Audyt bezpieczeństwa sieci

Zespół **SPAM**

A. **S**itarczyk, J. **P**elczar, S. **Al**-Saaiydeh, A. **M**ichalska

Informacje o audycie

Cel audytu:

Weryfikacja wdrożenia i skuteczności mechanizmów bezpieczeństwa w zakresie nowego biura w ramach realizacji projektu z przedmiotu BEKOM.

Zakres przedmiotowy:

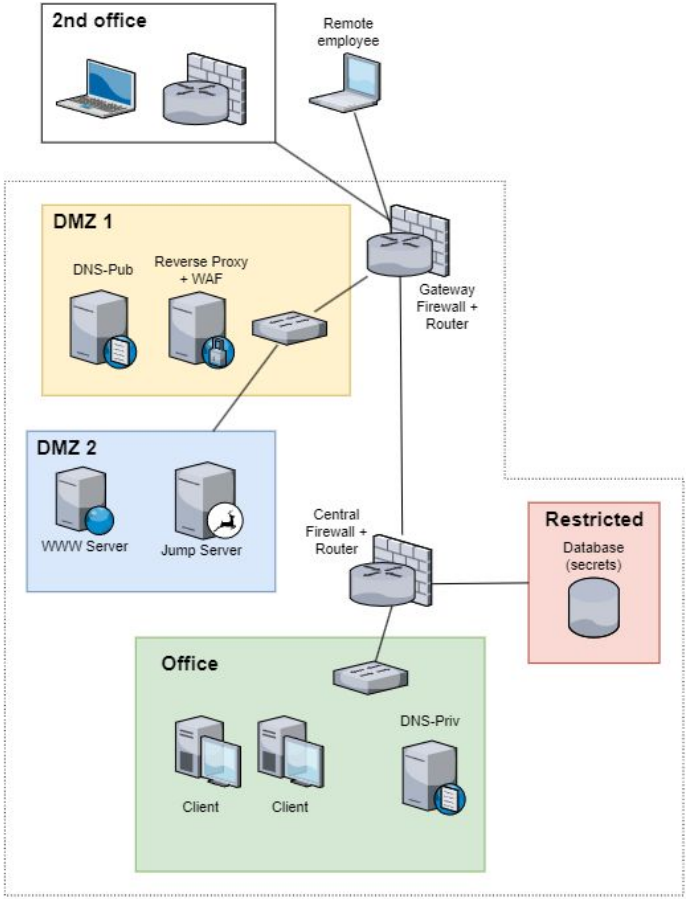
- Asset Management (ID.AM)
- Business Environment (ID.BE)
- Governance (ID.GV)
- Risk Assessment (ID.RA)
- Risk Management Strategy (ID.RM)
- Supply Chain Risk Management (ID.SC)
- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)
- Anomalies and Events (DE.AE)
- Security Continuous Monitoring (DE.CM)
- Detection Processes (DE.DP)
- Response Planning (RS.RP)
- Communications (RS.CO)
- Analysis (RS.AN)
- Mitigation (RS.MI)
- Improvements (RS.IM)
- Recovery Planning (RC.RP)
- Improvements (RC.IM)
- Communications (RC.CO)

Skład zespołu audytowego:

1. Sandra Al-Saaiydeh
2. Aleksandra Michalska
3. Jacek Pelczar
4. Aleksandra Sitarczyk

Diagram sieci

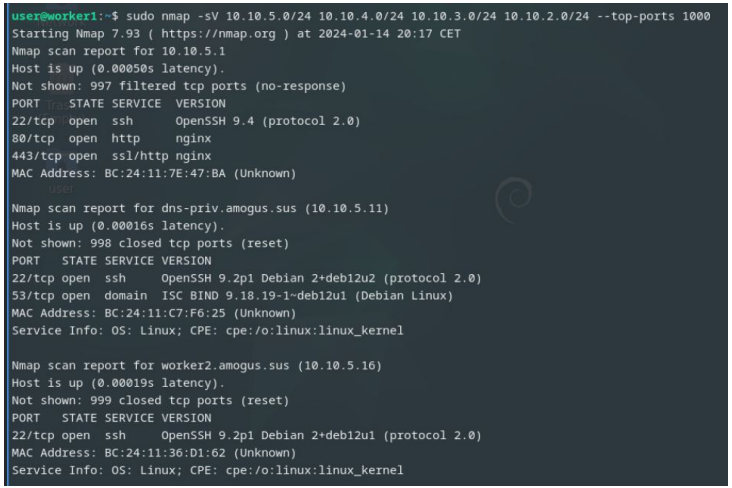
Następująco prezentuje się sieć środowiska, którego oceny bezpieczeństwa mamy dokonać, jako zespół odpowiedzialny za cyberbezpieczeństwo.

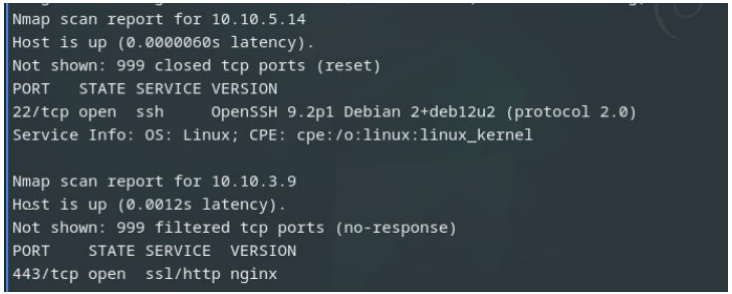


Część aktywna

W ramach części aktywnej przeprowadzone zostało skanowanie sieci w każdym VLAN-ie w firmowej sieci. Uzyskane wyniki pozwalają stwierdzić, że architektura sieci w zakresie routingu i switchingu jest bezpieczna, ponieważ hosty mogą połączyć się między sobą tylko w zakresie dostępu do usług wynikających z projektu sieci.

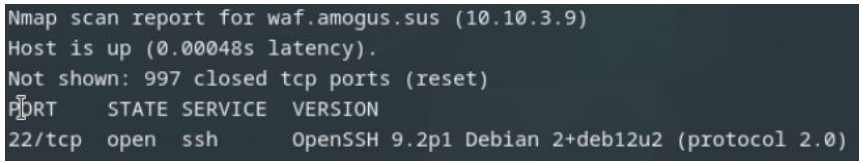
Skan miał także sprawdzić, czy dostępne usługi są przestarzałe, co dawałoby cień szansy na możliwą exploitację, na szczęście wszystkie usługi są aktualne do najnowszych dostępnych wersji.

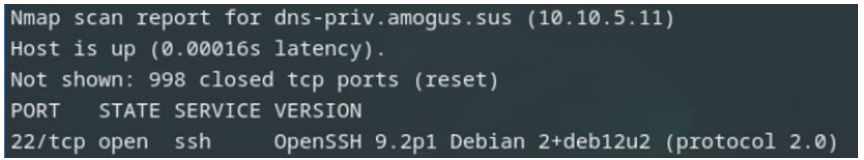


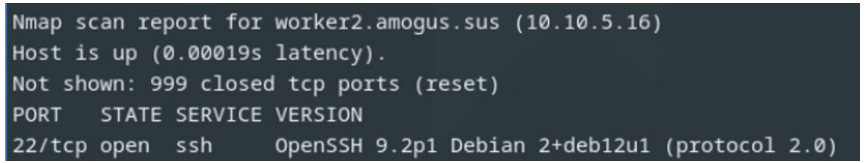


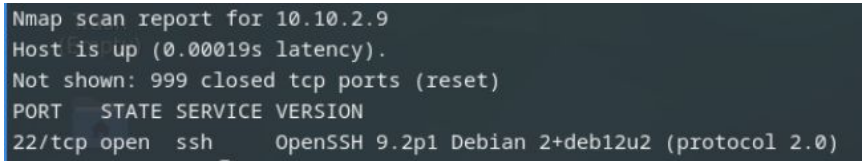
Potencjalne słabe punkty

Potencjalnym słabym punktem może być działanie serwerów SSH na wielu hostach na których jest to niepotrzebne, np. serwer dns, server waf itd. Może to tworzyć punkt wejścia dla złośliwego aktora. Proponowanym rozwiązaniem jest stworzenie Jump Server i skonfigurowanie hostów w taki sposób, aby akceptowały połączenia SSH tylko od niego, a dla wszystkich innych hostów serwery SSH byłyby niewidoczne. Użytkownik łączył by się bezpiecznym kanałem na Jump Server a następnie nawiązywałby połączenie do wybranego hosta z usługą serwera SSH.







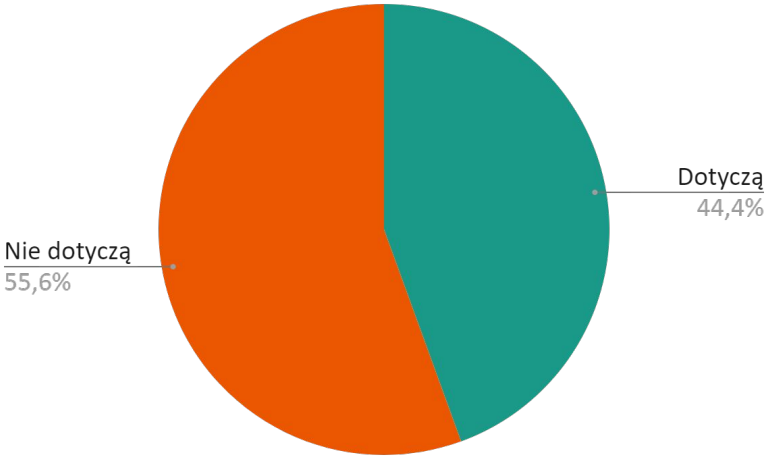


Audyt względem standardu

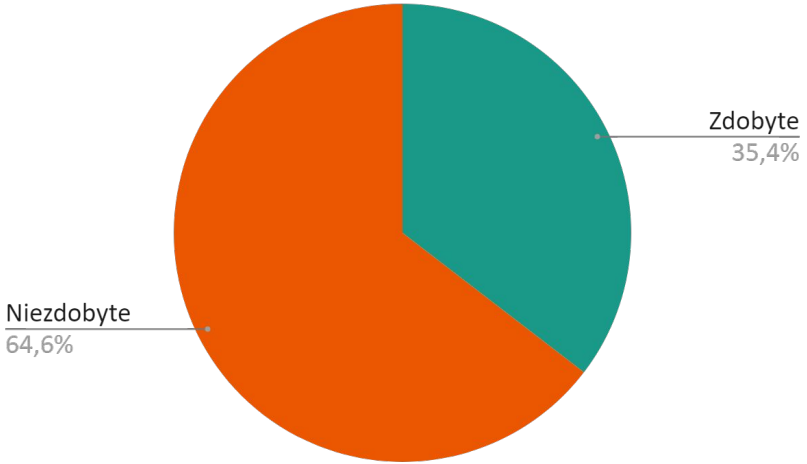
- Audyt dokonany względem kontroli pochodzących z NIST Cybersecurity Framework,
- W pliku Excel z kontrolami dodaliśmy kolumnę Rating, gdzie dokonaliśmy oceny każdej z kontroli,
- Legenda użytych oznaczeń w kolumnie Rating:
  - 1 - zrealizowane,
  - 0,5 - częściowo zrealizowane
  - 0 - niezrealizowane
  - N/D - kontrole niepodlegające problemowi (nie dotyczy)
- Po zsumowaniu przypisanych ocen możemy dokonać porównania, widocznego w tabeli poniżej. Wiele kontroli nas nie dotyczyło. Z kolei spora część kontroli, która nas dotyczyła nie została przez nas spełniona, ponieważ założenia projektowe nie obejmowały tych zagadnień.

Wszystkie kontrole	Ile uzyskaliśmy punktów	Ile kontroli nas dotyczyło	Ile kontroli nas nie dotyczyło
108	17	48	60

Wykresy kołowe przeprowadzonego audytu



Wykres dotyczących nas kontroli



Wykres zdobytych przez nas punktów

Obserwacje z audytu zgodności ze standardem

Znaczna liczba kontroli nie aplikowalnych do przedmiotu audytu wynika z braku możliwości uzyskania odpowiedzi od kadry menadżerskiej. Pracownicy audytowani nie byli w stanie formułować decyzji na temat strategii firmy, formalnych definicji ryzyk biznesowych czy oceniać wpływu incydentów na łańcuch dostaw produktów.

Ocenie podlegała pierwsza iteracja projektu i wdrożenia systemu, przygotowana przez inżynierów bezpieczeństwa. W celu przeznaczenia go do czynnego użytku w organizacji zalecane jest przeprowadzenie analizy ryzyk oraz przygotowanie planów ciągłości działania w zależności od szacowanych ryzyk i zagrożeń oraz przyjętego w firmie apetytu na ryzyko oraz obowiązujących regulacji prawnych. Ponadto, o bezpieczeństwie danych i infrastruktury decyduje również stopień wiedzy użytkowników systemu i regulacje wewnętrzne dot. dopuszczalnej eksploatacji.

Dziękujemy

Zespół **SPAM**

A. **S**itarczyk, J. **P**elczar, S. **A**l-Saaiydeh, A. **M**ichalska