Uppdragsbeskrivning externt penetrationstest

Denna uppdragsbeskrivning avser penetrationstest av X externt publicerade tjänster. Uppdraget utförs i syfte att kartlägga vilka system som exponeras och om något av dessa innehåller brister i funktion eller konfiguration som gör det möjligt att missbruka dem.

1.1 Metod

Uppdraget kommer utföras från Internet utan utökade behörigheter i förhållande till andra potentiella angripare. En specifikation över vilka IP-adresser som analysen ska omfatta är den enda information som delges inför testet.

1.2 Omfattning

Efter att respektive tjänst kartlagts kommer aktiva försök att upptäcka och utnyttja sårbarheter i dessa utföras för att besvara följande frågor:

- Vilken typ av system har identifierats
- Vilken information exponeras, kan läcka ut eller stjälas
- Finns möjlighet att manipulera informationen
- Finns möjlighet för vidare eskalering (på lokalt eller till andra system)
- Övriga sårbarheter som påträffas under arbetets gång

1.3 Avgränsning

Uppdraget syftar inte till att kartlägga hot där X är ett utpekat specifikt mål. Därför kommer nedanstående test/metoder inte att inkluderas.

- Social manipulation av anställda på X eller partners till X
- Ingen behörig åtkomst kommer ges till något system i syfte att därifrån testa möjligheter till eskalering
- Ingen sårbarhetsscanning/försök till intrång från X interna nätverk
- Ej använda identifierade sårbarheter för att signifikant försämra prestanda eller ta ned ett system, endast dokumentera möjligheter och troliga orsaker
- Ej faktiskt manipulera eller radera information, endast dokumentera möjligheter och troliga orsaker

1.4 Utförande

Arbetet utförs och slutförs under början av **februari 2023**. Arbetet får endast inledas och pågå under överenskommen tidpunkt och tidsspann.

- X informeras och godkänner i förväg vilka dagar testerna genomförs samt vilka IP-adresser som uppdraget kommer genomföras ifrån.
- Allvarliga sårbarheter skall rapporteras till X under arbetets gång, särskilt vid framgångsrik penetration av system och om detta kan lagas/hindras via en snabb och känd åtgärd.
- Lämpliga representanter från X förbinder sig att vara tillgängliga på kort varsel under uppdragets gång

1.5 Leverans

Uppdraget levereras i följande form:

- Rapporten ska vara skriven på engelska
- Skriftlig rapport som översiktlig beskriver hur uppdraget genomförts inkl. metoder, sammanfattar identifierade sårbarheter per system och förslag på åtgärder utformade som konkreta aktiviteter och prioriterat utefter allvarlighetsgrad. Framgångsrik penetration av system och åtkomst till information dokumenteras inkl. förslag på åtgärder utformade som konkreta aktiviteter och prioriterat utefter allvarlighetsgrad.
- Rapporten får endast levereras på ett säkert sätt, t.ex. krypterad enligt ök. före leverans.
- Om behov finns presenteras även resultatet på fysiskt möte med representanter från X. Kostnad för möte kan tillkomma om detta ej avtalats innan.

1.6 Sekretess

- All dokumentation kring uppdraget samt dokumenterade resultat av uppdraget skall betraktas och hanteras som mycket känslig information av uppdragstagaren.
- Utföraren av uppdraget förbinder sig att radera all information och dokumentation kring uppdraget när det avslutats (insamlad information, även rådata, arbetsmaterial samt framställd rapport).