

Laboration i DD2495: Säkerhetshål och attacker

18 februari 2009

Uppgift 1

Ladda ner och installera gratisprogrammet Nessus, och läs igenom användarmanualen på nätet om du känner att det behövs.

Starta därefter Nessus Server Configuration, och starta Nessus Scanner Service.

Starta sedan Nessus Client, och scanna den dator du sitter vid med Default Scanning Policy. Hittar du något som borde åtgärdas?

Scanna sedan 3 av dina favorithemsidor med Nessus. När du är färdig, visa rapporterna för dessa scannningar för en laborationsassistent, så får du ett IP.

Scanna IP-numret du fick. Får du något svar från servern? Hittar du något som borde åtgärdas? Redogör noggrant för alla säkerhetshål du hittar, hur de går att utnyttja, samt vad som går att göra för att laga dem.

Uppgift 2

Nu är det dags att vara lite elak. Tyvärr måste vi vara kontrollerat elaka, så denna del av laborationen får bara utföras på en egen laptop, eller den som tillhandahålls av laborationsassistenterna. Om du får vänta, läs dokumentation om programmet Cain & Abel under tiden.

Ladda ner och installera programmet Cain & Abel. Lek lite med det tills du känner dig någorlunda van vid det. Försök sedan knäcka lösenorden för de konton som finns på datorn med brute force. Testa olika permutationer av möjliga tecken. Hur länge orkar man rimligtvis vänta?

Cain & Abel har många fler funktioner. Till exempel går det att sniffa lokala nätverk, och utföra en man-in-the-middle-attack. För det sista steget ska du veta hur man utför en sådan, och vilken information man kan komma åt. Däremot ska du *inte* utföra attacken, då riskerar vi att det kommer en arg datasäkerhetsansvarig.