

Category: Miscellaneous

Challenge: Mission: “Sabanci”

Write-up:

We need to connect with Netcat to start the challenge.

After making some choices that are not requiring any cyber-security knowledge, we encounter a network forensics challenge.

1856	171.420293	192.168.141.128	46.101.155.145	HTTP	215	GET	/_vti_txt%0A	HTTP/1.1
1869	172.530047	192.168.141.128	46.101.155.145	HTTP	211	GET	/_www%0A	HTTP/1.1
897	90.346490	192.168.141.128	46.101.155.145	HTTP	228	GET	/long-urls-are-suspicious	HTTP/1.1
1157	112.582700	192.168.141.128	46.101.155.145	HTTP	231	GET	/look-at-the-end-of-response	HTTP/1.1
1290	123.611189	192.168.141.128	46.101.155.145	HTTP	217	GET	/recovery-code	HTTP/1.1
1882	173.634080	192.168.141.128	46.101.155.145	HTTP	211	GET	/~adm%0A	HTTP/1.1
1896	174.782536	192.168.141.128	46.101.155.145	HTTP	213	GET	/~admin%0A	HTTP/1.1
1909	175.884145	192.168.141.128	46.101.155.145	HTTP	221	GET	/~administrator%0A	HTTP/1.1

One can easily see the /recovery-code page. After following the TCP stream, we can see a base64 encoded string.

1290	123.611189	192.168.141.128	46.101.155.145	HTTP	217	GET	/recovery-code	HTTP/1.1
1882	173.634080	192.168.141.128	46.101.155.145	HTTP	211	GET	/~adm%0A	HTTP/1.1
1896	174.782536	192.168.141.128	46.101.155.145	HTTP	213	GET	/~admin%0A	HTTP/1.1
1909	175.884145	192.168.141.128	46.101.155.145	HTTP	221	GET	/~administra	HTTP/1.1
1922	176.989375	192.168.141.128	46.101.155.145	HTTP	214	GET	/~amanda%0A	HTTP/1.1
1935	178.100606	192.168.141.128	46.101.155.145	HTTP	214	GET	/~apache%0A	HTTP/1.1
1948	179.221098	192.168.141.128	46.101.155.145	HTTP	211	GET	/~bin%0A	HTTP/1.1
1961	180.347303	192.168.141.128	46.101.155.145	HTTP	211	GET	/~ftp%0A	HTTP/1.1
1974	181.448863	192.168.141.128	46.101.155.145	HTTP	213	GET	/~guest%0A	HTTP/1.1
1987	182.561601	192.168.141.128	46.101.155.145	HTTP	212	GET	/~http%0A	HTTP/1.1
2000	183.682921	192.168.141.128	46.101.155.145	HTTP	213	GET	/~httpd%0A	HTTP/1.1
2013	184.798468	192.168.141.128	46.101.155.145	HTTP	211	GET	/~log%0A	HTTP/1.1
2026	185.922137	192.168.141.128	46.101.155.145	HTTP	212	GET	/~logs%0A	HTTP/1.1
2039	187.072504	192.168.141.128	46.101.155.145	HTTP	210	GET	/~ln%0A	HTTP/1.1

Frame 1290: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits)			
Ethernet II, Src: VMware_4c:cf:e2 (00:0c:29:4c:cf:e2), Dst: VMware_e9:48:1b (00:50:56:e9:48:1b)			
Internet Protocol Version 4, Src: 192.168.141.128, Dst: 46.101.155.145			
Transmission Control Protocol, Src Port: 59168, Dst Port: 3001, Seq: 1, Ack: 1, Len: 163			
Hypertext Transfer Protocol			

Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP

Ctrl+M
Ctrl+D
Ctrl+T
Ctrl+Shift+T
Ctrl+Alt+C

Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

Ctrl+Alt+Shift+T
Ctrl+Alt+Shift+U
Ctrl+Alt+Shift+S
Ctrl+Alt+Shift+H

Encoded: “UmVjb3ZlcnkgY29kZSBpczogMTIzcmVjb3ZlcnkxMjM=”

Decoded: **“Recovery code is: 123recovery123”**

When we enter this recovery code, the game continues. After making some choices, we are encountering some puzzle.

The code is: **“3024”**

After entering the code, we are given encoded data.

Encoded: **“HFXGU{I3hK3xg+}”**. After some research, one can understand that it is a monoalphabetic cypher called Atbash. With decoding it with the Atbash Cipher scheme; **Flag is: SUCTF{R3sP3ct+}**

