Engineer

Penetrationstest

en godkänd attack som visar om sårbarheter går att utnyttja

Vad det är

Ett penetrationstest, ofta förkortat pentest, är säkerhetstestning där testarna efterliknar verkliga attacker för att hitta vägar runt säkerhetsfunktionerna i en applikation, ett system eller ett nätverk. NIST:s tekniska vägledning för testning och bedömning av informationssäkerhet, SP 800-115, konstaterar att det ofta innebär att genomföra riktiga attacker mot riktiga system och data, med de verktyg och tekniker som angripare själva använder. Den kortare definitionen i SP 800-53 Rev. 5, NIST:s katalog över åtgärder för säkerhet och integritetsskydd, tillägger att de som testar vanligtvis arbetar inom bestämda ramar, och det är just det som skiljer ett test från en attack: testet är godkänt, avgränsat och skriftligt överenskommet innan det börjar.

Det som skiljer det från annan säkerhetstestning är målet. En sårbarhetsskanner jämför det den ser med beskrivningar av kända svagheter och rapporterar vad som kan finnas där. Den som utför ett penetrationstest försöker utnyttja svagheten. SP 800-115 uttrycker skillnaden rakt: skannrar kontrollerar bara om en sårbarhet kan finnas, medan attackfasen i ett penetrationstest utnyttjar den för att bekräfta att den faktiskt finns. De flesta tester letar också efter kombinationer, alltså svagheter i ett eller flera system som tillsammans ger mer åtkomst än någon av dem skulle ge ensam.

OWASP:s Web Security Testing Guide (WSTG) konstaterar att tekniken också är allmänt känd som black box-testning eller etisk hackning. Teamet testar utifrån, utan att känna till målets inre funktion, och beter sig som en angripare skulle göra, även om det ofta får ett eller flera giltiga användarkonton.

Två val formar varje test. Det första är utgångspunkten. Ett externt test börjar utanför nätverket med lite mer än adresserna som ingår i omfattningen; ett internt test börjar innanför, oftast med en vanlig anställds åtkomst, och försöker

klättra vidare därifrån genom att eskalera sina privilegier. Det andra är vem som vet om testet. SP 800-115 kallar öppen testning för white hat-testning: den sker med IT-personalens kännedom och samtycke. Dold testning, eller black hat-testning, sker utan att IT-personalen känner till den, men med högsta ledningens fulla kännedom och tillstånd.

SP 800-115 delar in arbetet i fyra faser och tillägger i en fotnot att detta är ett av många godtagbara sätt att gruppera det. Under planeringen kommer man överens om reglerna, ledningens godkännande dokumenteras och målen sätts; själva testningen börjar i kartläggningen. Kartläggningen samlar information om målet, skannar det och jämför fynden med sårbarhetsdatabaser, bland dem den amerikanska NVD, och med testarnas egen kunskap. Attackfasen, som vägledningen kallar kärnan i varje penetrationstest, försöker utnyttja varje tänkbar svaghet. När ett lyckat angrepp ger ny åtkomst går testarna tillbaka till kartläggningen från den nya positionen. Rapporteringen löper parallellt med de tre andra faserna och slutar med en rapport som listar de sårbarheter som hittats, bedömer risken med dem och förklarar hur de kan åtgärdas. Andra metoder delar upp samma arbete på andra sätt: Penetration Testing Execution Standard (PTES), som WSTG räknar till sina referensmetodiker, har sju faser, från förberedande avstämningar före uppdraget till rapportering.

Använd begreppet i ett beslut

Använd ”Vad är ett penetrationstest?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Konton, lösenord och behörigheter ordnade så att alla har exakt den åtkomst deras arbete kräver, och de som slutar förlorar den samma dag.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Skrev 1 000 RBAC-regler som säkrar Linux-servrar — 1,000 åtkomstregler, skrivna för att täppa till en säkerhetslucka

Skrev 1 000 RBAC-regler som säkrar Linux-servrar Hör av er →

Varför det spelar roll

En skanners rapport är en lista över möjligheter. Vissa av dem går inte att utnyttja i er miljö, och en skanner kan inte se en svaghet som ingen har beskrivit, eller en som uppstår först när två till synes ofarliga svagheter används tillsammans. Ett penetrationstest besvarar en annan fråga: vad kan en angripare faktiskt göra här, och hur långt kan hen komma? SP 800-115 nämner vad det mer kan visa: hur väl ett system står emot verkliga attackmönster, hur skicklig en angripare skulle behöva vara, vilka ytterligare motåtgärder som skulle hjälpa, och om försvararna märker attacken och reagerar på den.

Därför väger fynden tungt även hos dem som aldrig läser skannerrapporter. Ett fynd som visar att en utomstående utan konto läste kundtabellen är ett bevis, inte en sannolikhet. SP 800-115 beskriver penetrationstestning som en iterativ process där minimal åtkomst används för att få större åtkomst, och en bra rapport visar den kedjan steg för steg, så att åtgärden kan bryta den i den billigaste länken.

Samma realism gör testet dyrt och riskabelt. NIST kallar det arbetsintensivt, säger att det kräver stor expertis och understryker att system kan skadas eller slås ut under testet; erfarna testare minskar risken, men den kan aldrig elimineras helt. Mycket av det en testare gör, till exempel att angripa system för att kompromettera dem, är aktiviteter som organisationens egna policyer normalt förbjuder. Det är därför spelreglerna för testet finns, på engelska rules of engagement (ROE): ett dokument, överenskommet innan testet börjar, som ger testteamet befogenhet att utföra bestämda aktiviteter och inget utöver dem.

Det är också en teknik bland flera, inte en dom i sig. WSTG konstaterar att många team använder penetrationstestning av webbapplikationer som sin främsta teknik för säkerhetstestning, och argumenterar för att den varken bör vara den främsta eller den enda. Webbapplikationer är nästan alltid specialbyggda, så att testa dem utifrån liknar mer forskning än att hitta kända svagheter i standardprodukter, och testet kommer sent i utvecklingens livscykel, när design och kod redan ligger fast. Där källkoden inte är tillgänglig, tillägger vägledningen, är ett penetrationstest klart bättre än ingen testning alls.

Frekvensen följer av kostnaden. SP 800-115 menar att det, på grund av den höga kostnaden och den möjliga påverkan, kan räcka att testa en organisations nätverk och system en gång om året, med regelbunden och lättare skanning däremellan. Vissa standarder kräver det också uttryckligen: WSTG konstaterar att PCI DSS, kortbranschens standard för datasäkerhet, har ett eget krav på penetrationstestning som omfattar både extern och intern testning.

Så ser det ut i praktiken

Det mesta av ett penetrationstest avgörs innan testarna rör målet. Bilaga B i SP 800-115 är en mall för spelreglerna, med avsnitt om syfte och omfattning, deltagarna och tidsplanen, hur parterna kommunicerar och när testningen avbryts, vilka system som ingår och vilka som är undantagna, vilka aktiviteter som är tillåtna och förbjudna, hur testdata hanteras, hur resultaten rapporteras, och

en sida med underskrifter. En nedkortad version för ett externt test av en webbutik skulle kunna se ut så här. Den är skriven för den här artikeln, och namn och adresser kommer från de intervall som är reserverade för dokumentation.

```
SPELREGLER: externt test av shop.example.com

Syfte          Ta reda på vilka svagheter en utomstående kan utnyttja,
               och hur långt var och en leder.
Mål            203.0.113.10–203.0.113.20, ägarskap kontrollerat i WHOIS
Undantag       203.0.113.15 (betaltjänstleverantör, inte vår att testa)
               Alla tredjepartstjänster som butiken anropar
Konton         Två kundkonton och ett supportkonto
Tidsram        3–14 november, 19.00–06.00 CET, utanför försäljningstoppar
Testarnas IP   Endast 198.51.100.7 och 198.51.100.8
Tillåtet       Utnyttja en bekräftad svaghet för att visa effekten; läsa
               data som tillhör testkontona; ladda upp en märkt testfil
               som tas bort när testet avslutas
Förbjudet      Överbelastningsattacker; ändra eller radera kunddata;
               social manipulation; fysiskt intrång
Stopp          Butiken går ner, riktiga kunddata syns eller det finns
               tecken på en verklig inkräktare: stoppa, ring
               säkerhetsansvarig
Återuppta      Endast efter skriftligt besked från säkerhetsansvarig
Testdata       Känsliga; endast på testteamets bärbara datorer, raderas
               30 dagar efter slutrapporten
Rapportering   Daglig lägesrapport; slutrapport inom tio arbetsdagar
Signerat       Testteamets ledare; informationssäkerhetschef
```

Varje rad besvarar en fråga som SP 800-115 tar upp. Vägledningen säger att man innan testningen börjar ska kontrollera att varje offentlig adress på mållistan tillhör organisationen, och hänvisar till registreringsuppgifterna i WHOIS för det. Den föreslår att en webbplats i drift testas på kvällen snarare än under de mest intensiva affärstimmarna. Den ber om adresserna som testarna arbetar från, så att administratörerna kan skilja testtrafik från en verklig attack. Listan över system som inte får röras kallar den en exclude list, och den säger att reglerna ska ange kriterier för att avbryta testet och en process för att återuppta det. Den frågar också vad som ska hända om testarna hittar en verklig inkräktare: ska testningen stoppas, när kan den börja igen, och vem avgör det? Som ett minimum skriver testteamets ledare och högsta ledningen under, och intygar därmed att de förstår omfattningen och dess gränser.

Med sådana regler följer attackfasen det mönster som WSTG beskriver för SQL-injektion. En skanning av butikens söksida pekar ut en möjlig svaghet. Det första beviset är ett databasfel när ett enkelt citattecken skrivs in i sökfältet. Sedan

skickar testaren specialutformad indata som ändrar grammatiken i SQL-frågan, och räknar svagheten som bekräftad först när frågan returnerar data som den inte borde returnera. Om de uppgifterna innehöll supportkontots session skulle testaren kunna gå in som support och se sig om därifrån, och rapporten skulle visa hela vägen: ett ofiltrerat fält, en läckt session och supportens insyn i alla beställningar.

Ett sådant test kompletterar andra kontroller i stället för att ersätta dem. Artikeln om ett löpande program för säkerhetsskanning från grundarens arbete för NextMariner beskriver statisk analys, dynamisk testning mot en körande instans och skanning av beroenden, allt automatiserat, och vid sidan av automatiseringen skriftliga säkerhetsgranskningar, bland dem en hotmodell och en bedömning mot OWASP:s testguide. Sidan förklarar också varför de kombineras: skannrar hittar de kategorier av problem som någon redan har beskrivit, och en hotmodell är där problem som är specifika för en enskild plattform får ett namn.

Var det går fel

Testning utan skriftligt tillstånd. Ett muntligt ”kör bara” från en teamledare täcker inte attacker som företagets policy förbjuder, och skyddar varken testarna eller dem som beställde testet. Skriv spelreglerna först, och låt testteamets ledare och högsta ledningen skriva under dem innan teamet skickar den första trafiken.

Testning av adresser som inte är era. En mållista som kopierats från ett gammalt diagram kan innehålla adresser som nu tillhör någon annan, och på delade plattformar finns andra kunder alldeles intill er. Kontrollera att varje offentlig adress i omfattningen tillhör organisationen, som SP 800-115 begär, och för upp varje tredjepartstjänst med namn på listan över undantag.

En skanning som säljs som penetrationstest. En skannerrapport med nytt försättsblad listar möjligheter, inte bevis. Kräv belägg för varje fynd: vad testaren gjorde, vilken åtkomst det gav och vad nästa steg skulle ha varit.

Penetrationstestet som enda säkerhetstestning. Ett enskilt test ser ett urval av riskerna, vid ett tillfälle och utifrån. WSTG placerar hotmodellering i designfasen, granskning och analys av källkod under utvecklingen och penetrationstestning i testfasen som följer. Använd dem alla, och använd penetrationstestet för att bekräfta det som de tidigare kontrollerna inte kunde visa.

Ingen regel för att avbryta. Om testarna slår ut en tjänst i drift eller hittar tecken på en verklig inkräktare, och ingen har kommit överens om vem som avbryter testet och vem som startar det igen, får folk improvisera under press. Skriv in kriterier för avbrott, en ringlista och en process för att återuppta testet i spelreglerna.

Resultaten behandlas som vanliga data. En rapport från ett penetrationstest är en karta över vad en motståndare skulle kunna utnyttja, och SP 800-115 säger att testresultat ska behandlas som känsliga. Kom överens innan testet börjar om hur fynd samlas in, skickas, förvaras och förstörs, och begränsa vilka som får hela rapporten.

Fynd stängs utan nytt test. En åtgärd kan vara ofullständig, eller hamna på ett annat ställe än svagheten. WSTG kallar testning som försöker utnyttja sårbarheter som hittats i tidigare granskningar för fokuserad penetrationstestning, och konstaterar att den visar om specifika svagheter faktiskt är åtgärdade i koden som är i drift. Kör det ursprungliga angreppet igen mot varje åtgärd innan fyndet stängs.

Förväntningen att ett dolt test hittar allt. Enligt SP 800-115 undersöker dold testning vilken skada en motståndare kan orsaka; den testar inte varje skyddsåtgärd och hittar inte varje sårbarhet, och den tar sig oftast in genom de mest grundläggande svagheterna. Välj ett öppet test när målet är täckning, och ett dolt när målet är att ta reda på om försvararna märker något.

Läs mer

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment — NIST:s vägledning för att planera och genomföra säkerhetstester, med de fyra faserna i ett penetrationstest och en mall för spelreglerna.
- OWASP Web Security Testing Guide v4.2: Introduction — var penetrationstestning hör hemma bredvid granskning och källkodsanalys, och varför det inte bör vara den enda tekniken.
- OWASP WSTG v4.2: Penetration Testing Methodologies — en kort översikt över PTES, PCI DSS-vägledningen, PTF, NIST SP 800-115 och OSSTMM.
- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations — NIST:s katalog över åtgärder för säkerhet och integritetsskydd, där åtgärd CA-8 täcker penetrationstestning och spelreglerna för den.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är ett penetrationstest?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/penetration-test/