Evaluating the Effectiveness of Various Developments to the Contactless 'Active' Reconnaissance Process

Liam Shillinglaw

Is it possible to accurately discover and evaluate your entire exposed attack surface indirectly?

INTRO

The Contactless 'Active' Reconnaissance (CAR) process refers to the indirect gathering of data gathered from third parties. By retrieving, collating and processing such data from various third-party sources a reliable and up to date exposed attack surface can be derived.

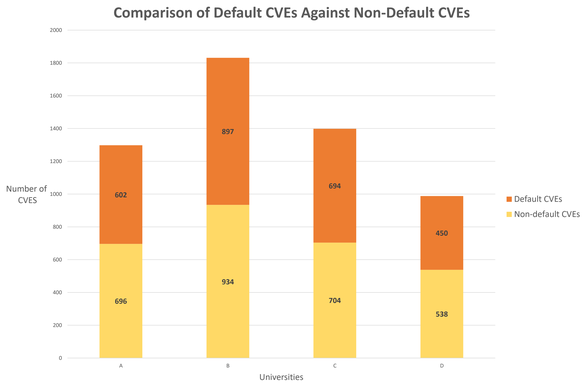
METHODS

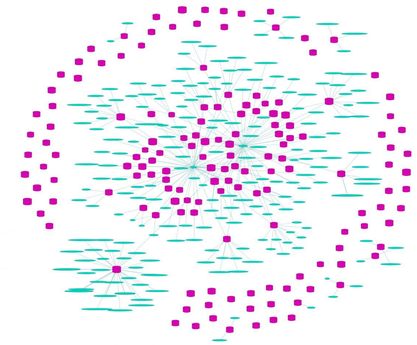
1. Correlation of data ingested from 4 well-established Internet-wide scanning platforms and 6 passive DNS sources.
2. Merging of Internet-wide scanning data from multiple data feeds.
3. Service banner analysis for CPE reconstruction, based on the Levenshtein distance algorithm.
4. User-friendly opensource, web accessible tool called **Informant**.

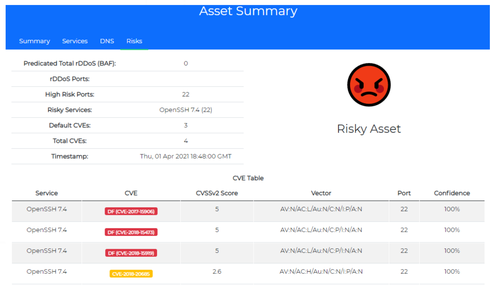
RESULT

Tool/Feature	Scout	ShoVAT	Nessus	OpenVAS	Informant
Passive	●●●	●●●	●	●	●●●
Active	●	●	●●●	●●●	●
Custom Banner	●●	●●	●●	●●	●●
CPE/CVE	●●●	●●●	●●●	●●●	●●●
PDNS	●	●	●	●	●●●
Default Config CVE Detection	●	●	●	●	●●
rDDoS Prediction	●	●	●	●	●●
Historical Data	●	●	●●	●●	●●●

Informant identified **5,515 vulnerabilities** across 4 UK universities **without leaving a trace.**







REFERENCES

Genge, B. and Enăchescu, C. (2016) 'ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services', *Security and Communication Networks*, 9(15), pp. 2696–2714. doi: 10.1002/sec.1262

Guo, H., Xing, Z. and Li, X. (2020). 'Predicting Missing Information of Vulnerability Reports', *WWW '20: Companion Proceedings of the Web Conference 2020,* pp. 81-22. doi: 10.1145/3366424.3382707

Leverett, E. and Kaplan, A. (2017) "Towards estimating the untapped potential: a global malicious ddos mean capacity estimate," *Journal of Cyber Policy,* 2(4), pp. 195-208. doi: 10.1080/23738871.2017.1362020

Li, R., Shen, M., Yu, H., Li, C., Duan, P. and Zhu, L. (2021) 'A Survey on Cyberspace Search Engines', *Communications in Computer and Information Science*, Beijing, China, pp. 206-214. doi: 10.1007/978-981-33-4922-3_15

O'Hare, J., Macfarlane, R. and Lo, O. (2019) 'Identifying Vulnerabilities Using Internet-Wide Scanning Data', *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, pp. 1-10. doi: 10.1109/ICGS3.2019.8688018.

Supervisor: Jamie O'Hare

Abertay University