Offre de stage Master 2

Intitulé : **Exfiltration des données à travers la stéganographie réseau**
Etablissement d'accueil : ENSSAT, Lannion
Laboratoire d'accueil : Equipe SOTERN, IRISA
Durée de stage : 06 Mois

CONTEXTE ET PROBLEMATIQUE

L'exfiltration des données désigne le transfert illicite et non autorisé des informations sensibles ou privées à partir d'un réseau d'une organisation vers une destination externe contrôlée par un attaquant. Pour mener ce type d'attaque, un attaquant peut utiliser différents vecteurs comme les canaux cachés, l'injection SQL, l'écoute clandestine ou la stéganographie. La stéganographie est une technique qui vise à dissimuler les informations sensibles dans un média de couverture (texte, image, audio, vidéo) de manière à ce que l'existence même de ces informations soit invisible et difficile à détecter. Parmi les techniques de stéganographie, on trouve la stéganographie réseau qui exploite les protocoles réseau existants (TCP/IP, DNS, HTTP, etc.) pour transmettre des données sur un réseau sans qu'elles ne soient détectées. L'exfiltration de données peut être très difficile à détecter tel est le cas lorsque celle-ci utilise stéganographie réseau.

Pour se prémunir contre l'exfiltration des données, divers techniques de prévention et de détection ont été développées. Ces techniques peuvent être classées en deux catégories : proactives et réactives. Parmi les approches proactives, on peut citer la classification des données (sensibles ou non sensibles), le contrôle d'accès, le chiffrement, le stockage distribué, etc. Parmi les techniques réactives, on trouve les méthodes qui inspectent le contenu des paquets, et celles qui se basent sur les anomalies.

ETAT DE L'ART et OBJECTIFS

Plusieurs travaux de recherche ont étudié l'exfiltration de données par le biais de la stéganographie réseau [1-5]. A titre d'exemple, les auteurs dans [1] ont exploité l'entête des paquets IP pour dissimuler des informations secrètes. Une approche de détection d'exfiltration des données en temps réel exploitant le protocole DNS a été présentée dans [2]. Les auteurs dans [3] ont proposé un Framework qui permet la détection de codes malicieux cachés dans les protocoles TCP/IP, tels que DNS et HTTP.

Ce stage de Master s'intéresse à la sécurité réseau et se focalisera sur l'exfiltration des données à travers la stéganographie. L'accent sera particulièrement mis sur la stéganographie réseau qui exploite les protocoles réseaux disponibles, tels que DNS et le HTTP. L'objectif principal est donc

d'étudier les différentes méthodes d'exfiltration des données. L'accent sera particulièrement mis sur les approches utilisant la stéganographie réseau [4, 5]. Dans un second temps, les techniques de prévention et de détection des attaques d'exfiltration des données par stéganographie proposées dans la littérature seront passées en revue et classifiées.

Le déroulement de ce stage est comme suit :

1. Identifier et étudier les différents vecteurs d'attaque d'exfiltration de données et les techniques de défense (contre-mesures) proposées dans la littérature ;
2. Proposer une classification à la fois des méthodes d'exfiltration et des contre-mesures
3. Faire une étude comparative des techniques étudiées ;
4. Identifier des scenarios d'attaques représentatifs et tester les techniques de défense identifiées afin d'évaluer la fiabilité de ces dernières.

REFERENCES

[1] Ganivev, A., Mavlonov, O., & Turdibekov, B. (2021, November). Improving data hiding methods in network steganography based on packet header manipulation. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-5). IEEE.

[2] Ozery, Y., Nadler, A., & Shabtai, A. (2024). Information based heavy hitters for real-time DNS data exfiltration detection. In Proc. Netw. Distrib. Syst. Secur. Symp (pp. 1-15).

[3] Zillien, S., Petrov, D., Ruffing, P., & Gross, F. (2024, June). A Development Framework for TCP/IP Network Steganography Malware Detection. In Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security (pp. 95-100).

[4] Seo, J. O., Manoharan, S., & Mahanti, A. (2016, August). A discussion and review of network steganography. In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 384-391). IEEE.

[5] Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (2014). Principles and overview of network steganography. IEEE Communications Magazine, 52(5), 225-229.

ENCADRANTS

Mohammed NAFI (mohammed.nafi@irisa.fr), SOTERN, IRISA, Lannion
Mohamed Aymen CHALOUF (mohamed-aymen.chalouf@irisa.fr), SOTERN, IRISA, Lannion
Pierre ALAIN (pierre.alain@irisa.fr), SOTERN, IRISA, Lannion
Guillaume DOYEN (guillaume.doyen@imt-atlantique.fr), SOTERN, IRISA, Rennes