Ogólne czynności jakie zostały wykonane podczas audytów bezpieczeństwa infrastruktury IT.

Test bezpieczeństwa stacji roboczych, sieci, serwerów został przeprowadzony na mobilnej stacji roboczej Dell Precision M4700 o specyfikacji sprzętowej:

System operacyjny: **Kali Linux**
Model procesora: **Intel Core i7-3840QM**
Liczba rdzeni procesora: **4**
Liczba wątków procesora: **8**
Taktowanie bazowe procesora (GHz): **2.8**
Taktowanie maksymalne procesora (GHz): **3.8**
Pamięć podręczna procesora(MB): **8**
Wielkość pamięci RAM: **32 GB**
Typ pamięci RAM: **DDR3**
Częstotliwość taktowania pamięci (MHz): **1600**
Rodzaj karty graficznej: **Grafika dedykowana**
Model karty graficznej: **NVIDIA Quadro K2000M**
Pamięć karty graficznej: **2 GB**
Typ dysku twardego: **SSD**
Szybkość odczytu dysku twardego [MB/s]: **550**
Szybkość zapisu dysku twardego [MB/s]: **520**

Tabela poniżej przedstawia ogólne informacje o przeprowadzanych atakach na infrastrukturę IT w celu weryfikacji oraz poprawy jakości bezpieczeństwa.

Typ ataku	Opis	Lokalizacja atakującego	Lokalizacja w infrastrukturze IT. uwagi
cracking	zgadywanie/łamanie/rozszyfrowywanie haseł dostępowych, algorytmów szyfrujących	Lokalnie/zdalnie	sieć WIFI/LAN/WAN, stacje robocze, serwery ***“Analiza zabezpieczeń”***
sniffing	podglądanie, podsłuchiwanie	Lokalnie/zdalnie	sieć Wifi/LAN/WAN, stacje robocze, serwer ***“Analiza zabezpieczeń”***
snooping	pasywne wejście do kabla: podpięcie do kabla i oczekiwanie na dane przekazywane np. analizatorami sieci	Lokalnie	Sieć Wifi/LAN/WAN ***“Analiza zabezpieczeń”***
spoofing	badanie sieci np.poprzez aktywne podpięcie do kabla tj. wpuszczanie do sieci danych i poleceń - np. symulowanego protokołu komunikacyjnego, podszywanie się pod kogoś - poprzez fałszywy adres internetowy- i uzyskanie dzięki temu nielegalnego dostępu do danych	Lokalnie	Sieć Wifi/LAN/WAN, urządzenia sieciowe ***“Analiza zabezpieczeń”***

back door	wejście do systemu systemu w inny sposób niż poprzez logowanie np. poprzez pocztę elektroniczną lub dzięki zainstalowaniu odpowiedniego oprogramowania, w celu np. podsłuchiwania wprowadzanych na klawiaturze znaków, co pozwala uzyskać hasło jeszcze przed jego zaszyfrowaniem	Lokalnie/zdalnie	Urządzenia sieciowe, sieć Wifi/LAN/WAN, stacje robocze, serwery ***"Analiza zabezpieczeń"***
Koń Trojański	Trojany zaszywane są w listach poczty elektronicznej, w plikach bat, com, exe, pseudo tekstowych (.hta) zawierających wykonywalne skrypty, obiektowych (.shs) , plikach rozpoznawanych na pierwszy rzut oka jako faktury, gry itp.	zdalnie	Urządzenia sieciowe, stacje robocze, serwery ***"Analiza zabezpieczeń"***
DDoS	blokowanie użytkownikom usług internetowych poprzez stwarzanie sztucznego tłoku w sieci	zdalnie	sieć WAN ***"Analiza zabezpieczeń"***
phishing	jest rodzajem oszustwa internetowego, polegającego na wyłudzeniu od klientów (po podszyciu się pod instytucję finansową - poprzez fikcyjną witrynę lub email) danych uwierzytelniających	Lokalnie	osoba fizyczna (pracownik) ***"Analiza zabezpieczeń"***
Evil Maid	atakujący z reguły musi uzyskać fizyczny dostęp do komputera ofiary aby podmienić bootloader. Stąd też nazwa "złośliwa pokojówka", wskazująca na sytuację w której zostawiamy laptopa w hotelowym pokoju, schodząc np. na kolację.	Lokalnie ataki zdalne są mało spotykane	stacje robocze, urządzenia mobilne ***"Analiza zabezpieczeń"***
brute force	echnika łamania haseł lub kluczy kryptograficznych polegająca na sprawdzeniu wszystkich możliwych kombinacji. Jest to prosta metoda pozwalająca w teorii na odgadnięcie każdego klucza.	lokalnie/zdalnie	Urządzenia sieciowe, sieć Wifi/LAN/WAN, stacje robocze, serwery, portale internetowe itp. ***"Analiza zabezpieczeń"***

Uwaga!

Każdy wymieniony powyżej (i nie tylko) atak na urządzenia cyfrowe przeprowadzany jest zazwyczaj w celu:

- **Utrudnienia poprawnego funkcjonowania systemów**
- **Kradzieży loginów/haseł oraz danych dostępowych**
- **Kradzieży danych** *(tzw. Wyciek Danych poufnych i nie tylko)*

PAMIĘTAJ!

Nic nie chroni cię w 100% w przypadku kradzieży między innymi przed:
- wyciekiem poufnych danych (nie tylko “Twoich”),
- kradzieżą tożsamości (nie tylko “Twojej”),
- Upublicznieniem danych oraz informacji itp.
-Przekazane Loginy, Hasła, oraz dostęp do danych poufnych należą tylko i wyłącznie do osoby upoważnionej do danych zasobów (ujawnienie tych danych osobom trzecim jest ***ZAKAZANE***)
-Dane dostępowe posiada również administrator oraz przedstawiciel firmy IT ART Łukasz Padula.

W razie jakiegokolwiek podejrzenia o wycieku danych bądź o jego możliwości niezwłocznie poinformuj o tym firmę

W razie niebezpieczeństwa kontakt 24/7
Oraz odpowiednie organy w tym PUODO

“Analiza zabezpieczeń”
Szczegółowe informację o wykonywanych czynnościach znajdują się w pliku ***“Analiza zabezpieczeń.xlsx”*** którego dokładną lokalizację zna tylko administrator.