

Capture The Flag

NAME: MICHAEL LAMBINICIO

TEAM NAME: R3JVDXAGMQ0=

Introduction

- The CTF Problem = Find Princess Leia's password.
- Steps to Solve === Start with Notepad++ & hash decrypter.
- The Solution ==== Decrypt the hash associated with Leia.
- Workplace Relevance = Medium to High

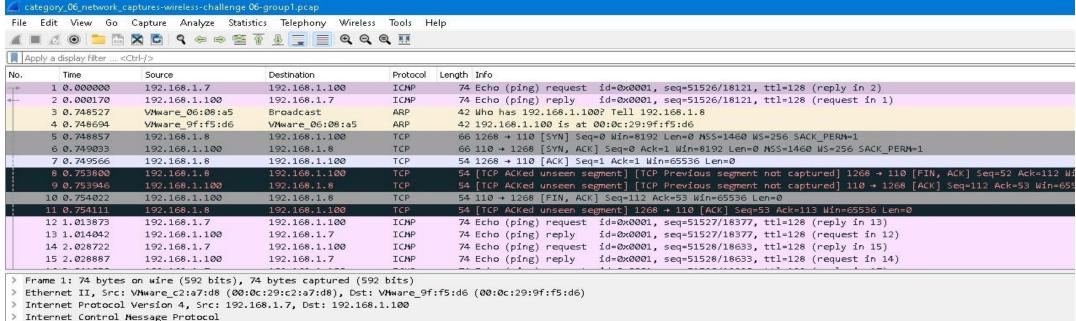


CTF Category Description

- Objective
 - The CTF provided a Packet Capture file to find Princess Leia's password
- Methods to solve
 - Utilizing different applications and techniques to search for certain information within the Packet Capture file
- Relation to Ethical Hacking
 - Searching within packet captured files can get you useful information about network activity and sensitive information
- Labs utilized for this problem
 - From EC-Council
 - Module 3 Scanning Networks



Introduction to the Problem



Started with Wireshark (ver. 3.6.4) to see if I can filter out and find the username



File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?



Unsuccessful through Wireshark, had to move to another application. Notepad++

(ver. 8.3.3)

```
🔚 category 06 network captures-wireless-challenge 06-group1.pcap 🔀
          NULJNULNULNULNULNULNULNULNULNULNI) Ÿöönulff) âşøbsnulenulnul<a(nulnulesohušà"sohbelà"sohabsnul
           NULSOHÉMabcdefghijklmnopgrstuvwabcdefghil] "
           Nuojnuonuojnuonuojnuonuonuopp) ås⊘nuopp) Ÿööesnuoenuonuo<u-nuonuo∈sohaeà"sohaà"sohabnuonuor
          NULSOHÉMADO defghijklmnopqrstuvwabo defghij Hæfnonul*Nulnulnul*Nulnulnulÿÿÿÿÿnulff) Ÿöößacknulsohbsnulackfotnulsohnulff) Ÿööà Sohdnulnulnulnulnul
           NULJNULNULNULNULNULNULNULPP) ŸöÖNULFF) ÂŞØBSNULFNULNUL<a|NULNUL€SOHU‱À"SOH(BELÀ"SOHdBSNUL FRNULSOHÉNabcdefghijklmnopqrstuvwabcdefghij] BD
           NUDJNULNULNULNULNULNULNULNULNI) ÅŞØNULFP) ŸÖÖBSNULENULNUL<u:\NULNULSOHAcà"SOHAcà"SOHBELNULNULGFFNULSOHÉNabcdefghijklmnopqrstuvwabcdefghik]
          NULJNULNULNULNULNULNULNULNULNULTE) ŸöÖNULFE) Å$ØBSNULFNULNUL<a) NULNUL€SOHU^ À"SOH(BELÀ"SOHdBSNUL "VINULSOHÉOabcdefghijklmnopqrstuvwabcdefghik] iz
          NUMINUMNUMINUMNUMNUMNUMNUMNUMINI) Yöönumini) \hat{a}søbenumenumnum\langle a \simnumnum\epsilonsohu\epsilonà" sohubenium\omega
           NULSOHÉPabcdefghijklmnopqrstuvwabcdefghiL] ü³
          nuljnulnuljnulnulnulnulnulnultt) åsønultt) yööbsnulenulnul<usnulnulesoha^à" sohaà" sohbelnulnult
          NULJNULNULNULNULNULNULNULNULNI) ŸöÖNULT?) ÂŞØBSNULENULNUL<ADELNULNULNULESOHU†À"SOHBELÀ"SOHBESNUL, NULSOHÉQabcdefghijklmnopgrstuvwabcdefghim] Lê
           nudjnudnudjnudnudnudnudri) âşønudre) yöörsnudenudnud<u²nudnudesoha[àˈsohdàˈsohgednudnude
                                                                                                                                                                                                         NULSONÉQabcdefghijklmnopgrstuvwabcdefghiN] OæMONU
  17
  18
           NULJNULNULNULNULNULNULNULNULFP) ŸööNULFP) ÅŞØBSNULENULNUL<a%NULNUL€SOHU|À"SOHBELÀ"SOHdBSNULfŸNULSOHÉ[abcdefqhijklmnopqrstuvwabcdefqhiw] ó
  19
  20
          NULJNULNULNULNULNULNULNULNULNULNULNI) ŸöÖBSNULENULNUL<br/>NULNULSOHATÄ" SOHATÄ" SOHBELNULNUL<br/>
VINULSOHAT [abcdefghijklmnopqrstuvwabcdefghix] USA
          NULJNULNULNULNULNULNULNULNULNULNULNULNI) ÄSØESNULENULNUL<ašnulnulesohu(à sohueblà sohuebnulpnulsohé\abcdefghijklmnopqrstuvwabcdefghix) ÉA
          NULJNULNULNULNULNULNULNULNULNULNI) ŸöÖBSNULENULNUL<br/>
vulnulnulsohd`sohednulnul<br/>
valnulnulnulsohd\sohednulnul<br/>
valnulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulnulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohednulsohd\sohed
          NULJNULNULNULNULNULNULNULNULNULNI) ÅŞØBSNULENULNULNUL<br/>(ak NULNULSOHUZÀ" SOHBELÀ" SOHBELÀ"
          NULJNULNULNULNULNULNULNULNULNULNULNULNULNUL (
ŠØNULTI) YÖÖESNULENULNUL</br>
          NUL*NULNULNULNULNULNULNULNULNULFF) ACKESYNULFF) ŸÖÖBSACKNULSOHESNULACKEOTNULSOHNULFF) ŸÖÖÀ"SOHANULFF) ACKESYÀ"SOHESD] **
           nul*nulnul*nulnulnulnulnult) åsønult) jööbsacknulsohbsnulackeodnulsohnult) jööà" sohdnult) åsøà" sohbell si
          NUL*NULNUL*NULNULNULNULNULT?) ŸÖÖNULTE) ÂŞØESACKNULSOHESNULACKEOTNULSTXNULTE) ÂŞØÄ" SOHEELNULT?) ŸÖÖÄ" SOHEM] D, STXNULJNULNULNULNULNULNULNULNULT?)
          =:) Kanudnudnudnud `Stresnud ` nudnudstreotenoʻo] | Cteacenud: nudnudnud: nudnudnudnudnudnud a 2 nudce) a 2 nudce) astesnude nudnud, *potinudnud ' acrjvà" soheà" sohi¬-< so
  34
                  NULNULALKÖ^À" SOHEÀ" SOHT¬<NULSYN:) KMNULNULNULNULNUL STXEOTNULÝ HULNULSTXEOTENO ° 0]
          $FRNUL: NULNULNULNULNULNULNULNULNULNUL) $ 2NULFR) dSIESNULENULNUL, LANULNULSACK («À" SOHEÀ" SOHT ¬ < NULFER: ) KANULNULNULNULNULNULNUL STRESNULÙ † NULNULSTREOTENO (° )
          à some à som -; nuldca: (K¿nulnulnulnul stresnulù šnulnulstreoteno o s+sonul: nulnulnul nulnulnulnulta) à ?nulga) dsdesnule nulnul, cî nulnul; cch ; "
          : (Kandendendenden) stresnueù nudaudstreoreng (d) en sonue: nudaudaud nudaudauden) à ?nuden) delesaudendende, t'' nudaudo ackdeda à "sohe à "s
```



Hit "search" in the top tab and select "Find..."

File	Edit	Search Communication Company Search	.ungs 1001s Iviacro	Run Plugins Window ?
6	H	Find	Ctrl+F	
ea	tegory	Find in Files	Ctrl+Shift+F	
1	ÔÃ	Find Next	F3	
2	M	Find Previous	Shift+F3	WUNWUNUœNWUNWU€DC180À"SOHdÀ"SOHÿNWU‱NWU‰NWU:]€
3	(M)	Select and Find Next	Ctrl+F3	ulenulnul <a{ "sohbelà"="" nulnul∈sohušà="" sohdbsnul"<="" td=""></a{>
5	OM .	Select and Find Previous	Ctrl+Shift+F3	ulenulnul <u nulnulesohaeà"sohdà"sohbelnulnule<="" td=""></u>
6	ON O	Find (Volatile) Next	Ctrl+Alt+F3)MIN + MINUMINAM + MINUMINAM - ŸŸŸŸŸŸMINŒP) ŸÕÖBSACKAM
7	(M)	Find (Volatile) Previous	Ctrl+Alt+Shift+F3	ulenulnul <a nulnulesohu&à"sohbelà"sohdesnul, fr<br="">ulenulnul<u¢nulnulesohacà"sohdà"sohbelnulnuler< td=""></u¢nulnulesohacà"sohdà"sohbelnulnuler<></a nulnulesohu&à"sohbelà"sohdesnul,>
9	äŒ	Replace	Ctrl+H	icknulsohbsnulickeotnulsohnulff) Ÿööà" sohdnuln
10		Incremental Search	Ctrl+Alt+l	ulenulnul <a}nulnulesohu^à"sohbelà"sohdbsnul,.w< td=""></a}nulnulesohu^à"sohbelà"sohdbsnul,.w<>
11 12	(M)	Search Results Window	F7	ULENUINUI <u×nuinui€sohaaà"sohaà"sohbeinuinuien ULENUINUI<a~nuinui€sohu‡à"sohbeià"sohdesnui <="" td=""></a~nuinui€sohu‡à"sohbeià"sohdesnui></u×nuinui€sohaaà"sohaà"sohbeinuinuien
13	M	Next Search Result	F4	
14 15		Previous Search Result	Shift+F4	ulenulnul <usnulnul∈soha^à"sohdà"sohbelnulnule Bnul+nulnulnul+nulnulnulÿÿÿÿÿnulen)ÿööbsackn</usnulnul∈soha^à"sohdà"sohbelnulnule
16	7000	Go to	Ctrl+G	ulenunul <adelnulnulesohu+à" sohbelà"="" sohdbsnul,<="" td=""></adelnulnulesohu+à">
17	OM .	Go to Matching Brace	Ctrl+B	ULENUUNUL <u² [à"="" nuunul€="" soha="" sohbeunuunule<="" sohdà"="" td=""></u²>
18 19		Select All Between Matching Braces	Ctrl+Alt+B	ULENUINUI≺a‰NUINUL€SOHU À″SOHBELÀ″SOHdBSNUL∫ÿN
20		Mark	Ctrl+M	DECEMBRIDA CONTROL A SOURCE NO A
21	M			— ulenulnul <uç "sohdà"="" nulnul∈sohaf="" sohbelnulnul<="" td="" à="" ÿ<=""></uç>
22	OM .	Style All Occurrences of Token	>	> ulenulnul <ašnulnul@sohu{à"sohbelà"sohdesnulfpn< td=""></ašnulnul@sohu{à"sohbelà"sohdesnulfpn<>
23	NI NI	Style One Token	>	, wenuenue <uánuenue "sohdà"="" (þ<="" sohadà="" sohbelnwenue="" td=""></uánuenue>



Type in "leia" to search the name and click "Find All in Current Document"

SNUJENUJNUJ<usnujnujesoha^à"sohaà"sohbeunujnuje BfBSNUB*NUBNUBNUB*NUBNUBYYYYYYNUBB) Yööbsacknubsohbsnubackdornubsohubbo) Yöäl"sohdnubnubnubnubnubnubnubnub - 66 SNUJENUJNUJ-(alijanujnuje Sohut à "Sohuanà" Sohusanà, nujsohé Qabodefqhi jklmnopqrstuvy bodefqhi M. Lê SOUDENUMUUK (u*NUMUUK SORA [À " SORAÀ " SORREMNUMUUM NUBSONEQabcdefghijklmnopqrsturabcdefghin] Omennun *NUBNUUNUS *NUBNUUNUS NUBNUUNUS YVYYYY AFF) Yöössin SNUBENUBNUS at NUBNUS SOBU | À SOBBED À SOBBEN À SOBBENUB F (abcdef ghijklmnop grst w sabcdef ghi V) 6 SNUBENUBNUS<u/>
nubnus€SOHAFÀ"SOHdà"SOHBESNUBNUS

yNUBSOHÉ[abcdefghijklmnopqr/tuvwabcdefghix] USA SNUJENUJNUJ<ašNUJNUJ€SOBU(À"SOBSDÀ"SOBSBRUJFÞNUJSOBÉ\abcdefghijklmnopg stuvvabcdefghiX] ÉA **SNUJENUJNUJ**<a< **NUJNUJESOH**UZÀ"**SOHEEL**À"**SOHEEL**À"**SOHESNUJ**fý**NUJSOH**É] abcdefghijklmno<mark>j</mark>qrstuvwabcdefghiY] < y SNUBENUBNUS-vänubnus-sohaak Sohda Sohda Nubnusnus ynubsohé abcdefghijkly lopgrstuvwabcdefghiz] – Då Snonus-nubnubnus nubnubnubny byyyyynubsis) Yöössker SNUBENUBNUB<aCNUBNUBESOHUyà"SOHOHÀ"SOHOSHÀ"SOHOSNUBfüNUBSOHÉ^abcdefghijklyhopqrstuvwabcdefghi2] µi SNULENULNUL
 SOHOL SOHBELINU Find O*NUT (WANUAYYYYYYNWAET) ŸÖÖESE YÖÖBSKORNUURSOHBSNUURKORDONNUURSOHNUURFE) YÖÖÀ BSVBSIACKNULISOHIBSINULIACKIEOTINULISTXINULIFF) ACKIE Find Replace Find in Files Firm Projects Mark DF () İSØ**GSNUD**ENUONUO<a"NUONUO SIACKINULISOHIBSINULIACKIEOTINULISOHINULIFFI) ŸÖÖÄ" SOH ISACRNULSONESNULACREOTNULSTANULET) Å50Å" SON Find what : leial **ØBSNUJENUJNUJ**<až**NUJNUJ€SO**HUg Find Next **B, MOR**ÓOÀ"**SOR**eÀ"**SOR**¬<**SOR**»:)K%(Maria (1994) - Alian de la company de la com Count RECURSION COMPRESSION STREET NUONUONUO STYREOTINUO Ý + NUONUO STYREOTIEMO (° °) In selection Find All in Current a) dengenusenusnus, lanusnus stor («à " soile à " sto INDONUS: NUONUSNUSNUSNISS) à ?NI Document NUMŮŠNUMNUMSTVÆROTENO O S‡SONUM: NUMNUMNUM: 9 ¬; GESO: (K/NUDNUDNUDNUD`STR(Backward direction O'O] EM'SONUS: NUONUONUS: NUONUONUONUONUORES) à Find All in All Opened UD STREET NUMBER OF STREET OF SECOND : NUMBER OF STREET OF SECOND : NUMBER OF STREET O Match whole word only Documents SOBe A SOB ¬; NUOB: (K/ NUONUUNU UNURANUASIWASIWASIWASIWASIWANIA pj 6ÚNIUANIUA: NUANUANIUA: (SOH ¬<1~:) K%NUUNNUUNNUUN STURE Match case Close NUMBO (q' OMERCESSURAUMO), SUMEDISCIE SUME M2 NOW NA SOME A SOM -< NUM Wrap around p] XâNUANUA: NUANUANUA: NUANUANUANUANUAN OCINERALIDARIDA À RIDACIDARIZA : RIDACIDA NUO STREENUO / NUONUOSTREOTENO (p) Tänuonuo őÀ SOBEÀ SOB ¬<NUSC:) K⊀NUSNUS Search Mode Transparency (CNO'p) COPASTENDE: NUCLUONUS : NUCLUONUS NUCL O Normal On losing focus ano pj gastanus: nuonuonus: nuonuonuonuonuosis) à Extended (\n, \r, \t, \0, \x...) O Always Dôb**nudnudstwicknicko** pj ôa**stwinud: nudnudnud: n**i B¬; CHANO: (K/ NIMBOMBOMBOMB) STAND Regular expression . matches newline WANUA STANDIANUA Î HOMANUASTANC +À"SOHeÀ"SOH¬;SOH>: (K¿NUMNUM a (p. őöskende: audamande: audamandende) à COMO (p) 6: CHARGUS: RUBRUBRUS: RUBRUBRUBRUSCIE) à nudija) dstubbnudenudnud, \$°nudnud. Agrā-a" sohea" soh ¬<soh' :) kanudnudnudnud strajanudôranudnuds INDIA) dSDBBNUDENUDNUD,+NUONUD: RORD×À"SOHEÀ"SOHEA"SOHE): KANUONUDNUDNUDNUDNUD STRIANUDÔ NUONUDSTREOTENO [p] SENOEOTINUD: NUONUDNUD NUONUDNUDNUD A :) KANUUNUUNUUNUUN STAADIENUUS (NUUNUUSTAASONENO 'p] + 3) d**Shesnulenuunuu,** aynuunuus **ac**ráhà" soheà" soh ¬<€ 3) dSNBSNUJENUJANJA, DŽNUJANJASKOK (Ž. SOBEŽ. SOB ¬<BOX :) KANJANJANJANJANJA (SVRCONNJJOŽENIJANJASTREODICNO (p) (6



The results are generated below..

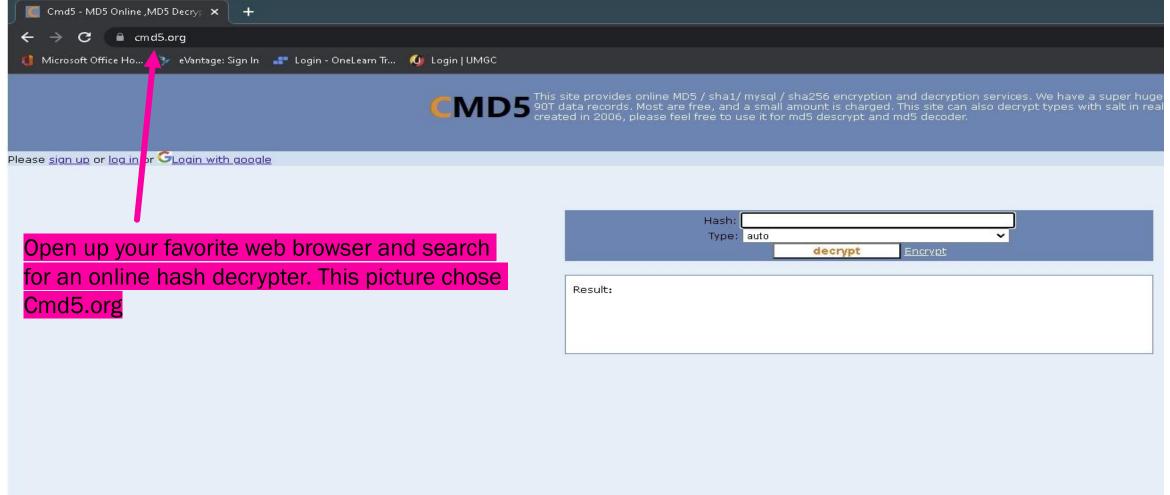
Working Toward a Solution

```
hacker:1004:a9a1d510b01177d1aad3b435b51404ee:afc44ee7351d61d00698796da 6b1ebf:::
       HelpAssistant:1000:56991ec2debe0a22379753c3550506a8:535b8a5cb471c874/15fa13259623614:::
4041
       IUSR WINXP:1017:b38a8793d0549054c29621c527673248:34fb426f13af9aad4a3a85381c11631c:::
4042
       leia:1012:088870ba8ea71662aad3b435b51404ee:4619c592fda516c8140486d2fbf707fc:::
4043
       luke:1011:6a47580eb4df42a5aad3b435b51404ee:e9776ecb486cc1d778 10de53b30588:::
4044
       r2d2:1014:dc2031e004699438aad3b435b51404ee:affe9616fbd19e3a/44447309962e477:::
4045
4046 stormtrooper:1015:dca7d3c500543d6baad3b435b51404ee:c70569/627d5de4c57e4e78e01a14eaa:::
       SUPPORT 388945a0 MOnetCach M: 1002:aad3b435b51404eeaad2.435b51404ee:9765e54143f42ee07ec69cee5b4280c3:::
4047
      vader:1010:7b96b77a223162b1aad3b435b51404ee:2c8a51b3b 2395d6f3623a0b7c4f1cfa:::
4048
      victim:1005:aad3b435b51404eeaad3b435b51404ee:31d6cf_0d16ae931b73c59d7e0c089c0:::
4049
       yoda:1016:828a670f0fd85ea7aad3b435b51404ee:cf7c4e_71bd9d719e05aa399c6f528b5:::
4050
4051
       nulnulnulppnulstxnuleotnulnulnulnuló` þætnul6nulnulnul6nulnulnulpplef) à ?nulff) aslesnulenulnul (ùy@nul@acköñà"sof
       …POPES^ "QNWNWIÔ`_RSg@WNWIJNWNWINWIJN<mark>Y".NWINWINWER</mark>) ŸÖÖNWER) ÂSØBSNWENWINWI<e*NWINWESORQÛÀ"SORBEIÀ"SORdBSNW€NWI
4052
       nul*nulnul*nulnulnulnulff) îsønulff) 🧓 Óbsacknulsohesinulack(eotnulsohnulff) Ÿőöà" sohanulff) îsøà" soh(belú` h‡
4053
       nul*nulnulnul*nulnulnulnulff) yöönulff (ásøbsacknulsohbsnulackeotnulstxnulff) ásøà" sohbelnulff) yööà" sohdû` "?&stxnul*nul
4054
4055
       HOST: 239.255.255.250:1900
4056
       MAN: "ssdp:discover"
       MX: 1
4057
       ST: urn:dial-multiscreen-org:service:dial:1
4058
       USER-AGENT: Google Chrome/86.0 1240.75 Windows
4059
Search results - (1 hit)
 Search "leia" (1 hit in 1 file of 1 searched)
   C:\Users\Hidden Gem\Desktop\CMIT321\Project 2\category 06 network captures-wireless-challenge 06-group1.pcap (1 hit)
     Line 4043: leia:1012:088870ba8ea71662aad3b435b51404ee:4619c592fda516c8140495d2fbf707fc:::
 Search "leia" (1 hit in 1 file of 1 searched)
```

Copy the hash on the far right to decrypt

Normal text file







Arriving at the Solution

• After finding the hash, simply copy and paste it in the Hash text box and hit decrypt to retrieve the password.





Strategies, Pitfalls, Lessons Learned

Strategies

 Using Wireshark to search for the username on the packet capture file did not work. Learned to search within a different application (Notepad++) to obtain the username. Understanding that the password was a hash, used an online decrypter to decrypt and obtain the password.

Pitfalls

Relying on a single application to find the answer.

Lessons Learned

Your first choice of application may not always work in finding the answer you are looking for. Learning other applications can be useful
to jump start your search criteria. Also utilizing online sources to help provide the solutions.



The Relationship to the Workplace

Using alternative methods in finding a solution is highly recommended as sometimes, having only
one method could also be a single point of failure. Having different tactics can expose weaknesses
within their system. But it can also help you strategize on how to prevent it.



Summary

- Sometimes, relying on just one application may not get you the answer you need, even if using technical application such as Wireshark. There are various tools that are simple as notepad that can make searching for usernames easy. When you understand coding and hashes, you then can utilize resources online to complete your problem.
- Most username/passwords aren't show in plain site and sometimes going through different steps with alternate tools are necessary to find them. This shows that your username/password are never truly protected, but why most organizations manage the account policies by having workers change their passwords frequently.



References

- "What is notepad++," Notepad++. [Online]. Available: https://notepad-plus-plus.org/. [Accessed: 26-Apr-2022].
- "Wireshark," Wireshark · Go Deep. [Online]. Available: https://www.wireshark.org/#learnWS. [Accessed: 26-Apr-2022].
- "MD5 online ,MD5 decryption, MD5 Hash Decoder," Cmd5. [Online]. Available: http://www.cmd5.org/. [Accessed: 26-Apr-2022].