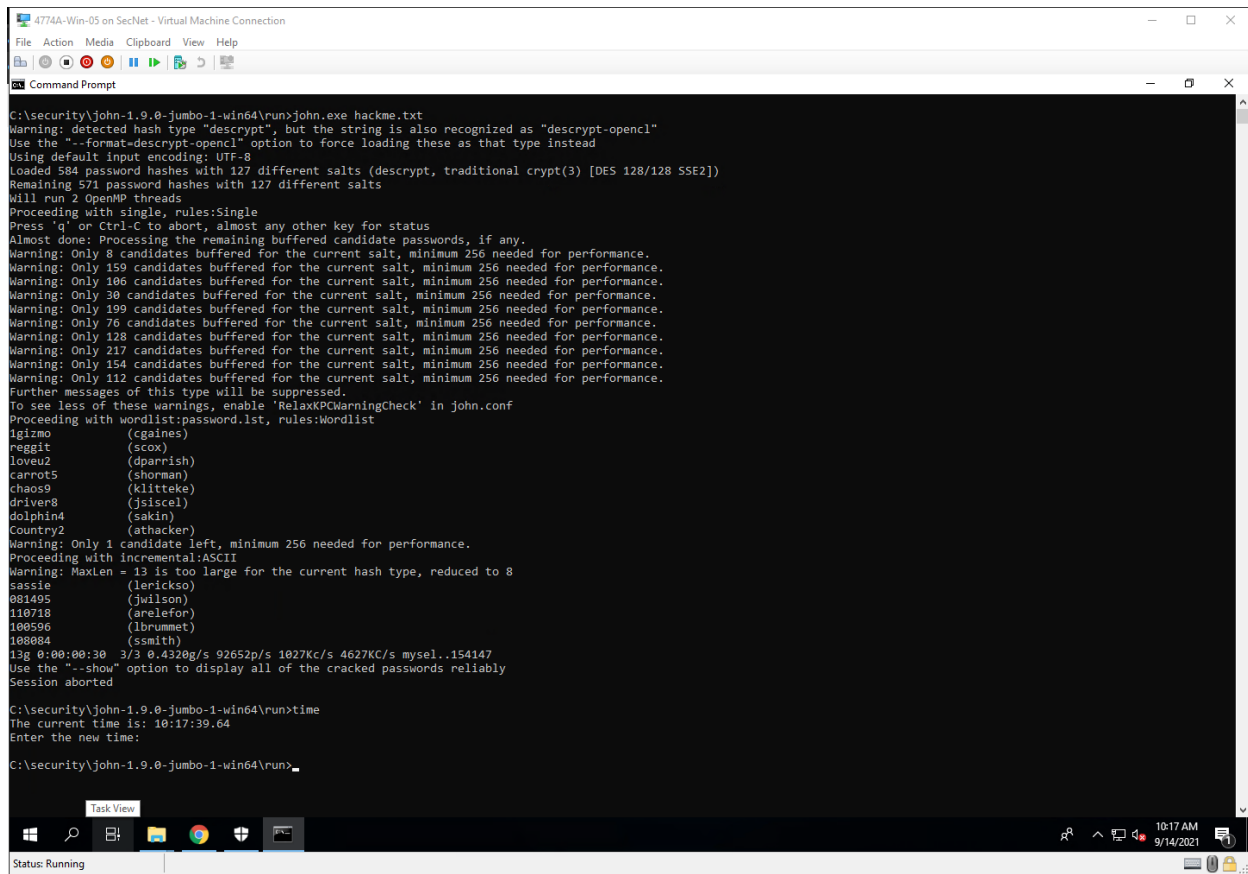


```
C:\security\john-1.9.0-jumbo-1-win64\run>john.exe -wordlist=password.lst hackms.txt
Warning: detected hash type "descrypt", but the string is also recognized as "descrypt-openc1"
Use the "--format=descrypt-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 584 password hashes with 127 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
primus      (1stoneba)
trustno1    (aschick)
pacers      (lschwant)
vedder      (nhuff)
hammer      (preardon)
thomas      (mrice)
scoobydo    (sfuemme1)
scoobydo    (jreynold)
hottie      (jming)
iloveu2     (kjohns01)
asdfjkl     (sholtwic)
marino      (whenley)
hal9000     (csalzman)
13g 0:00:00.00 DONE (2021-09-14 10:16) 39.51g/s 10765p/s 1367Kc/s 6287Kc/s 123456..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed

C:\security\john-1.9.0-jumbo-1-win64\run>time
The current time is: 10:16:10.25
Enter the new time:

C:\security\john-1.9.0-jumbo-1-win64\run>
```

Step 38



```
C:\security\john-1.9.0-jumbo-1-win64\run>john.exe hackme.txt
Warning: detected hash type "descrypt", but the string is also recognized as "descrypt-openc1"
Use the "--format=descrypt-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 584 password hashes with 127 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2])
Remaining 571 password hashes with 127 different salts
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 8 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 159 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 186 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 30 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 199 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 76 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 128 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 217 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 154 candidates buffered for the current salt, minimum 256 needed for performance.
Warning: Only 112 candidates buffered for the current salt, minimum 256 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxPCWarningCheck' in john.conf
Proceeding with wordlist:password.lst, rules:Wordlist
1gizmo (cgaines)
reggit (scox)
loveu2 (dparrish)
carrots (shorman)
chaos9 (klitteke)
driver8 (jsiscel)
dolphin4 (sakin)
Country2 (athacker)
Warning: Only 1 candidate left, minimum 256 needed for performance.
Proceeding with incremental:ASCII
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
eassie (lerickso)
081405 (jwilson)
110718 (arelefor)
100596 (lbrummet)
108084 (ssmith)
13g 0:00:00:30 3/3 0.4320g/s 92652p/s 1027Kc/s 4627Kc/s mysel..154147
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

C:\security\john-1.9.0-jumbo-1-win64\run>time
The current time is: 10:17:39.64
Enter the new time:

C:\security\john-1.9.0-jumbo-1-win64\run>
```

Step 41

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

Command Prompt

john.pot - Notepad

```
C:\>
Warn HI33ZYhDpwuc.:primus
Use L.byvlaonZigg:trustno1
Load mECIdjBG0h2Ac:pacers
Rema 07tkQIcer7Qbw:vedder
Will jValshh6f0vPw:hammer
Proc tJ5x9xeaFUvp0:thomas
Almo XMVe4Gve.6602:scoobydo
Warn fmQCyQ0vuwomIk:scoobydo
Warn patMaWvi.j0GY:hottie
Warn w4eyK4i00TRf2:iloveu2
Warn 39YtFCQVF6uxs:asdFjk1
Warn YvQ641.su13Gg:marino
Warn YvrLGvC4pckFw:ha19000
Warn HdvLS2of3K78g:1gizmo
Warn yD1CPuRU4BC42:reggit
Warn z19U.Kapo1/ec:loveu2
Furt 7FkvdufnGYyLU:carrot5
To s F5XbU8LDjkMPY:chaos9
Proc Z6efMPpj.2N92:driver8
Igit T1XVhoYmleone:dolphin4
regg gY6JukSPaIXbE:Country2
love GE2LSo/6nJ3mw:sassie
carr KMrtDydjk8qGE:081495
chao 3W2puOheaD2Ac:110718
driv 56H8XTCXnHJRg:100596
dolo H2.QQZA6Wjo1s:108084
Coun
Warn
Proc
Warn
sass
0814
1107
1005
108084
13g 0:00:00:30 3/3 0.4320g/s 92652p/s 1027Kc/s 4627Kc/s mysel..154147
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

C:\security\john-1.9.0-jumbo-1-win64\run>time
The current time is: 10:17:39.64
Enter the new time:

C:\security\john-1.9.0-jumbo-1-win64\run>notepad john.pot

C:\security\john-1.9.0-jumbo-1-win64\run>
```

Task View

Status: Running

10:18 AM 9/14/2021

Project Questions

1. The dictionary force attack cracked 13 passwords.
2. The brute force attack cracked 26 passwords.
3. I let the brute force attack run for about 30 seconds.
4. JTR made approximately 0.432 guesses per second.

Thought Questions

1. The cracking program cracks passwords in one of two ways. A dictionary attack tries a predefined list of passwords. A brute force attack tries any combination of characters.
2. Password crackers can crack any password through a brute force attack, however stronger passwords will make that process take significantly longer.
3. I think that if you were to use a larger dictionary, it would take longer crack passwords because there is more to reference.
4. Yes, JTR does support using foreign language word lists.

6.6 Password Evaluator

Screenshots

Step 4

The screenshot shows a web browser window titled "GeodSoft Password Evaluator/Checker" running on a virtual machine. The browser address bar shows the URL: `geodsoft.com/cgi-bin/pwcheck.pl?form=used&password=PoincianaDouglas08$&minPWL=15&minDWL=8&maxDWL=30&maxDW=1&maxWLR=0.66&maxCO=0...`. The page features a blue header with the GeodSoft logo and navigation links. The main content area displays the password "PoincianaDouglas08\$" with a length of 19 and a strength of 24. It also shows a list of settings for password evaluation, including minimum password length, dictionary word length, and various character and pattern requirements. The settings are listed in a table with checkboxes and input fields. The right sidebar contains a "Site map" with links to various resources. The bottom status bar indicates the virtual machine is running.

GeodSoft

Password Evaluator/Checker

Password: PoincianaDouglas08\$ Length = 19, Strength = 24
Dict. words = poinciana
Contains dictionary word poinciana

PoincianaDouglas08\$ Password [Submit] [Instructions for Password Evaluator](#)

NEW SETTINGS for minimum 15 character passwords: use the [original settings](#) for 6 character passwords or try the [suggested settings](#) for 12 character passwords.

- ☐ [Check Passwords for Systems Using LM Hashes](#)
(Pre Vista Windows and Other Systems)
- 15 [Minimum Password Length](#)
- 8 [Minimum Dictionary Word Length](#)
- 30 [Maximum Dictionary Word Length](#)
- 1 [Maximum Dictionary Words](#)
- 0.66 [Maximum Word Length Ratio](#)
- 0.8 [Maximum Character Occurrences \(count > 1, ratio < 1\)](#)
- 0.6 [Minimum Duplicate or Mirrored Sequence Length \(C\)](#)
- 0.5 [Maximum Sequence Characters \(C\)](#)
- 0.5 [Maximum Repeat Characters \(C\)](#)
- 0.45 [Maximum 2 Character Pattern Repeats \(C\)](#)
- 0.4 [Maximum 3 Character Pattern Repeats \(C\)](#)
- 0.3 [Maximum 4 Character Pattern Repeats \(C\)](#)
- 0.99 [Maximum Vowels Only \(C\)](#)
- 0.99 [Maximum Consonants Only \(C\)](#)
- 0.8 [Maximum Digit Ratio for Full Strength Estimate](#)
- ☒ [Do Not Allow All Digits](#)
- ☐ [Do Not Allow Phone Numbers](#)
- ☐ [Do Not Allow Dates](#)
- ☐ [Do Not Allow Social Security Numbers](#)
- ☒ [Check Words Across Non Letters](#)
- 2 [Additional Minimum Word Length when checking words across non letters](#)
- 0.75 [Maximum Suffix Word Length Ratio](#)

[Home](#) >
[CGI Scripts](#) >
[pwcheck.pl](#)

[What's New](#)
[How-To](#)
[Opinion](#)
[Book](#)

[Email address](#)

Site map:
[Home](#)
[What's New](#)
[About GeodSoft](#)
[Large Web Project](#)
[Designing GeodSoft](#)
[Building GeodSoft](#)
[How-To](#)
[Good Passwords](#)
[10 Security Steps](#)
[Intrusion Detection](#)
[Secure Shell \(SSH\)](#)
[Harden OpenBSD](#)
[Dual Boot Open Source](#)
[Style Sheets \(CSS\)](#)
[Time Synchronization](#)
[Reviews & Commentary](#)
[Product Packages](#)
[Software Licenses](#)
[Open Source Limits](#)
[Server Comparison](#)
[Bogus PHP Bug](#)
[Corel Linux](#)
[Book Assn. Webs](#)
[Introduction](#)
[Network & Web Basics](#)
[Assn. Computer Security](#)
[Publishing Myth](#)
[Terms of Use](#)
[Privacy Policy](#)

[Password Generator](#)

Status: Running


Step 7

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

GeodSoft Password Evaluator/Checker

Not secure | geodsoft.com/cgi-bin/pwcheck.pl?form=used&password=%24EstridgeMiddleDouglas08%21&minPWL=15&minDWL=8&maxDWL=30&maxDW=1&maxWLR=0.66&...

 **GeodSoft**

Password Evaluator/Checker

Password \$EstridgeMiddleDouglas08! Length = 25, Strength = 35
Dict. words = estridge
Contains dictionary word estridge

Password [Instructions for Password Evaluator](#)

NEW SETTINGS for minimum 15 character passwords: use the [original settings](#) for 6 character passwords or try the [suggested settings](#) for 12 character passwords.

☐ [Check Passwords for Systems Using LM Hashes](#)
(Pre Vista Windows and Other Systems)

15	Minimum Password Length
8	Minimum Dictionary Word Length
30	Maximum Dictionary Word Length
1	Maximum Dictionary Words
0.66	Maximum Word Length Ratio
0.8	Maximum Character Occurances (count > 1, ratio < 1)
0.6	Minimum Duplicate or Mirrored Sequence Length (")
0.5	Maximum Sequence Characters (")
0.5	Maximum Repeat Characters (")
0.45	Maximum 2 Character Pattern Repeats (")
0.4	Maximum 3 Character Pattern Repeats (")
0.3	Maximum 4 Character Pattern Repeats (")
0.99	Maximum Vowels Only (")
0.99	Maximum Consonants Only (")
0.8	Maximum Digit Ratio for Full Strength Estimate
<input checked="" type="checkbox"/>	Do Not Allow All Digits
<input type="checkbox"/>	Do Not Allow Phone Numbers
<input type="checkbox"/>	Do Not Allow Dates
<input type="checkbox"/>	Do Not Allow Social Security Numbers
<input checked="" type="checkbox"/>	Check Words Across Non Letters
2	Additional Minimum Word Length when checking words across non letters
0.75	Maximum Suffix Word Length Ratio

[Home](#) >
[CGI Scripts](#) >
[pwcheck.pl](#)

What's New
[How-To](#)
[Opinion](#)
[Book](#)

[Email address](#)

Site map:
[Home](#)
[What's New](#)
[About GeodSoft](#)
[Large Web Project](#)
[Designing GeodSoft](#)
[Building GeodSoft](#)
[How-To](#)
[Good Passwords](#)
[10 Security Steps](#)
[Intrusion Detection](#)
[Secure Shell \(SSH\)](#)
[Harden OpenBSD](#)
[Dual Boot Open Source](#)
[Style Sheets \(CSS\)](#)
[Time Synchronization](#)
[Reviews & Commentary](#)
[Product Packages](#)
[Software Licenses](#)
[Open Source Limits](#)
[Server Comparison](#)
[Bogus PHP Bug](#)
[Core! Linux](#)
[Book Assn. Webs](#)
[Introduction](#)
[Network & Web Basics](#)
[Assn. Computer Security](#)
[Publishing Myth](#)
[Terms of Use](#)
[Privacy Policy](#)

[Password Generator](#)

Status: Running

10:37 AM
9/14/2021

Project Questions

1. My normal password was 19 characters long.
2. My strong password was 25 characters long.
3. My normal password has a number at the end of it.
4. The password with a repeated word had issues because by default, the security option “Maximum Dictionary Words” is set to 1.

Thought Questions

1. It’s a phrase that, although makes no sense to most people, makes sense to me and is easy for me to remember.
2. I would hope so. That way others’ passwords would be more secure because its not a basic password. It is also better because it is harder to remember complex passwords.
3. Yes, hackers know what patterns users use to choose their passwords, and they use that knowledge to further their goals.
4. No, I don’t use the same password for every account. I have my main password that allows me to access my password vault where I have passwords stored