**Vision WoodPecker FTP Penetration Jonas Holte jh222vp**

*Introduktion*

Mitt intresse för IT-Säkerhet har länge funnits med i bilden, men det är inte förens nu jag har lagt ner tid på att undersöka vilka tekniker och mjukvaror som finns för att testa och undersöka säkerheten hos datorer och serverar. Planen med mitt mjukvaruprojekt blir att bygga ett eget verktyg som testar att säkerheten mot en server som använder sig av File Transfer Protocol (FTP) med hjälp av olika attacker. Allt är i utbildningssyfte för att få kännedom och kunskap hur en attackerare kan tänka och gå tillväga när de bygger sina vektyg för att penetrera säkerheten hos tillexempel en klient eller server.

Användargrupper

Penetrationtestare

-Hög teknisk kompetens, bred kunskap inom IT-Säkerhet.

Säkerhetkonsulter

-Hög teknisk kompetens, stor kunskap inom IT-Säkerhet och dess system.

IT-Säkerhetsintresserade

-Medel till hög teknisk kompetens, liten, medel eller hög kunskap inom IT-Säkerhet.

Studenter

Kunskap kan skilja sig hos denna grupp angående den tekniska kompetensen, liten, medel eller hög kunskap inom IT-Säkerhet.

Människor som vill pröva sin egen säkerhet/ lösenord.

-Medel till hög teknisk kompetens, liten, medel eller hög kunskap inom IT-Säkerhet.

Övriga intressanter

-Okänd teknisk kompetens, okänd kunskap inom IT-Säkerhet.

Liknande System

THC Hydra

[https://www.thc.org/thc-hydra](https://www.thc.org/thc-hydra/)

FTP Password Kracker

<http://securityxploded.com/ftp-password-kracker.php>

FTP Brute Force Tester

<http://www.secure-bytes.com/ftp-brute-force-tester.php>

Low and Slow Brute Force FTP Scanner

[http://low-and-slow-brute-force-ftp-scanner.soft112.com](http://low-and-slow-brute-force-ftp-scanner.soft112.com/)

FTP-Brute

<http://nmap.org/nsedoc/scripts/ftp-brute.html>

Ncrack - Brute Force Attack on RDP, VNC, SSH, FTP

<http://www.securitytube.net/video/6780>

Baskrav

**1.1** Applikation FTP Brute Force kommer bestå av en samling med olika attacker, några av dessa kommer t.ex vara:  
  
**Brute Force:** Gissar kominationer tills det rätta lösenordet hittas.

**Username Brute Force:** Välj ett lösenord som man sedan testar en mängd olika användarnamn emot tills det att en match uppstår.

**Dictionary Attack**: Läser ord ur en vald ordlista för att gissa sig fram till rätt lösenord på servern.

**Low Radar Brute Force**: Välj antal försök som ska gissas på lösenordet för att sedan vänta en önskad tidsperiod innan nästa försök görs igen.

**Burst Mode:** Gör tre försök på användarnamn / lösenord för att sedan vänta ett slumpat antal minuter innan nästa tre försök görs.

**2.1**

Statistik ska skrivas till en textfil när en attack är lyckad. Denna ska innehålla tid, datum, antal gissade försök på användarnamn/lösenord, samt användarnamn och lösenord som gav lyckat resultat.

**2.2** Möjlighet att skicka ett e-post till en önskad adress när en attack är lyckad. E-postet ska innehålla tid, datum, antal gissade försök på användarnamn/lösenord, samt användarnamn och lösenord som gav lyckat resultat.

**3.1** Möjlighet att se nödvändig information innan attacken börjar, så som intern samt extern IP adress, MAC-adress, CPU med klockfrekvensen och mänden RAM med mera.

**4.1** Möjlighet att scanna av portar från en server. Portscanner.

Teknik

Jag kommer bygga mitt verktyg i form av en Console Application i språket C# för att hålla ned prestandan som krävs av klienten för att köra programmet. Jag väljer också att använda mig av språket C# eftersom det är något jag tidigare arbetat med och känner mig säker i.