

Projet Sécurité: CTF

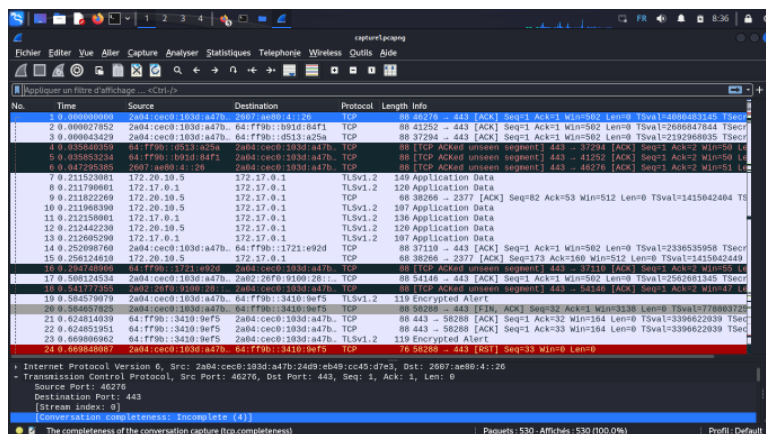


GROUPE	BACKDOOR	Solution
PHASE 1	DEVELOPPEMENT CTF	
NIVEAU	FACILE	RESEAU

Flag 1:

Analyser la capture Wireshark :

- Ouvrez la capture Wireshark fournie.
- Appliquez un filtre pour afficher uniquement les paquets TELNET en utilisant la commande : `tcp.port==23`.



Repérer le paquet contenant le flag :

- Parcourez les paquets TELNET et recherchez des données inhabituelles ou potentiellement codées.
- Identifiez le paquet qui semble contenir le flag. Cela peut être indiqué par une longueur de données suspecte, ou d'autres signes distinctifs.

No.	Time	Source	Destination	Protocol	Length	Info
263	7.452726247	:::1	:::1	TelNET	89	Telnet Data ...
264	7.452745660	:::1	:::1	TCP	88	23 → 49968 [ACK] Seq=39 Ack=45 Win=512 Len=0 TSval=4183488957 TSecr=...
265	7.472633733	:::1	:::1	TelNET	193	Telnet Data ...
266	7.472657537	:::1	:::1	TCP	88	49968 → 23 [ACK] Seq=45 Ack=45 Win=512 Len=0 TSval=4183488977 TSecr=...
267	7.472746067	172.20.10.5	172.20.10.5	TelNET	93	Telnet Data ...
268	7.472786948	172.20.10.5	172.20.10.5	TCP	68	33848 → 23 [ACK] Seq=45 Ack=45 Win=512 Len=0 TSval=4927943372 TSecr=...
269	7.488153745	172.20.10.5	172.20.10.5	TelNET	69	Telnet Data ...
270	7.488322830	:::1	:::1	TelNET	69	Telnet Data ...
271	7.488259843	172.20.10.5	172.17.0.1	TLSv1.2	298	Application Data

Extraire le paquet avec le flag :

- Identifiez le numéro de séquence du paquet contenant le flag.
- Utilisez les fonctionnalités de filtrage de Wireshark pour extraire uniquement ce paquet.

No.	Time	Source	Destination	Protocol	Length	Info
318	7.693592960	172.20.10.5	172.20.10.5	TelNET	89	Telnet Data ...
319	7.693676110	:::1	:::1	TelNET	89	Telnet Data ...
320	7.700738710	:::1	:::1	TelNET	193	Telnet Data ...
321	7.700854434	172.20.10.5	172.20.10.5	TelNET	83	Telnet Data ...
322	7.723889387	172.20.10.5	172.20.10.5	TelNET	69	Telnet Data ...
323	7.723976588	:::1	:::1	TelNET	89	Telnet Data ...
331	7.752676988	:::1	:::1	TelNET	193	Telnet Data ...
332	7.752985282	172.20.10.5	172.20.10.5	TelNET	69	Telnet Data ...
333	7.754707080	172.20.10.5	172.20.10.5	TelNET	69	Telnet Data ...
334	7.754797885	:::1	:::1	TelNET	89	Telnet Data ...
335	7.761889561	:::1	:::1	TelNET	89	Telnet Data ...
336	7.762392999	172.20.10.5	172.20.10.5	TelNET	83	Telnet Data ...
337	7.864023317	172.20.10.5	172.20.10.5	TCP	68	33848 → 23 [ACK] Seq=55 Ack=195 Win=512 Len=0 TSval=4827943784 TSecr=...
339	7.864133596	:::1	:::1	TCP	88	49968 → 23 [ACK] Seq=55 Ack=195 Win=512 Len=0 TSval=4183488489 TSecr=...
354	9.4876957742	172.20.10.5	172.20.10.5	TelNET	184	Telnet Data ...

Déchiffrer les données

Operations	Recipe	Input	Output
From Base64	From Base64	RevZyZb3V3b3V3Zl11KQ==	Flag(YouFoundMe)
Remove non-alphabet chars	<input checked="" type="checkbox"/> Remove non-alphabet chars		
Strict mode	<input type="checkbox"/> Strict mode		

Flag(YouFoundMe)

Flag 1:

Analyser la capture Wireshark :

- Ouvrez la capture Wireshark fournie et examinez les connexions entrantes et sortantes.
- Identifiez des schémas de trafic suspects ou des ports qui pourraient être associés à Netcat.

