LABB 2

VINCENT PALMA
IOT20

SNIFFING

WIRESHARK

TCPDUMP & LIBPCAP

UPPGIFT

Labben går ut på att sniffa en simulerad anslutning mellan en webbserver och en webbläsare i den virtuella maskin du använde i labb 1.

Målet är att få ut användarnamnet och lösenordet som används för inloggningen.

Mängder av nätverksprotokoll används för att kommunicera mellan olika tjänster eller hårdvara, exempelvis FTP för filservrar, HTTP för webb, Telnet för att nå nätverksroutern (bland andra användningsområden), osv. Dessa skickar paket av information till och från.

Om protokollet kommunicerar i klartext, och någon skrupellös aktör sniffar paketen, kan känslig information enkelt utläsas.

Poängen med den här labben är att visa er det.

Utförandet av uppgiften

Ubuntu körs på en virtuell maskin som är installerad på en PC med Windows 10. En zip som innehöll kod för att kunna utföra denna labb var förberedd från skolan användes.

Allt genomfördes via terminalen förutom Wireshark då den har ett grafiskt gränssnitt.

Två av de medförda filerna i typen bash behövdes göras körbara och för att uppnå det skriver man chmod +x [namnet på filen] i terminalen.

chmod står för Change Mode och det vi gör med +x kommandor är att vi gör den specifierade filen körbar med att ändra dess kör-rättigheter.
(*https://sv.wikipedia.org/wiki/Chmod*)

Detta behöver vi ändra på samtliga filer då vi måste kunna läsa och skriva till dem för att kunna använda dem. Finns risk att få fel om detta inte görs.

Skulle säga att det som utförs är liknande om inte en MiTM attack (man in the middle) där vi lägger oss mellan användaren och sidan för att se trafiken. Det är svårt att upptäcka då vi bara lyssnar.

https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Det som är bra att tänka på är att köra allting med root privileges, mao sudo ....
Detta "låser" upp så att vi kan använda de programmen vi behöver för uppgiften med root rättigheter.
Sudo (superuser do) bör köras med försiktighet då den har rättigheter att ändra operativet vilket med fel hantering kan få det att krasha.
Detta är dock okej i detta fall då operativet körs i en virtuell miljö och det är lätt att återställa.

De frågor som skall besvaras

: TVÅFAKTORSAUTENTISERING

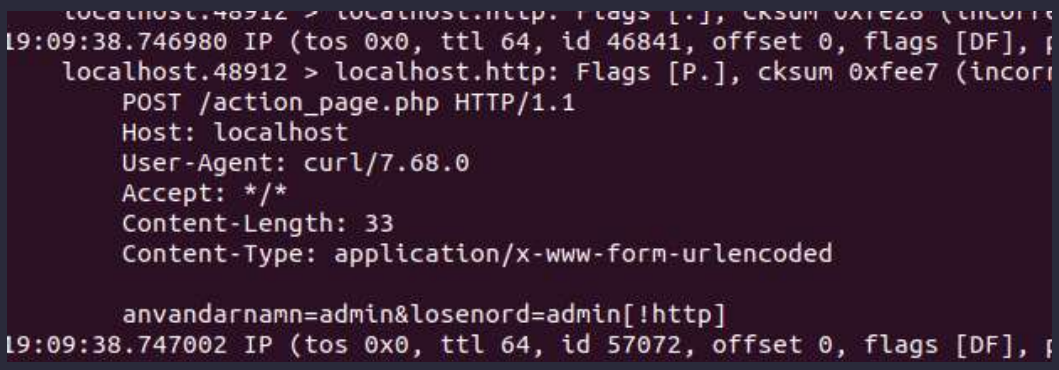
Det här är uppenbarligen problematiskt, och visar på hur viktigt det är med krypterad trafik. Ett annat
sätt att höja säkerhetsnivån gällande inloggningar är något som kallas för “tvåfaktorsautentisering”.

1. Redogör vad det är för något.
2. På vilket sätt skulle det kunna hjälpa oss här?
3. På vilket sätt skulle det inte hjälpa oss här

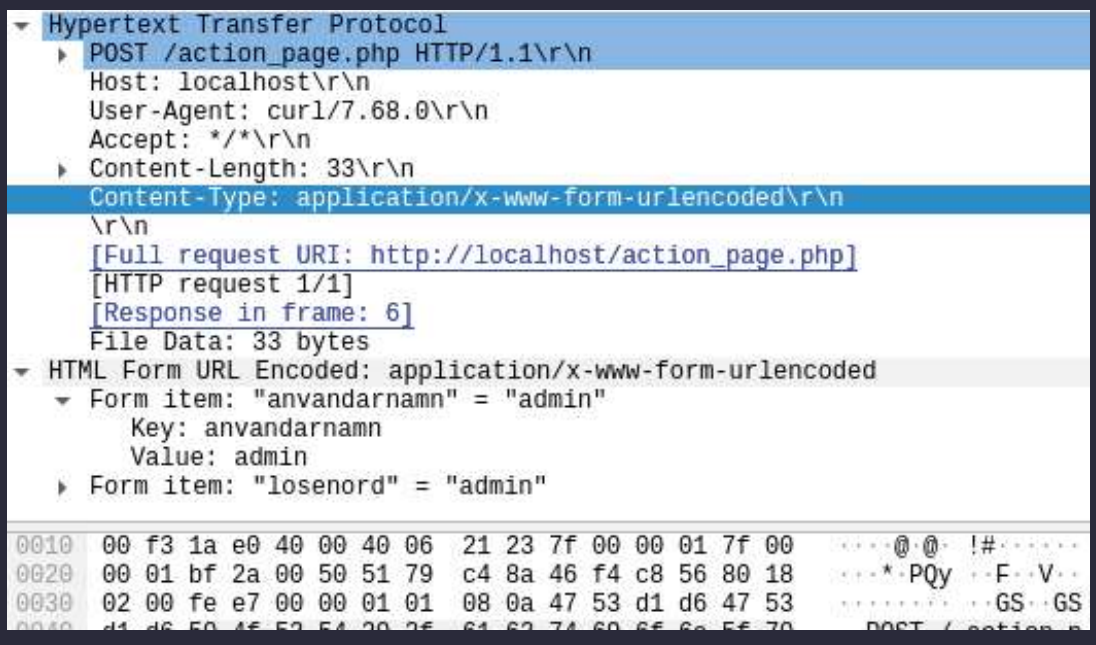
1.
Tvåfaktorsautentisiering (2FA) ger oss möjligheten att kunna hålla borta oönskade intrång till vår information med hjälp av en kombination av två olika komponenter. Ett exempel är Paypal som i år har ändrat reglerna för att följa europas nya standard för betalhantering.
När man loggar in så skriver man in sitt användarnamn och lösenord, detta är en standard Enfaktorssautentisering men de har nu lagt på en obligatorisk faktorautentisering där de skickar ett meddelande med en kod till den mobilen som är registrerat på kontot. Detta nummer skriver man in i rutan som kommer upp på sidan och är den korrekt så kan man använda tjänsten. Detta är en 2FA.

2.
Problemet vi har i denna uppgift är att det är väldigt lätt att se användarnamnet och lösenordet för adminkontot om man nu tar och sniffar datat som skickas.

Både när man använde tcpdump och läste av trafiken som skickades fram och tillbaka samt även när Wireshark användes så kunde vi lätt se hur användarnamn samt lösen exponerades i trafiken.



Här kan vi se en print screen på terminalen där det som egentligen ska vara hemligt inte är det.



Här kan vi se en print screen av Wireshark där det som egentligen ska vara hemligt inte är det.

3.

Bra fråga. Eftersom att trafiken inte är krypterad och vi kan se vad som skickas och tas emot så kan vi även lätt komma åt datat för den andra verifieringen. Räcker med att den visas en gång så kan vi även komma åt kontot. Finns massa sätt att knäcka 2FA skyddade, hittade tex denna artikel som ger 5 sätt att göra det på *https://www.csoonline.com/article/3620223/how-to-hack-2fa.html* .