# Basic Pentesting

![HEADER]()

## Introduction

Detta är en writeup av rummet basic testning. Man skulle kunna se det som en Black box penn testing då vi egentligen bara fick ett i p nummer men kanske att man ska kalla det grey box i och med att vi hade en rad frågor att utgå ifrån som i viss mån avslöjade vad vi letade efter. Jag gjorde uppgiften tillsammans med en kompis vilket var väldigt kul då vi kunde hjälpas åt och lära oss av varandra.

Rummet bestod av ganska många frågor och jag kommer inte att presentera svaret på alla, utan jag kommer att skriva en sammanhängande text som sen resulterar i hur vi hittade svaret på den sista frågan. Den sista frågan var:

> What is the final password you obtain?

## Initial Recon

Eftersom vi bara hade ett i p nummer så började vi med att köra en en nmap scan för att ta reda på vilka öppna portar det fanns och vilken service de körde.

![NMAP SCAN]()

Som vi kan se så fanns det några intressanta portar öppna, bland annat till SSH, HTTP och SMB. SMB särskilt intressant för att det är förknippat med olika sårbarheter, men låt oss börja men jag kolla port 80. Jag startade webbläsaren och slog in IP-numret och hittade den här trevliga hemsidan:

![LANDING PAGE]()

Detta hintade ju om att det skulle kunna finnas fler sidor att upptäcka. Jag kollade source och fick se en kommentar som uppmanar en om att kolla development notes. Det var dags att leta efter fler paths. Jag satte i gång Gobuster och fick en träff relativt omgående.

![GOBUSTER]()

Jag lät Gobuster och köra igenom hela listan men hittade inga andra paths. På /development så fanns det länkar till två olika textfiler med följande innehåll:

![DEV\_TXT]()

![J\_TXT]()

Texterna verkade innehålla kommunikation mellan några som kallade sig för J och K, Man kunde anta att det var första bokstaven i deras namn. I den ena texten stod det även att Apache och SMB körs något som vi redan hade bekräftat med vår nmap scan. Extra intressant var meddelandet som verkade antyda att K använde ett svagt lösenord. Förhoppningsvis skulle vi kunna utnyttja detta senare.

## Keep on Enumerating

Eftersom vi inte hittade någon uppenbar väg in via hemsidan valde vi att titta vidare. Jag körde enum4linux mot IP-adressen för att se vad jag kunde hitta. Något som var extra intressant var listan över användare, det fanns två namn som matchade med vad vi hade hittat på hemsidan, nämligen `kay` och `jan`.

![USERS]()

Jag kollade även vad det fanns för shares via SMB och jag kunde hitta att det fanns en som heter `Anonymous`.

![SMB]()

Jag kopplade upp mig till en anonymus och där fanns en textfil som hette `staff.txt`. Tyvärr innehöll den inget annat än ytterligare ett meddelande mellan Kay och Jan.

![STAFF\_TXT]()

## Two Semi-fails in a Row

Vi tog oss an två angrips försök som egentligen inte ledde någonstans, därför kommer jag inte beskriva dem i detalj men jag vill ändå nämna hur vi tänkte.

Det första var att försöka knäcka SMB-lösenorden till användarna Kay och Jan. Vi lyckades med det men vi kunde inte hitta några fler shares. It was dead end.

Det andra vi försökte ta oss an var att komma in via Tomcat. Vår nmap scan visade ju att port 8080 var öppen och körde Tomcat. Vi provade att bruteforce så inloggningen där utan någon lycka. Det var dags att tänka vidare.

## Port 22

Vi hade ju sett att pott 22 var öppen och vi visste att användarna Kay och Jan fanns på systemet. Det var alltså dags att försöka bruteforce SSH-inlogget. Jag satte i gång hydra och fick relativt snart en träff på användaren Jan.

![HYDRA\_SSH]()

Vi loggade in med Jan och började titta runt på systemet. Det vi letade efter var intressanta filer och vektorer för att öka våra privilegier. Vi kunde snabbt dra slutsatsen att `Jan` var en vanlig användare utan några större behörigheter. Jag började därför undersöka om det fanns några bin-filer med `the s bit set`, men det fanns tyvärr inga jag kunde utnyttja. Den enda som fanns var `pkexec`, men det krävdes att man kunde köra det med `sudo`.

Genom att köra kommandot `getent group sudo` kunde vi däremot avgöra att användaren `kay` hade sudo-behörighet:

![SUDO]()

Vi kollade i Kay’s home-folder och där fanns flera intressanta saker, bland annat en fil som hette `pass.bak` och ett par mappar, bland annat `.ssh`. När jag försökte skriva ut innehållet av `pass.bak` fick jag tyvärr access denied, så det här var åtminstone en fil jag ville återkomma till.

Efter en närmare titt i `.ssh` kunde vi hitta inget mindre än en privat ssh-nyckel! Och den gick att skriva ut, sweet!

![PRIV\_KEY]()

## Cracking Time

Med lite tur så hade användaren `kay` använt ett svagt lösenord kopplat till sin privata nyckel. Vi lät `john` do it’s magic. Först `ssh2john` för att få ett format som `john` förstår, sen cracking time. Om det var ett svagt lösenord? Oh yes.

![JOHN]()

Nu var det easy peasy att ssh:a in som `kay` med den privata nyckeln och skriva ut innehållet i `pass.bak`.

![PASS\_BAK]()

## Final Thoughts

Detta var en rätt klurig utmaning då vi inte hade så mycket att gå på, som sagt, nästan en black box pentest. Även om det ser ut att ha varit ganska straight forward så tog det lång tid, och vi fördjupade oss i ett antal olika steg som inte ledde någonstans. Men! Att stegen vi tog inte ledde oss till svaret direkt gjorde egentligen inget, då vi i stället fick en större förståelse för systemet vi arbetade med för att vi till slut skulle kunna lägga pusslet.