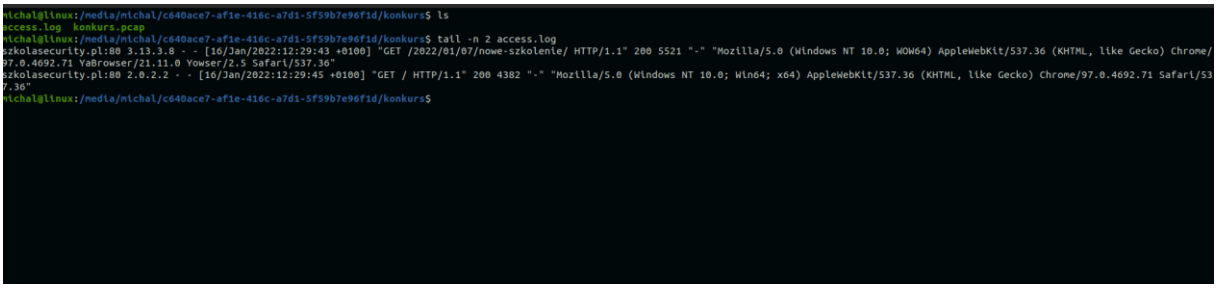
Logi Web serwera

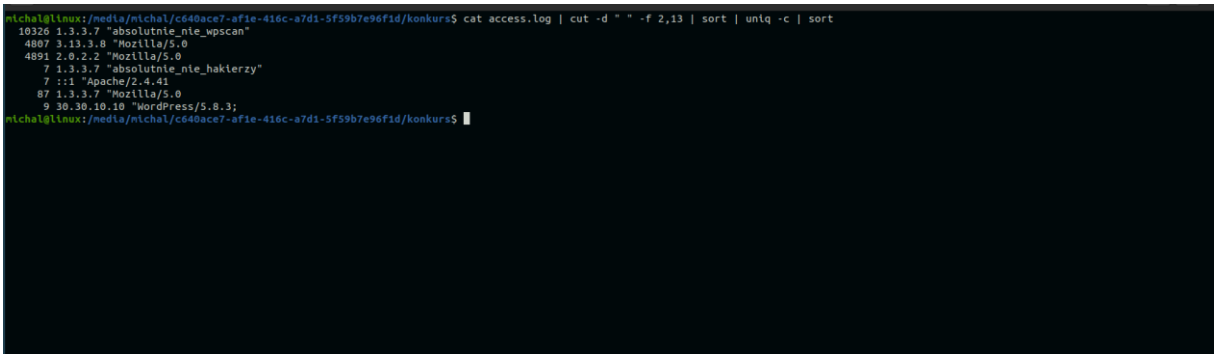
Otrzymujemy dwa pliki plik pcappng oraz logi serwera http, plik z ruchem sieciowym polecam zamienić na pcap umożliwi nam to jego analizę również w narzędziu tcpdump jednak w tym przypadku nie będziemy go używać.

1.Jaki jest adres IP Atakującego

Pierwszą rzeczą jaką zrobimy będzie wyświetlimy pierwsze dwa logowania aby sprawdzić dokładny format logów co pomoże nam w dalszej fazie analizy



Za pomocą narzedzi do filtrowania takich jak cat,cut,grep,uniq,sort będziemy starali się wyciągnąć coś podejrzanego:



Jak widać na screenie udało nam się znaleźć adres z podejrzanym polem User-agent a dokładnie z trzema różnymi, jest to prawdopodobny atakujący czyli odpowiedzą jest:

1.3.3.7

2.Z jakiego "User-agent" korzystał atakujący (podaj wszystkie 3):

Odzpowiedz znaleźliśmy już podczas wykonywania pierwszego zadania:

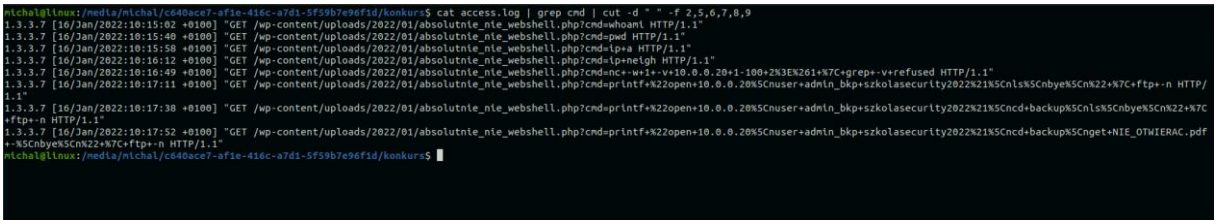
absolutnie_nie_wpscan

Mozilla/5.0

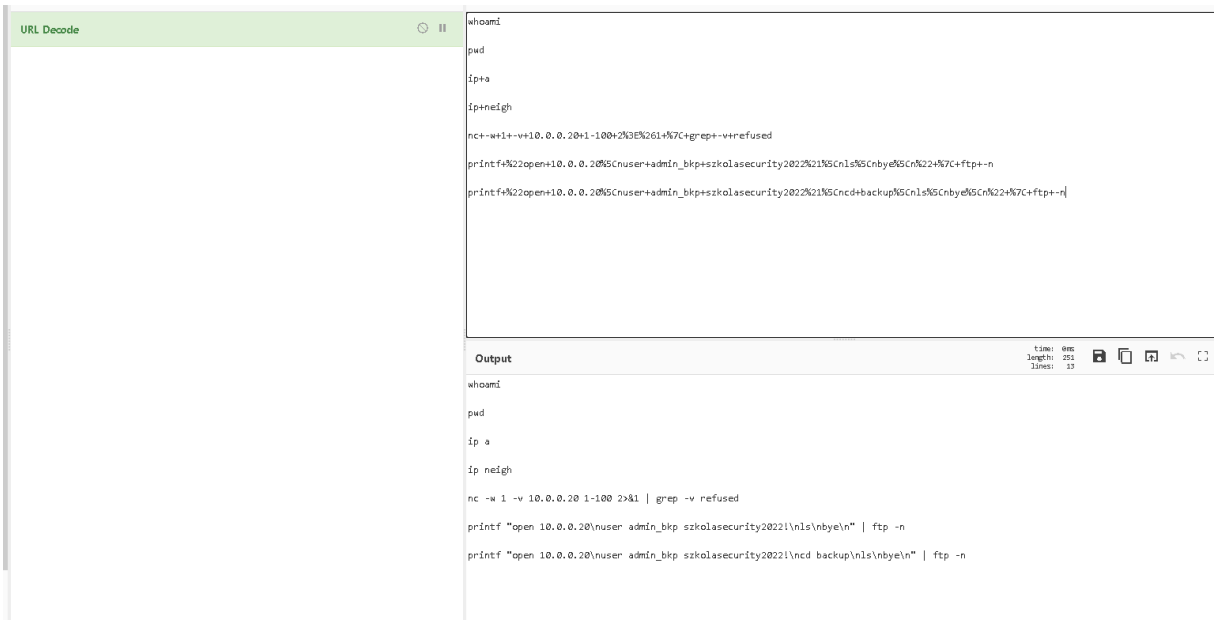
absolutnie_nie_hakierzy

3.Jakich komend używał atakujący przez webshell (podaj wszystkie 8)

Webshell jest to wrzucony na serwer webowy backdoor w postaci pliku php w którym znajduje się argument cmd do którego atakujący może się odwoływać np. poprzez modyfikacje nagłówka http lub po prostu doklejając do adresu ?cmd=”polecenie” spróbujmy więc znaleźć taki argument w zapytaniach z adresu atakującego:



Nie wszystkie polecenia są dla nas czytelne ponieważ zostały zakodowany aby można było je wykonywać z poziomu przeglądarki przypisując je do argumentu cmd dlatego użyjemy narzędzia cyberchef aby je odkodować:



Odpowiedź:

whoami

pwd

ip a

ip neigh

nc -w 1 -v 10.0.0.20 1-100 2>&1 | grep -v refused

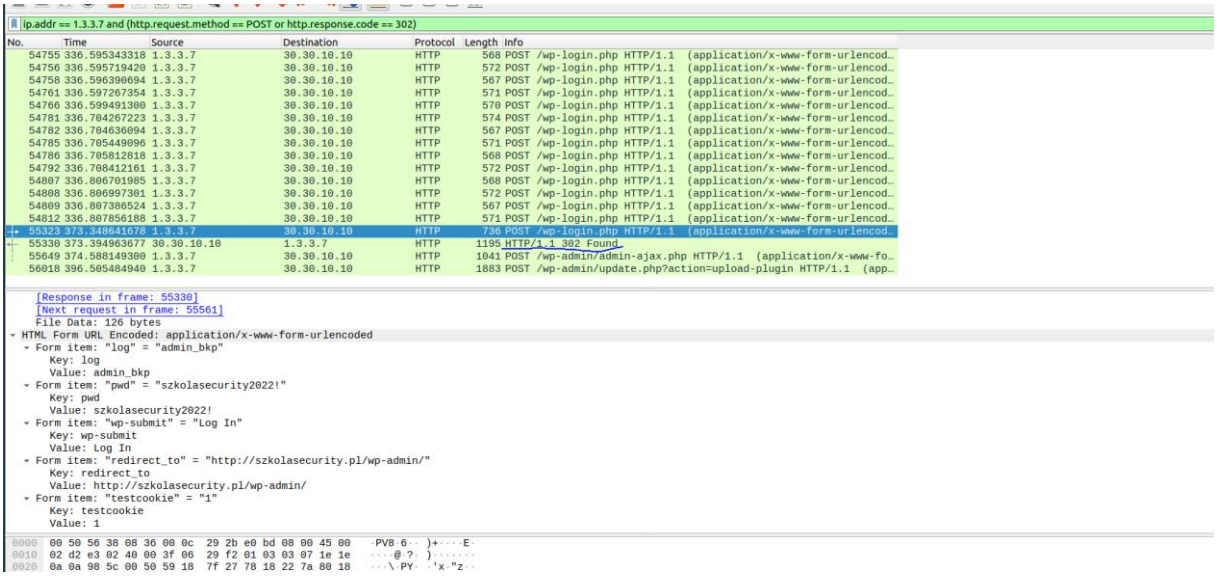
printf "open 10.0.0.20\nuser admin_bkp szkolasecurity2022!\nls\nbye\n" | ftp -n

printf "open 10.0.0.20\nuser admin_bkp szkolasecurity2022!\ncd backup\nls\nbye\n" | ftp -n

PCAP

4.Wpisz poprawne credentiale do wp (format: “login:pass”)

Aby odpowiedzieć na to pytanie musimy znaleźć zapytania które skutkowało odpowiedzą od serwera www kodem 302 czyli przekierowaniem na inną podstronę robimy to w następujący sposób:

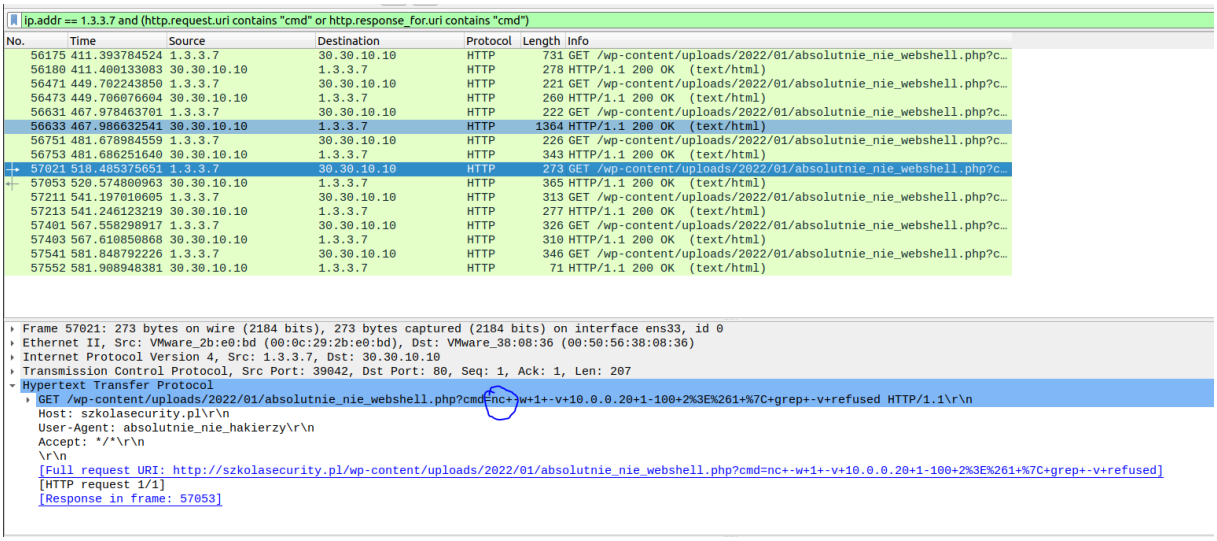


Odpowiedz:

admin_bkp:szkolasecurity2022!

5.Jaka jest odpowiedź z toola do rekonesansu wewnętrznego (jaki porty są otwarte - podaj 2)

Wiemy już że atakujący odwoływał się do parametru cmd w adresie aplikacji www dlatego tym razem również postaramy się wyfiltrować ten parametr w ruchu sieciowym.



W tym przypadku atakujący korzysta z narzędzia netcat co widać w odwołaniu do argumentu cmd w zapytaniu, zapewne serwer do którego miał dostęp nie było innych narzędzi dzięki którym mógłby to sprawdzić a pobieranie czegokolwiek wywołało by zbyt duży ruch.

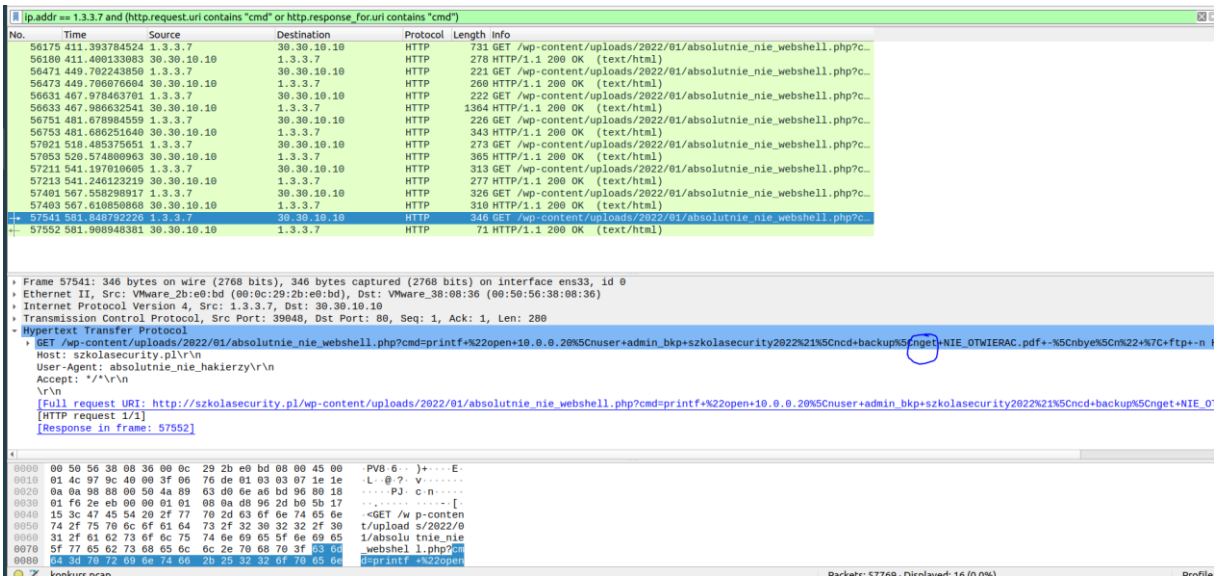
Odpowiedź:

Pod zapytaniem z parametrem cmd znajduje się odpowiedz serwera która wskazuje że porty 21 oraz 80 odpowiadają oznacza to że są otwarte (działają na nich usługi)

21,80

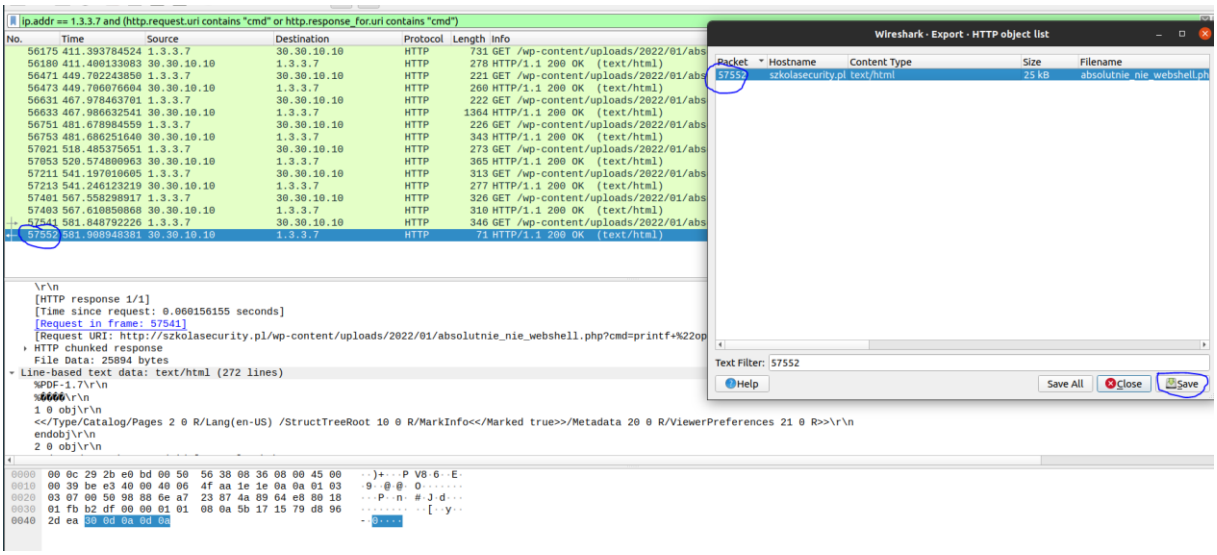
6.Jaki plik został ściągnięty przez atakującego?

Korzystając z tego samego filtru jak w pytaniu 5 idąc niżej możemy wywnioskować że atakującego zainteresował serwer FTP działający na porcie 21. Wyświetlił pliki które dostępne są na serwerze następnie wykonał polecenie get w lokalizacji w której znajdował się plik NIE_OTWIERAC.pdf:



7.Jaka była zawartość ściąganego pliku?

Przechodzimy w wiresharku do: File > Export Objects następnie filtrujemy po numerze pakietu widocznym po lewej stronie w pierwszej kolumnie:



Zapisujemy plik z rozszerzeniem .pdf możemy go uruchomić jako normalny plik pdf: