STOLEN MOUNT INVESTIGATION - PRE-REPORT - TIER 1 SECURITY ANALYST L1 - MSSP

INFORMATION:

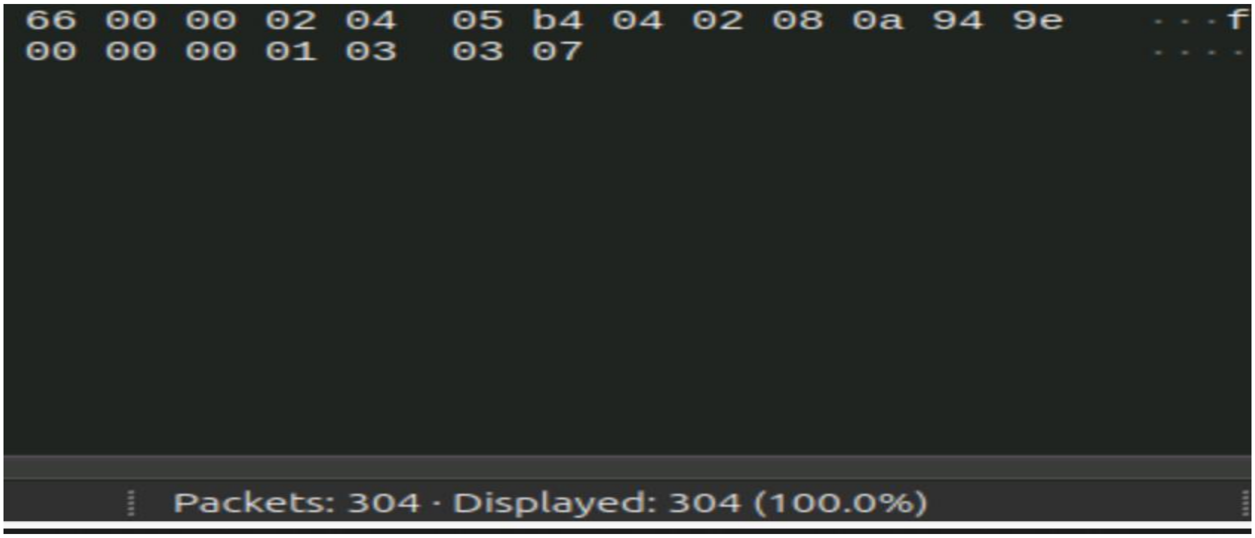
I AM TASKED WITH ANALYSING NETWORK TRAFFIC RELATED TO AN UNAUTHENTICATED FILE SHARE ACCESS ATTEMPT. I AM FOCUSING ON POTENTIAL SIGNS OF DATA EXFILTRATION. THE ADVERSARY'S TARGET IS A NFS SERVER WHERE BACKUP FILES ARE STORED. A CLASSIFIED SECRET WAS ACCESSED & STOLEN. THE ONLY TRACES LEFT BEHIND BY THE ADVERSARY WAS A PCAP FILE DURING THE INCIDENT.

SCOPE:

THE INVESTIGATION IS FOCUED ON A PCAP FILE NAMED 'CHALLENGE.PCAP'. NOT MUCH INFORMATION IS KNOW ON HOW THIS INCIDENT WAS DETECTED BUT WE ARE LOOKING INTO THE POTENTIAL EXFILTRATION OF A CLASSIFIED FILE CONTAINING TOP SECRET INFORMATION. I AM GOING TO BE CONDUCTING MY INVESTIGATION USING WIRESHARK. THE SCOPE WAS LIMITED TO TRAFFIC PRESENT IN THE PCAP FILE & DID NOT INCLUDDE HOST-BASED FORENICS OR ENDPOINT TELEMETRY.

INVESTIGATION:

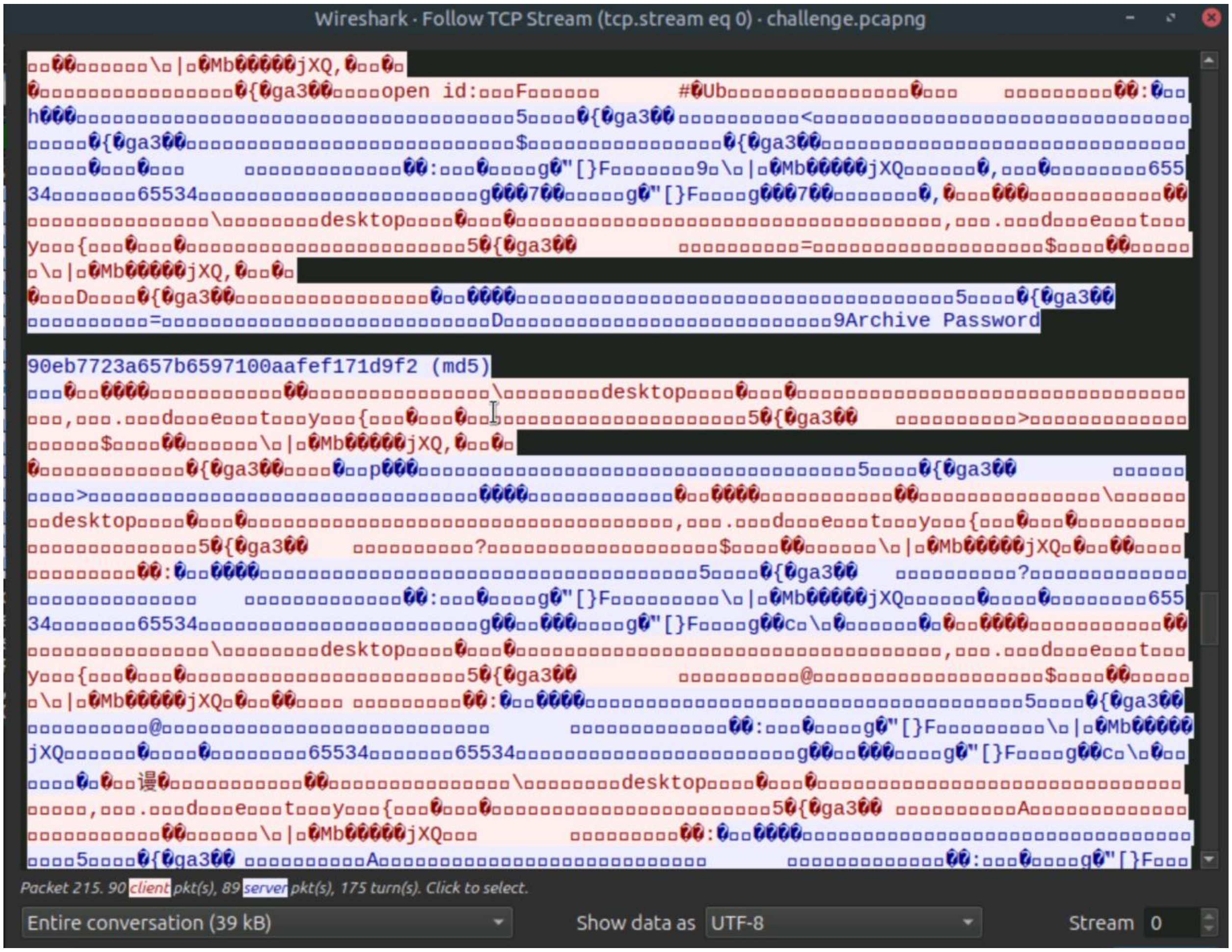
THE TOTAL PACKETS WITHIN THE CHALLENGE.PCAP FILE IS A TOTAL OF 304 PACKETS. WHEN FILTERED FOR NFS SERVER THE TOTAL PACKETS WENT DOWN TO 179 PACKETS.



```
66 00 00 02 04  05 b4 04 02 08 0a 94 9e   ···f
00 00 00 01 03  03 07                     ····
```

Packets: 304 · Displayed: 304 (100.0%)

I FOLLOWED THE TCP STREAM OF ONE OF THE NFS PACKETS & AS I SCROLLED, I ENCOUNTERED A PASSWORD HASHED WITH MD5: 90eb7723a657b6597100aafef171d9f2. I TOOK THIS MD5 HASH TO CRACKSTATION & THE RESULT WAS 'avengers' WHICH IS OUR PASSWORD.



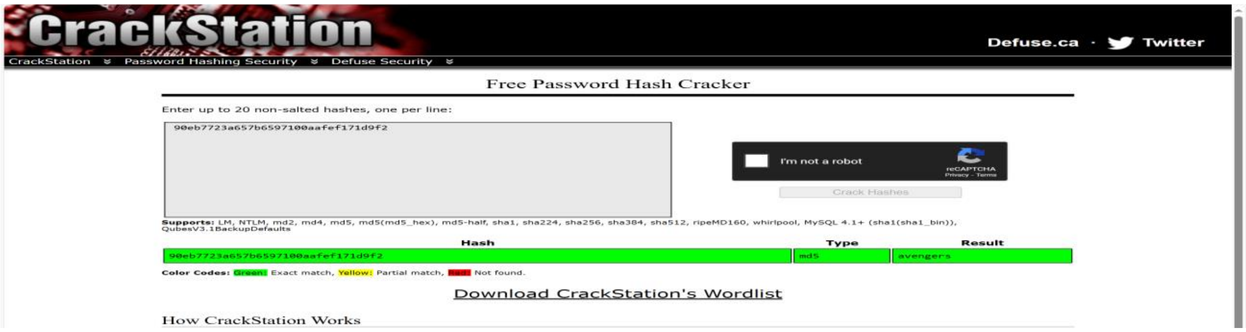
Wireshark · Follow TCP Stream (tcp.stream eq 0) · challenge.pcapng

```
□□��□□□□□□\□|□�Mb�����jXQ,�□□�□
�□□□□□□□□□□□□□□□�{�ga3��□□□□open id:□□□F□□□□□□       #�Ub□□□□□□□□□□□□□□□�□□□    □□□□□□□□□��:�□□
h���□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□5□□□□�{�ga3�� □□□□□□□□□□<□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□�{�ga3��□□□□□□□□□□□□□□□□□□□□□□□□□□□□$□□□□□□□□□□□□□□□□�{�ga3��□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□�□□□�□□□     □□□□□□□□□□□□□��:□□□�□□□□g�"[}F□□□□□□□9□\□|□�Mb�����jXQ□□□□□□�,□□□�□□□□□□□□□655
34□□□□□□□65534□□□□□□□□□□□□□□□□□□□□□□□□□g���7��□□□□□g�"[}F□□□□g���7��□□□□□□□�,�□□□���□□□□□□□□□□□□��
□□□□□□□□□□□□□□□\□□□□□□□□desktop□□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□,□□□.□□□d□□□e□□□t□□□
y□□□{□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□5�{�ga3��        □□□□□□□□□□=□□□□□□□□□□□□□□□□□□□$□□□□��□□□□□
□\□|□�Mb�����jXQ,�□□�□
�□□□D□□□□�{�ga3��□□□□□□□□□□□□□□□□□�□□����□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□5□□□□�{�ga3��
□□□□□□□□□□=□□□□□□□□□□□□□□□□□□□□□□□□□□D□□□□□□□□□□□□□□□□□□□□□□□□□□□9Archive Password

90eb7723a657b6597100aafef171d9f2 (md5)
□□□�□□����□□□□□□□□□□□��□□□□□□□□□□□□□□□\□□□□□□□□desktop□□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□,□□□.□□□d□□□e□□□t□□□y□□□{□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□5�{�ga3��    □□□□□□□□□□>□□□□□□□□□□□□□
□□□□□□$□□□□��□□□□□□\□|□�Mb�����jXQ,�□□�□
�□□□□□□□□□□□□�{�ga3��□□□□�□□p���□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□5□□□□�{�ga3��        □□□□□□
□□□□>□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□����□□□□□□□□□□□□□�□□����□□□□□□□□□□□□��□□□□□□□□□□□□□□□\□□□□□□
□□desktop□□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□,□□□.□□□d□□□e□□□t□□□y□□□{□□□�□□□�□□□□□□□□□
□□□□□□□□□□□□□5�{�ga3��    □□□□□□□□□□?□□□□□□□□□□□□□□□□□□$□□□□��□□□□□□\□|□�Mb�����jXQ□�□□��□□□□
□□□□□□□□��:�□□����□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□5□□□□�{�ga3��    □□□□□□□□□□?□□□□□□□□□□□□□
□□□□□□□□□□□□□□     □□□□□□□□□□□□□��:□□□�□□□□g�"[}F□□□□□□□□□\□|□�Mb�����jXQ□□□□□□�□□□□�□□□□□□□□□655
34□□□□□□□65534□□□□□□□□□□□□□□□□□□□□□□□□□g��□□���□□□□g�"[}F□□□□g��c□\□�□□□□□□�□�□□����□□□□□□□□□□□□��
□□□□□□□□□□□□□□□\□□□□□□□□desktop□□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□,□□□.□□□d□□□e□□□t□□□
y□□□{□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□5�{�ga3��        □□□□□□□□□□@□□□□□□□□□□□□□□□□□□$□□□□��□□□□□
□\□|□�Mb�����jXQ□�□□��□□□□ □□□□□□□□□��:�□□����□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□5□□□□�{�ga3��
□□□□□□□□□□@□□□□□□□□□□□□□□□□□□□□□□□□□□□      □□□□□□□□□□□□□��:□□□�□□□□g�"[}F□□□□□□□□□\□|□�Mb�����
jXQ□□□□□□�□□□□�□□□□□□□□□65534□□□□□□□65534□□□□□□□□□□□□□□□□□□□□□□□□□g��□□���□□□□g�"[}F□□□□g��c□\□�□□
□□□□�□�□□谩�□□□□□□□□□□□□��□□□□□□□□□□□□□□□\□□□□□□□□desktop□□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□,□□□.□□□d□□□e□□□t□□□y□□□{□□□�□□□�□□□□□□□□□□□□□□□□□□□□□□□□5�{�ga3�� □□□□□□□□□□A□□□□□□□□□□□□□
□□□□□□□□□□□��□□□□□□\□|□�Mb�����jXQ□□□       □□□□□□□□□��:�□□����□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□5□□□□�{�ga3�� □□□□□□□□□□A□□□□□□□□□□□□□□□□□□□□□□□□□□□     □□□□□□□□□□□□□��:□□□�□□□□g�"[}F□□□
```

Packet 215. 90 client pkt(s), 89 server pkt(s), 175 turn(s). Click to select.

Entire conversation (39 kB)   Show data as UTF-8   Stream 0



CrackStation
Defuse.ca · Twitter
CrackStation ▾ Password Hashing Security ▾ Defuse Security ▾

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
90eb7723a657b6597100aafef171d9f2
```

□ I'm not a robot

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

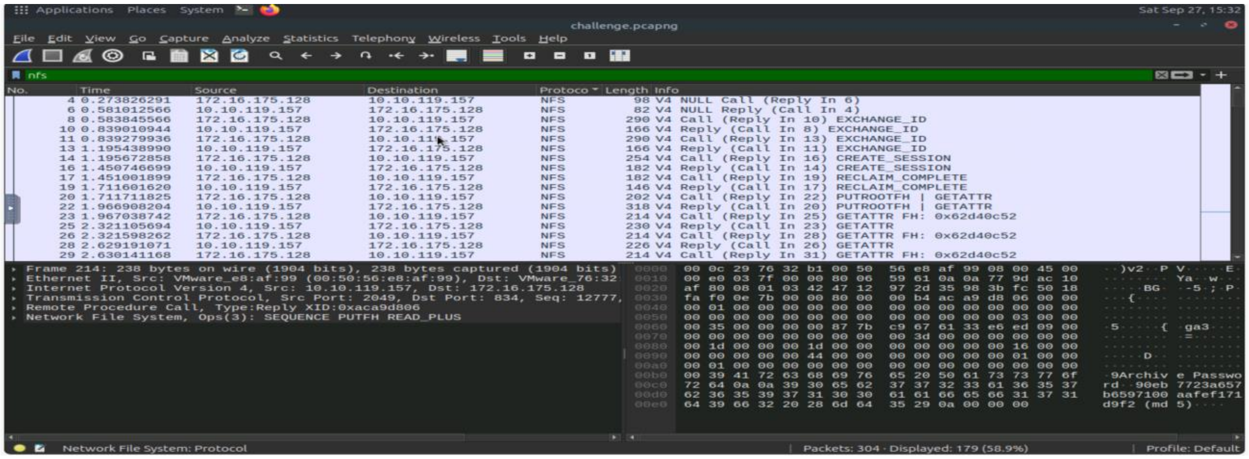
Hash	Type	Result
90eb7723a657b6597100aafef171d9f2	md5	avengers

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

THERE ARE ONLY TWO IP ADDRESSES: 172.16.175.128 & 10.10.119.157. I BELEIVE THE ADVERSARY IS USING THE 172.16.175.128 IP ADDRESS.



Applications Places System
Sat Sep 27, 15:32
challenge.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
nfs

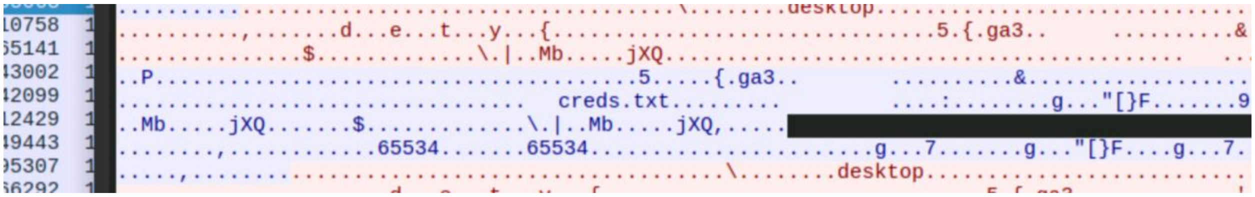
```
No.     Time           Source            Destination       Protoco  Length Info
      4 0.273826291    172.16.175.128    10.10.119.157     NFS        98 V4 NULL Call (Reply In 6)
      6 0.581012566    10.10.119.157     172.16.175.128    NFS        82 V4 NULL Reply (Call In 4)
      8 0.583845566    172.16.175.128    10.10.119.157     NFS       290 V4 Call (Reply In 10) EXCHANGE_ID
     10 0.839010944    10.10.119.157     172.16.175.128    NFS       166 V4 Reply (Call In 8) EXCHANGE_ID
     11 0.839279936    172.16.175.128    10.10.119.157     NFS       290 V4 Call (Reply In 13) EXCHANGE_ID
     13 1.195438990    10.10.119.157     172.16.175.128    NFS       166 V4 Reply (Call In 11) EXCHANGE_ID
     14 1.195672858    172.16.175.128    10.10.119.157     NFS       254 V4 Call (Reply In 16) CREATE_SESSION
     16 1.450746699    10.10.119.157     172.16.175.128    NFS       182 V4 Reply (Call In 14) CREATE_SESSION
     17 1.451001899    172.16.175.128    10.10.119.157     NFS       182 V4 Call (Reply In 19) RECLAIM_COMPLETE
     19 1.711601620    10.10.119.157     172.16.175.128    NFS       146 V4 Reply (Call In 17) RECLAIM_COMPLETE
     20 1.711711825    172.16.175.128    10.10.119.157     NFS       202 V4 Call (Reply In 22) PUTROOTFH | GETATTR
     22 1.966908204    10.10.119.157     172.16.175.128    NFS       318 V4 Reply (Call In 20) PUTROOTFH | GETATTR
     23 1.967038742    172.16.175.128    10.10.119.157     NFS       214 V4 Call (Reply In 25) GETATTR FH: 0x62d40c52
     25 2.321105694    10.10.119.157     172.16.175.128    NFS       230 V4 Reply (Call In 23) GETATTR
     26 2.321598262    172.16.175.128    10.10.119.157     NFS       214 V4 Call (Reply In 28) GETATTR FH: 0x62d40c52
     28 2.629191071    10.10.119.157     172.16.175.128    NFS       226 V4 Reply (Call In 26) GETATTR
     29 2.630141168    172.16.175.128    10.10.119.157     NFS       214 V4 Call (Reply In 31) GETATTR FH: 0x62d40c52
```

```
▸ Frame 214: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)
▸ Ethernet II, Src: VMware_e8:af:99 (00:50:56:e8:af:99), Dst: VMware_76:32
▸ Internet Protocol Version 4, Src: 10.10.119.157, Dst: 172.16.175.128
▸ Transmission Control Protocol, Src Port: 2049, Dst Port: 834, Seq: 12777,
▸ Remote Procedure Call, Type:Reply XID:0xaca9d806
▸ Network File System, Ops(3): SEQUENCE PUTFH READ_PLUS
```

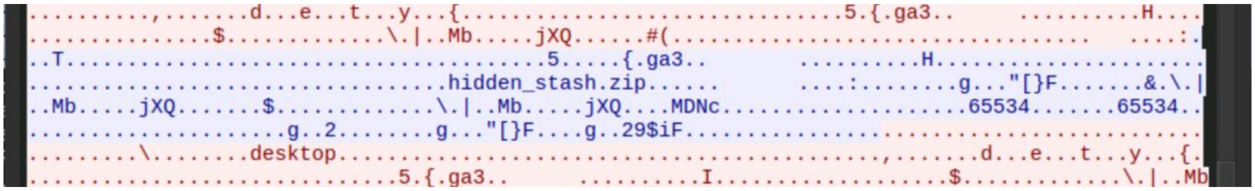
```
0000  00 0c 29 76 32 b1 00 50  56 e8 af 99 08 00 45 00   ··)v2··P V·····E·
0010  00 e0 03 7f 00 00 80 06  59 61 0a 0a 77 9d ac 10   ········ Ya··w···
0020  af 80 08 01 03 42 47 12  97 2d 35 98 3b fc 50 18   ·····BG· ·-5·;·P·
0030  fa f0 0e 7b 00 00 80 00  00 b4 ac a9 d8 06 00 00   ···{···· ········
0040  00 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 03 00 00   ········ ········
0060  00 35 00 00 00 00 87 7b  c9 67 61 33 e6 ed 09 00   ·5·····{ ·ga3····
0070  00 00 00 00 00 00 00 00  00 3d 00 00 00 00 00 00   ········ ·=······
0080  00 1d 00 00 00 1d 00 00  00 00 00 00 00 16 00 00   ········ ········
0090  00 00 00 00 00 44 00 00  00 00 00 00 00 01 00 00   ·····D·· ········
00a0  00 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 39 41 72 63 68 69 76  65 20 50 61 73 73 77 6f   ·9Archiv e Passwo
00c0  72 64 0a 0a 39 30 65 62  37 37 32 33 61 36 35 37   rd··90eb 7723a657
00d0  62 36 35 39 37 31 30 30  61 61 66 65 66 31 37 31   b6597100 aafef171
00e0  64 39 66 32 20 28 6d 64  35 29 0a 00 00 00         d9f2 (md 5)····
```

Network File System: Protocol
Packets: 304 · Displayed: 179 (58.9%)
Profile: Default

SCROLLING THROUGH THE LOGS I NOTICED 2 FILES ONE FILE IS CALLED CREDS.TX / CREDS.TXT & ANOTHER FILE CALLED HIDDEN_STASH.ZIP. AFTER RESEARCHING ONLINE THE NEXT STEP I TOOK WAS TO SAVE THE TCP STREAM IN RAW FORMAT I SAVED ONE UNDER CREDS.TXT & THE OTHER SAVED AS HIDDEN_STASH.ZIP

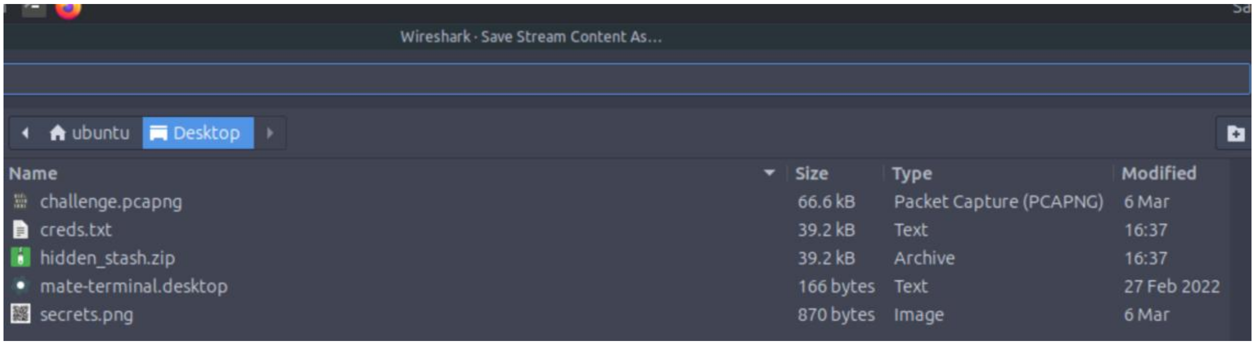


```
       ....................................\........desktop..............................
10758  ..........,.......d...e...t...y...{.........................5.{.ga3..     ..........&
55141  ...............$.............\.|..Mb.....jXQ......................................  ...
43002  ..P...................................5.....{.ga3..        ..........&.................
42099  .................................   creds.txt.........       ....:........g..."[}F.......9
12429  ..Mb.....jXQ.......$.............\.|..Mb.....jXQ,..... [redacted]
49443  ........,.............65534.......65534.......................g...7.......g..."[}F....g...7.
95307  ....,.........................................\........desktop............................
56292
```



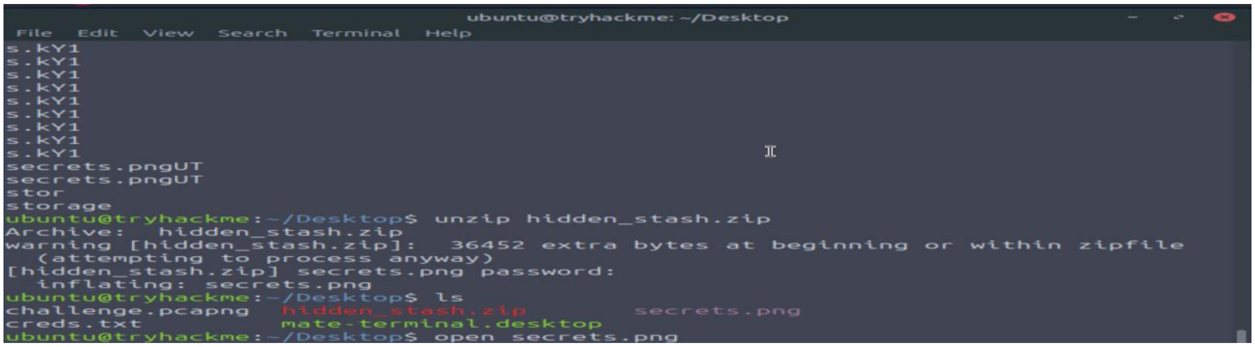
```
..........,.......d...e...t...y...{...............................5.{.ga3..     ..........H....
...............$.............\.|..Mb.....jXQ......#(.................................    .....:.
..T.....................................5.....{.ga3..       ..........H......................
.................................hidden_stash.zip......      ....:........g..."[}F.......&.\.|
..Mb.....jXQ.......$.............\.|..Mb.....jXQ....MDNc.....................65534.......65534..
.......................g..2........g..."[}F....g..29$iF...........................................
.........\........desktop..........................................,.......d...e...t...y...{.
.............................5.{.ga3..     ..........I...................$.............\.|..Mb
```

THE CREDS.TXT FILE I SAVED WAS A DUPLICATE OF THE DATA WE SAW IN THE TCP STREAM



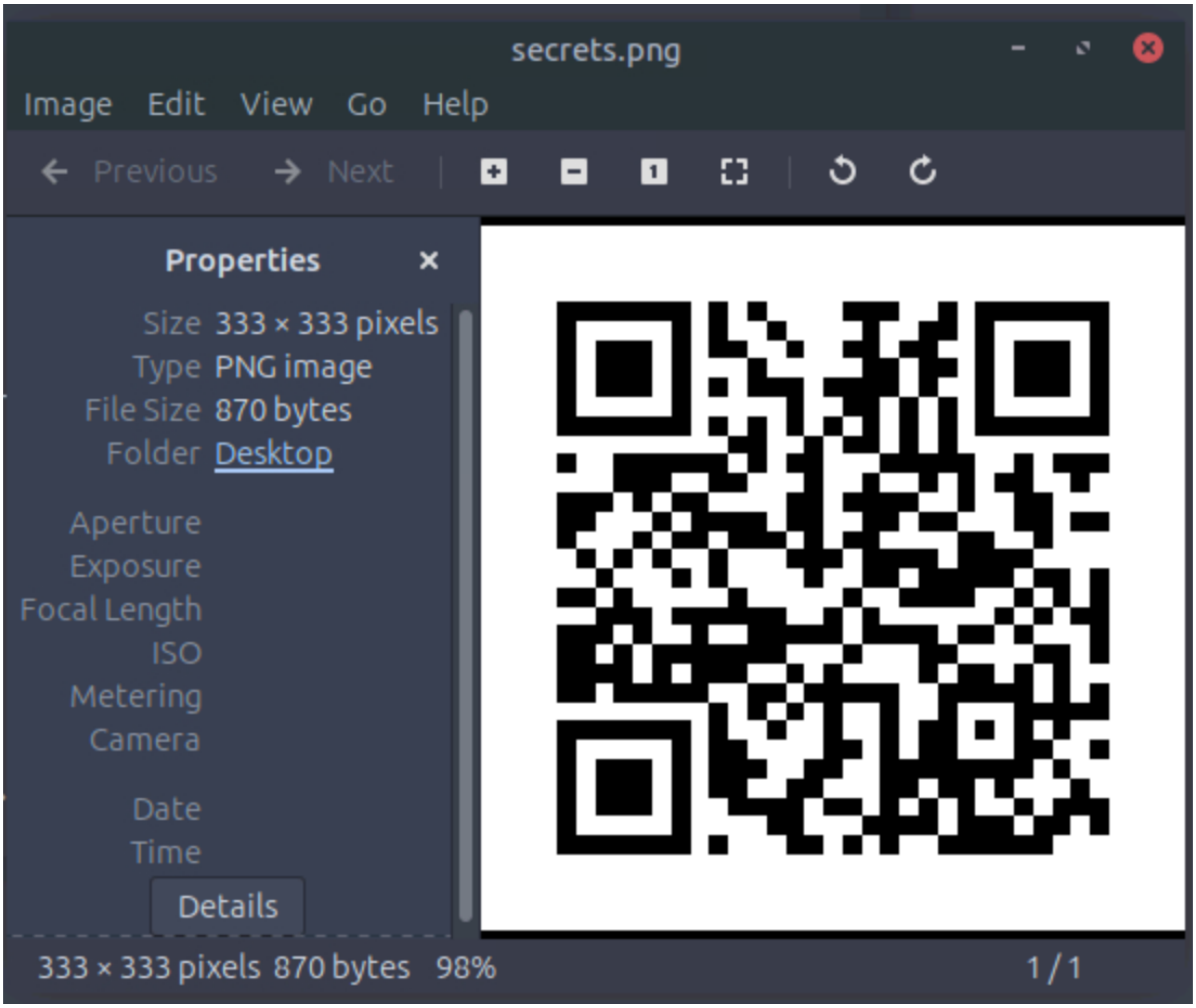
Name	Size	Type	Modified
challenge.pcapng	66.6 kB	Packet Capture (PCAPNG)	6 Mar
creds.txt	39.2 kB	Text	16:37
hidden_stash.zip	39.2 kB	Archive	16:37
mate-terminal.desktop	166 bytes	Text	27 Feb 2022
secrets.png	870 bytes	Image	6 Mar

THE FILE I SAVED AS HIDDEN_STASH.ZIP WAS UNZIPPEDD USING THE 'UNZIP HIDDEN_STASH.ZIP'. IT PROMPT ME FOR A PASSWORD SO I ENTERED THE PASSWORD I FOUNDD EARLIER: 'avengers'. THE ZIP FILE CONTAINED ONLY ONE FILE WITHIN IT CALLED: 'SECRETS.PNG'. ITS A FILE OF A QR CODE.



ubuntu@tryhackme: ~/Desktop
File Edit View Search Terminal Help

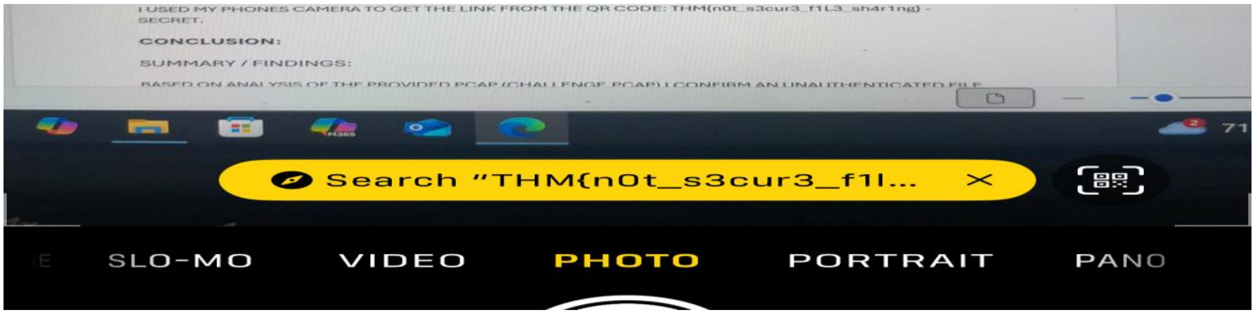
```
s.kY1
s.kY1
s.kY1
s.kY1
s.kY1
s.kY1
s.kY1
s.kY1
s.kY1
secrets.pngUT
secrets.pngUT
stor
storage
ubuntu@tryhackme:~/Desktop$ unzip hidden_stash.zip
Archive:  hidden_stash.zip
warning [hidden_stash.zip]:  36452 extra bytes at beginning or within zipfile
  (attempting to process anyway)
[hidden_stash.zip] secrets.png password:
  inflating: secrets.png
ubuntu@tryhackme:~/Desktop$ ls
challenge.pcapng  hidden_stash.zip        secrets.png
creds.txt         mate-terminal.desktop
ubuntu@tryhackme:~/Desktop$ open secrets.png
```



Size 333 × 333 pixels
Type PNG image
File Size 870 bytes
Folder Desktop
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time

333 × 333 pixels 870 bytes 98% 1 / 1

I USED MY PHONES CAMERA TO GET THE LINK FROM THE QR CODE: THM{n0t_s3cur3_f1L3_sh4r1ng} - SECRET.



I USED MY PHONES CAMERA TO GET THE LINK FROM THE QR CODE: THM{n0t_s3cur3_f1L3_sh4r1ng} - SECRET.

CONCLUSION:

SUMMARY / FINDINGS:

BASED ON ANALYSIS OF THE PROVIDED PCAP (CHALLENGE.PCAP) I CONFIRM AN UNAUTHENTICATED FILE

CONCLUSION:

SUMMARY / FINDINGS:

BASED ON ANALYSIS OF THE PROVIDED PCAP (CHALLENGE.PCAP) I CONFIRM AN UNAUTHENTICATED FILE SHARE ACCESS RESULTING IN THE THEFT OF A CLASSIFIED FILE. THE PCAP CONTAINS 304 PACKETS (179 NFS RELATED). ONLY TWO IP ADDRESSES APPEAR: 172.16.175.128 AND 10.10.119.157. I ASSESS 172.16.175.128 AS THE ADVERSARY SOURCE. WITHIN A TCP STREAM I EXTRACTED AN MD5 HASH (90EB7723A657B6597100AAFEEF171D9F2) THAT CRACKED TO THE PASSWORD: avengers. TWO ARTIFACTS WERE RECOVERED FROM THE STREAM: CREDS.TXT (DUPLICATE OF STREAM DATA) AND HIDDEN_STASH.ZIP. HIDDEN_STASH.ZIP REQUIRED A PASSWORD; USING 'avengers' I DECRYPTED IT AND FOUND SECRETS.PNG (A QR CODE). SCANNING THE QR PRODUCED: THM{n0t_sa3cur3_f1i3_sh4r1ng} CONFIRMED SECRET EXFILTRATED.

IMPACT:

A CLASSIFIED SECRET WAS ACCESSED AND EXFILTRATED FROM THE NFS BACKUP SHARE. CREDENTIALS/SHARE PASSWORDS WERE PRESENT IN CLEARTEXT/RECOVERABLE FORM FROM NETWORK TRAFFIC INDICATES WEAK/EXPOSED AUTHENTICATION PRACTICES. ATTACKER USED NETWORK-LEVEL ACCESS ONLY (NO HOST FORENSICS AVAILABLE), BUT SUCCESSFUL EXTRACTION OF A SENSITIVE FILE IS PROVEN BY THE QR FLAG.

INDICATORS / ARTEFACTS (IOC):

ADVERSARY IP: 172.16.175.128 OTHER OBSERVED IP: 10.10.119.157 MD5 HASH: 90eb7723a657b6597100aafef171d9f2 → PASSWORD: avengers RECOVERED FILES: CREDS.TXT, HIDDEN_STASH.ZIP, SECRETS.PNG EXFILTRATED SECRET (QR PAYLOAD): THM{n0t_s3cur3_f1L3_sh4r1ng}

LIMITATIONS:

SCOPE WAS LIMITED TO THE PCAP ONLY NO ENDPOINT/HOST LOGS, NO ACTIVE DIRECTORY/FILE-SERVER AUDITS, NO SYSTEM TIMELINES. THIS LIMITS ABILITY TO ATTRIBUTE BEYOND NETWORK OBSERVABLES OR TO DETERMINE LATERAL MOVEMENT/INITIAL ACCESS VECTOR OUTSIDE THE CAPTURE. IF THE PCAP IS PARTIAL (TRUNCATED/INCOMPLETE) THERE MAY BE ADDITIONAL ACTIVITY NOT SEEN HERE. RECOMMENDATIONS / NEXT STEPS (PRIORITIZED): ISOLATE & PRESERVE: ENSURE THE NFS SERVER/NETWORK SEGMENT IS ISOLATED (IF NOT ALREADY) AND PRESERVE IMAGES / FULL NETWORK

CAPTURES. COLLECT ENDPOINT TELEMETRY FOR 172.16.175.128 AND 10.10.119.157 IF AVAILABLE. ENGAGE DFIR: ESCALATE TO FULL DFIR TEAM COLLECT HOST FORENSICS, SERVER FILE TIMESTAMPS, AUTH LOGS, AND BACKUP INTEGRITY CHECKS. CREDENTIAL ROTATION: IMMEDIATELY ROTATE ANY CREDENTIALS/SHARE PASSWORDS IDENTIFIED (INCLUDING “avengers”) AND FORCE PASSWORD CHANGES FOR ACCOUNTS WITH ACCESS TO THE NFS BACKUP. HARDEN NFS ACCESS: REVIEW AND RESTRICT NFS EXPORTS, ENFORCE AUTHENTICATION/ENCRYPTION (USE KERBEROS/STRONGER AUTH), DISABLE UNNECESSARY ANONYMOUS/UNAUTHENTICATED ACCESS. MONITOR & DETECT: IMPLEMENT/ADJUST IDS/NSM RULES TO ALERT ON SIMILAR NFS READS, TCP STREAM EXTRACTIONS, AND ANY TRANSFERS INVOLVING HIDDEN_STASH.ZIP/SECRETS.PNG OR THE IDENTIFIED IPS. COMMS & NOTIFICATION: NOTIFY STAKEHOLDERS / DATA OWNERS / LEGAL / COMPLIANCE PER ORGANIZATIONAL POLICY. CONSIDER LAW ENFORCEMENT IF CLASSIFICATION / REGULATORY OBLIGATIONS REQUIRE. POST-INCIDENT REVIEW: PERFORM A ROOT-CAUSE ANALYSIS FOCUSED ON HOW THE CREDENTIAL/SHARE BECAME EXPOSED ON THE NETWORK AND REMEDIATE (CONFIG, POLICY, USER BEHAVIOR). HUNTING: RUN THREAT HUNTING FOR SIMILAR ARTIFACTS ACROSS THE ENVIRONMENT (OTHER ZIPS, QR FILES, KNOWN PASSWORD USAGE), AND CHECK FOR OTHER POTENTIAL DATA DESTINATIONS OR C2.

CONFIDENCE:

EVIDENCE IS STRONG THAT A SECRET WAS EXFILTRATED VIA NFS ACCESS AND NETWORK TRAFFIC CONTAINS BOTH CREDENTIALS AND THE EXFILTRATED ARTIFACT. CONFIDENCE IS MODERATE TO HIGH FOR NETWORK LEVEL FINDINGS; LOWER FOR FULL SCOPE/ATTRIBUTION DUE TO LACK OF HOST FORENSICS.

CLOSING:

THE PCAP ANALYSIS PROVES A SUCCESSFUL DATA THEFT FROM THE NFS BACKUP SHARE USING RECOVERABLE CREDENTIALS. ACTIONS SHOULD FOCUS FIRST ON CONTAINMENT, EVIDENCE PRESERVATION, AND CREDENTIAL ROTATION, THEN ON A FULL DFIR INVESTIGATION TO DETERMINE EXTENT, TIMELINE, AND ROOT CAUSE.