

Attackväg 2 - Wifi

Physical - Lager

Angriparen skannar området och hittar wifi-nätet som använder ålderdomlig kryptering.

WPA eller WPA2 med TKIP

Data-link - Lager 2

Angriparen utför en deauth-attack så klienter kopplas bort från nätet och måste återansluta.

Med tex airdump ng så fångar han 4-way handshake när de återansluter.

Angriparen kan nu i lugn o ro testa en massa lösenord offline med verktyg som tex hashcat eller Aircrack ng.

Om det testade lösenordet ger samma hash så har han hittat rätt.

Network - Lager

Wifi:et är uppsatt för att det ska förenkla för de anställda. Accesspunkten är därför antagligen ansluten till VLAN 10. Angriparen har nu tillgång till VLAN 10 och har samma åtkomst som interna arbetsstationer.

Angriparen som nu fått ett internt IP via dhcp kan nu nå servern och få tillgång till företagets data.

Lager 4 - 7

Datan stulen och ev krypterad server.

Confidentiality: Hög - angriparen når interna system och data

Integrity: Medel - risk att data manipuleras eller trafik påverkas

Availability: Låg-Medel - nätet kan störas (deauth, DoS)

Attackväg 3 - SQLI

Application Layer

Angriparen hittar en extern webbsida som körs på port 80.

Webbplatsen har endast ett lösenordsfält och saknar username.

Skriver ' OR 1=1 -- i lösenordsfältet.

1=1 är alltid sant, så databasen returnerar minst en rad. Applikationen tolkar detta som en lyckad inloggning.

Network Layer

Webbservern kommunicerar direkt med den interna databasen. Angriparen får nu samma åtkomst som den interna backend-processen och kan exekvera fler SQL-frågor via webben.

Application Layer

Angriparen har åtkomst till

- Kunduppgifter
- Persondata
- Användarkonton
- Löneinformation
- Struktur över hela databasen

Lager 4 - 7

Datan stulen eller ändrad.

Confidentiality: Hög, angriparen får direkt åtkomst till databasen.

Integrity: Hög, data kan ändras, raderas eller manipuleras.

Availability: Medel, risk för driftstopp om databasen skadas.