Albert DePierro
depierroa@mail.sacredheart.edu

Network Forensics

Network Security Lab #7
CY-367

Table of Contents

I. **Executive Summary** **3**

Objectives

II. **Lab Description Details** **3**

Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

III. **Supporting Evidence** **3**

IV. **Conclusion & Wrap-Up** **4**

Summary with observations, Success & Failures, Challenges

Executive Summary

We were hired to investigate a data breach by analyzing the aptured network traffic log. They are looking to find answers to questions below.

Lab Description Details

1. What are the IP addresses of the attacker machine and server from where the file was stolen?

Attacker is .132 it was stolen from .133

2. What network service/protocol is used to steal the data? [20 points]

FTP

3. What were the compromised credentials used to gain access to the network server?

His username and password which is irfan and vcu123

4. What is the name of the stolen file?

vcu.abc

5. The attacker has renamed the file extensions to subvert IDS signatures. What is the original extension of the file?

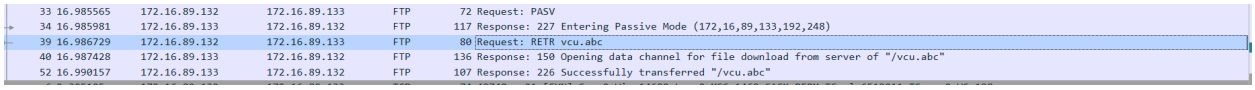
png file

6. What are the contents of the files? [20 points]

(In screenshot below)

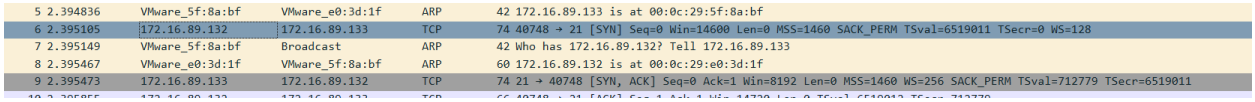
Supporting Evidence

This is vcu.abc file that was stolen



33	16.985565	172.16.89.132	172.16.89.133	FTP	72	Request: PASV
34	16.985981	172.16.89.133	172.16.89.132	FTP	117	Response: 227 Entering Passive Mode (172,16,89,133,192,248)
39	16.986729	172.16.89.132	172.16.89.133	FTP	80	Request: RETR vcu.abc
40	16.987428	172.16.89.133	172.16.89.132	FTP	136	Response: 150 Opening data channel for file download from server of "/vcu.abc"
52	16.990157	172.16.89.133	172.16.89.132	FTP	107	Response: 226 Successfully transferred "/vcu.abc"

Shows attacker and server

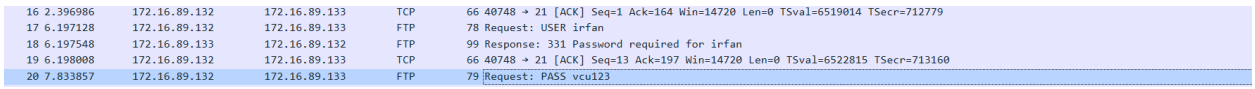


5	2.394836	VMware_5f:8a:bf	VMware_e0:3d:1f	ARP	42	172.16.89.133 is at 00:0c:29:5f:8a:bf
6	2.395105	172.16.89.132	172.16.89.133	TCP	74	40748 → 21 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=6519011 TSecr=0 WS=128
7	2.395149	VMware_5f:8a:bf	Broadcast	ARP	42	Who has 172.16.89.132? Tell 172.16.89.133
8	2.395467	VMware_e0:3d:1f	VMware_5f:8a:bf	ARP	60	172.16.89.132 is at 00:0c:29:e0:3d:1f
9	2.395473	172.16.89.133	172.16.89.132	TCP	74	21 → 40748 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=712779 TSecr=6519011

Shows that it is a png file


```
.PNG
.
...
IHDR..
6...R.....[.t....     pHYs...#...#.x.?v....iTXtXML:com.adobe.xmp.....<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xm
lns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21        "> <rdf:RDF xmlns:rdf="http://www.w3.org/1
999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/
1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.co
m/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop CC (Macintosh)" xmp:CreateDate="2017-10-23T14:18:33-04:00" xmp:ModifyDa
te="2017-10-23T14:24:20-04:00" xmp:MetadataDate="2017-10-23T14:24:20-04:00" dc:format="image/png" photoshop:ColorMode="3" photoshop:ICCP
rofile="sRGB IEC61966-2.1" xmpMM:InstanceID="xmp.iid:6c58dc36-e9a2-4469-8d80-1f5fac0c665d" xmpMM:DocumentID="xmp.did:6c58dc36-e9a2-4469-
8d80-1f5fac0c665d" xmpMM:OriginalDocumentID="xmp.did:6c58dc36-e9a2-4469-8d80-1f5fac0c665d"> <xmpMM:History> <rdf:Seq> <rdf:li stEvt:acti
on="created" stEvt:instanceID="xmp.iid:6c58dc36-e9a2-4469-8d80-1f5fac0c665d" stEvt:when="2017-10-23T14:18:33-04:00" stEvt:softwareAgent=
"Adobe Photoshop CC (Macintosh)"/> </rdf:Seq> </xmpMM:History> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.@_...FBIDA
Tx....x.....?.~       NH.i.&#..k..d.&U.(N4..g.....=.lh..&E7)..
.
..K..6.....O[m        0....S3P.b..2`...Z.'..6.@FQ ...Lb~....=..o..U.~.....d&.+...I./_.`...b.dJ.V....^...............&.lD".].,I...K..;/.
...s...c......~...{Sq.g.j..............`#b6(.h.....c..|c*..Y...O.~y$.$..............!......M}..y..0.$e.U.:.......x<i\9.............
01.l....2O}........jR.Y...=.......Y..............G..'.@.q._s..&m.S_.......F..............`...wY.$9D.1....N::.............@..6.s~...
.0.CR.X..q./...$.../
\?...!...taT.,.v....<.q.y..~r.$)..I.?..^.....1iTg...t.S}..O.................6.C~......%.+c......e.v.Wo._'..W.....@.1...?UWeLR.uS.9s.
nY0E.fLR.......c......d.............tD.q......e&z....:.v.N.....^....:.Vo..1...S..l..~r.nY0E..&..6%.(B.................4..3.Z      ..
.q....]..N..../.zTt...m.-.........S.1..?..`*..N..............n.6.......0.jI.....t.~.vI/...Z..4.;1&...S..6U.Y0E..S..t<....3Q..........
...@:!..&...WKZ6...;2..w......8.....^...g...q;..............L$..S.....4.Q.-o\./[/.......8....}.M...2Mw}j.rf.F.....pt..2.............Hm.
.S..e.'i..U........wQ.......Zx.d.X2]+.LS.......>.................. ..lL!~.e....w..G*...l....L.?~\...#.....r.......H...9"..;p.j.j...jjjJ
z......YINI..S
............`.!......j.....7...%.....        3...i...:~..v..)I..lz...e6.C>....d..y<.......<.9N.S../.....Gf.Y>.Ommm...........S..w.'..3.?
`.,.v.....Z.d.h.U7....'q..............q.6.h4...3~.}......:.Vo.K...j.=......J.n..F}...../n..U.6l.Xo......P...#...|......q...r8.A.nooWQQ.
.....z..G..?..Ijll.5.\....^/.......n.....U.....1).-~.....[..............-....M.......w.../>LtY1kkkSnnn.{..).+++...;F\_.v.@w..ZZZTPP0..
5.\3$.8XII.v..5.....Rmmm.Z.m.6....S...o..?.A...3d.u.l._:]e.L.wT5.G.............i.`...7..
..C......;.n..!...........,XGE...cMM.....-
.a.?t.........777.......'N.....|...}.].............i.<N..............@Z".8....C.v..hl?.........OFY.......g4k.,..'?          ..0.......zUT
T.\.l.t{{....F..Z.z..wF\..........q.P]!}>.....z......D..m.7.a.V.vz<c....p<.............. ..6&..eY....w....sQO.......d.%.........j
9J...Uk..
..q........j....BuI......Yv.}..PAH.o...={.........`.....V../^..o.]...#>_+W..........W\....X.m...T.................. qbNG!2..2...4H:..B..
./h.W.u..sI.5..?.~.P.$......_TYYY.{...........].v....9....+......G\.....f.......$.../l...V..k..K...z......
...i..Ejoo.Xw.....H....../.EU?x_-o\...U.N.].M.................`c..]..@p... YT...+....o.&.....G999...k....r..l...;....4.7....{I
:.y._..W#..\.2..g.}6..PA....K..m...uX.Vegg..~.....=.....~I}]..^o.3.....uK.Y....K.1S.F..r20..............R....  ..<.6./@..X....z.r8.A.'.
f.......{.......x&......Bua...>.t.`A...J..f.....h/^.8..p....5*.8......p.+i..e9.wY.%.:.................Q
..>$i...c...h............{cccc...mmm..O}.Sa..e....?.t.`A.{..GR.....~..#.uvvF.-....7..MTg......3.h..C.....&.................. z..Ga...;.
Y...%...s  .4..v......Y---...........GK.....~_UU...cii.ZZZTRR..~....n.).......0Z.V.w.}.4.
```


Shows his username and password



16	2.396986	172.16.89.132	172.16.89.133	TCP	66	40748 → 21 [ACK] Seq=1 Ack=164 Win=14720 Len=0 TSval=6519014 TSecr=712779
17	6.197128	172.16.89.132	172.16.89.133	FTP	78	Request: USER irfan
18	6.197548	172.16.89.133	172.16.89.132	FTP	99	Response: 331 Password required for irfan
19	6.198008	172.16.89.132	172.16.89.133	TCP	66	40748 → 21 [ACK] Seq=13 Ack=197 Win=14720 Len=0 TSval=6522815 TSecr=713160
20	7.833857	172.16.89.132	172.16.89.133	FTP	79	Request: PASS vcu123

Shows FTP protocol

395473	172.16.89.133	172.16.89.132	TCP	74 21 → 40748 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval
395855	172.16.89.132	172.16.89.133	TCP	66 40748 → 21 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=6519012 TSecr=712779
396631	172.16.89.133	172.16.89.132	FTP	108 Response: 220-FileZilla Server version 0.9.43 beta
396737	172.16.89.133	172.16.89.132	FTP	126 Response: 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
396833	172.16.89.133	172.16.89.132	FTP	127 Response: 220 Please visit http://sourceforge.net/projects/filezilla/
396899	172.16.89.132	172.16.89.133	TCP	66 40748 → 21 [ACK] Seq=1 Ack=43 Win=14720 Len=0 TSval=6519014 TSecr=712779
396900	172.16.89.132	172.16.89.133	TCP	66 40748 → 21 [ACK] Seq=1 Ack=103 Win=14720 Len=0 TSval=6519014 TSecr=712779
396986	172.16.89.132	172.16.89.133	TCP	66 40748 → 21 [ACK] Seq=1 Ack=164 Win=14720 Len=0 TSval=6519014 TSecr=712779
197128	172.16.89.132	172.16.89.133	FTP	78 Request: USER irfan
197548	172.16.89.133	172.16.89.132	FTP	99 Response: 331 Password required for irfan
198008	172.16.89.132	172.16.89.133	TCP	66 40748 → 21 [ACK] Seq=13 Ack=197 Win=14720 Len=0 TSval=6522815 TSecr=713160
333857	172.16.89.132	172.16.89.133	FTP	79 Request: PASS vcu123
334310	172.16.89.133	172.16.89.132	FTP	81 Response: 230 Logged on
335126	172.16.89.132	172.16.89.133	TCP	66 40748 → 21 [ACK] Seq=26 Ack=212 Win=14720 Len=0 TSval=6524451 TSecr=713323

This is contents on file

VCU College of Engineering

Conclusion & Wrap-Up

Overall I thought this lab was good, it was a good refresher for me because I have not used wireshark in a semester, but using it again was good and it was cool to see that we saw a bunch of random stuff and we were able to convert it into a png and see what we were really looking for. A challenge we faced was finding the right tcp stream to follow, but we were able to figure it out.