NUCCC 2012

The ServerGames

Missa inte årets hackerhändelse sista veckan i augusti (28-31),

Kan du operativ IT-säkerhet? Eller har du bara väntat på ett tillfälle att få testa Metasploit lite mer? I så fall kan det vara du som vinner ServerGames 2012 och får ta emot pris på NUCCC den 14 september. Anta utmaningen!

Vad handlar tävlingen om?

I en annan tid och ett annat moln har alla datorföreningar blivit av med sina datorhallar och behöver därför skaffa nya. Samtidigt finns det massor av oanvända datorer som bara väntar på att bli övertagna. I ServerGames är målet att hitta maskiner som innehåller särskilda ”tickets” och ta kontroll över dessa. Poäng delas ut kontinuerligt baserat på de ”tickets” som lagen förfogar över.

Datorer med ”tickets” kommer att placeras i datornät som realtidövervakas av en systemadministratör. Eftersom administratören kommer att försvara systemen finns skäl att vara försiktig så att attacker och övertagande av ”tickets” görs obemärkt. Dessutom, de datorer som innehåller ”tickets” måste först hittas.

Vinner gör det lag som efter tävlingen har samlat på sig flest poäng genom att ta över ”tickets” och behålla dem för sig själva.

The ServerGames – en tävling i IT-säkerhet

När, var och hur?

Tävlingen genomförs i samarbete mellan Lysator och FOI i FOI:s datorkluster. Detta är en miljö bestående av över 300 fysiska servrar varpå ett stort antal virtuella maskiner körs. I den virtuella miljön kan det skapas komplexa nätverksmiljöer och förtagsnät med servrar, klienter och simulerade datoranvändare. Miljön har tidigare använts till såväl internationella red-team vs. blue-team tävlingar (t.ex. Baltic Cyber Shield 2010) som direkta experiment på IT-säkerhet. Lagen får använda vilka verktyg man vill, men verktygen i distributionen BackTrack [1] är tillräckliga. Mer detaljerade instruktioner kommer att delas ut till anmälda lag.

I FOI:s datorkluster kommer en IT-miljö att skapas som är anpassad just för denna tävling. Deltagarna ansluter till datorklustret med sina egna maskiner (lämpligen från en virtuell dator) över Internet via en VPN-lösning. Tävlingen startar kl 8:00 tisdag 28:e augusti och pågår dygnet runt till kl 15:00 fredag den 31:a augusti. Under måndag 27:e Aug sker kommunikationstester mellan lagen och spelmiljön.

Anmälan och mer information

Deltagande är gratis och görs i lag om maximalt 8 personer. Anmälan skickas till servergames@foi.se innan torsdag den 23:e augusti med information om lagnamn, deltagare och epostadress. En eventuell avanmälan skickas till samma adress.

Vinnarna av Baltic Cyber Shield 2010.

Varför är FOI med och anordnar en tävling?

FOI har sedan flera år forskat på IT-säkerhet. Precis som andra forskargrupper med intressen i IT-säkerhetsområdet har FOI svårt att samla in högkvalitativ data rörande IT-säkerhet (tex attacker) från driftsatta IT-miljöer. Dels är sådan data ofta känslig, dels har den ofta kvalitetsproblem (tex vet sällan säkert vilka attacker som egentligen skett). Att utföra tävlingar i en kontrollerad miljö är en lösning på detta problem. FOI kommer alltså att samla in data från denna tävling i forskningssyfte och sedan publicera och/eller dela sådan data med kollegor vid universitet och andra institutioner inom forskarvärlden. Exempel på data som kommer att samlas in är loggar från IDS:er som är installerade i systemet, nätverkstrafik och lagens förfogande över ”tickets”. Deltagande förutsätter att man accepterar att data samlas in. För mer information om detta, kontakta Teodor Sommestad (teodor.somemstad@foi.se).

Det bakomliggande forskarprojektet finns bl.a. beskrivet i: http://www2.foi.se/rapp/foir3342.pdf och http://www2.foi.se/rapp/foir3419.pdf .

För mer information, kontakta oss på
servergames@foi.se

Framsidesbild: Simon A. Eugster, Dagmar d'Surreal

FOI
Totalförsvarets Forskningsinstitut
164 90 Stockholm

Tel: 08-555 030 00
Fax: 08-555 031 00

www.foi.se