Engineer

Penetrationstest

et godkendt angreb, der viser, om sårbarheder kan udnyttes

Hvad det er

En penetrationstest, i daglig tale ofte kaldet en pentest, er sikkerhedstest, hvor testerne efterligner virkelige angreb for at finde veje uden om sikkerhedsfunktionerne i en applikation, et system eller et netværk. NIST's tekniske vejledning i test og vurdering af informationssikkerhed, SP 800-115, beskriver, at det ofte betyder rigtige angreb på rigtige systemer og data med de værktøjer og teknikker, som angribere selv bruger. NIST's katalog over sikkerheds- og privatlivskontroller, SP 800-53 Rev. 5, tilføjer i sin kortere definition, at testerne typisk arbejder inden for bestemte rammer, og det er dét, der skiller en test fra et angreb: den er godkendt, afgrænset og aftalt skriftligt, før den begynder.

Det, der adskiller den fra anden sikkerhedstest, er målet. En sårbarhedsscanner sammenligner det, den ser, med beskrivelser af kendte fejl og melder, hvad der måske findes. En tester forsøger at udnytte fejlen. SP 800-115 formulerer forskellen klart: scannere undersøger kun, om en sårbarhed muligvis findes, mens angrebsfasen i en penetrationstest udnytter den for at bekræfte, at den er der. De fleste test leder også efter kombinationer: svagheder på ét eller flere systemer, som tilsammen giver mere adgang, end hver af dem ville give alene.

OWASP's Web Security Testing Guide (WSTG) bemærker, at teknikken også er almindeligt kendt som black box-test eller etisk hacking. Teamet tester udefra uden at kende målets indre opbygning og opfører sig, som en angriber ville, selv om det ofte får en eller flere gyldige brugerkonti at arbejde med.

To valg former enhver test. Det første er udgangspunktet. En ekstern test begynder uden for netværket med næppe andet end de adresser, der er omfattet; en intern test begynder indenfor, som regel med en almindelig medarbejders adgang, og forsøger at arbejde sig opad derfra ved at skaffe sig

flere privilegier. Det andet er, hvem der er indviet. SP 800-115 kalder åben test for white hat-test: den foregår med it-personalets viden og samtykke. Skjult test, eller black hat-test, foregår, uden at it-personalet ved det, men med den øverste ledelses fulde viden og tilladelse.

SP 800-115 deler arbejdet i fire faser og nævner i en fodnote, at det kun er én af mange acceptable inddelinger. I planlægningen aftales reglerne, ledelsens godkendelse dokumenteres, og målene fastlægges; selve testen begynder først i afdækningen. Afdækningen indsamler oplysninger om målet, scanner det og sammenholder fundene med sårbarhedsdatabaser som den amerikanske National Vulnerability Database og med testernes egen viden. Angrebsfasen, som vejledningen kalder kernen i enhver penetrationstest, forsøger at udnytte hver mulig fejl. Når et angreb åbner ny adgang, går testerne tilbage til afdækningen fra den nye position. Rapporteringen løber sideløbende med de tre andre faser og ender med en rapport, der oplister de fundne sårbarheder, vurderer risikoen ved dem og beskriver, hvordan de udbedres. Andre metoder deler det samme arbejde anderledes op: Penetration Testing Execution Standard (PTES), som WSTG nævner blandt sine referencemetoder, har syv faser, fra de indledende aftaler til rapporteringen.

Brug begrebet i en beslutning

Brug »Hvad er en penetrationstest?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Konti, adgangskoder og rettigheder sat op, så folk har præcis den adgang, jobbet kræver, og fratrådte mister den samme dag.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har skrevet 1.000 RBAC-regler til Linux-servere — 1,000 adgangsregler skrevet for at lukke et sikkerhedshul

Har skrevet 1.000 RBAC-regler til Linux-servere Kontakt os →

Hvorfor det betyder noget

En scannerrapport er en liste over muligheder. Nogle af dem kan ikke udnyttes i jeres opsætning, og en scanner kan ikke se en fejl, som ingen har beskrevet, eller en, der kun opstår, når to uskyldigt udseende svagheder bruges sammen. En penetrationstest besvarer et andet spørgsmål: hvad kan en angriber faktisk gøre her, og hvor langt kan vedkommende komme? SP 800-115 nævner, hvad testen ellers kan vise: hvor godt et system modstår virkelige angrebsmønstre, hvor dygtig en angriber skal være, hvilke yderligere modforanstaltninger der vil hjælpe, og om forsvarerne opdager angrebet og reagerer på det.

Derfor vejer fundene tungt hos folk, der aldrig læser output fra en scanner. Et fund, der viser, at en udefrakommende uden konto kunne læse kundetabellen, er et bevis og ikke en sandsynlighed. SP 800-115 beskriver penetrationstest som en iterativ proces, der bruger minimal adgang til at skaffe sig mere, og en god rapport viser den kæde trin for trin, så rettelsen kan bryde den ved det billigste led.

Den samme realisme gør testen dyr og risikabel. NIST kalder den arbejdskrævende, siger, at den kræver stor ekspertise, og advarer om, at systemer kan blive beskadiget eller sat ud af drift under testen; erfarne testere mindsker risikoen, men den kan aldrig fjernes helt. Meget af det, en tester gør, for eksempel at angribe systemer for at kompromittere dem, er handlinger, som organisationens egne politikker normalt forbyder. Derfor har testen spilleregler, på engelsk rules of engagement (ROE): et dokument, der aftales, før testen begynder, og som giver testteamet bemyndigelse til bestemte handlinger og intet ud over dem.

Den er også én teknik blandt flere og ikke en dom i sig selv. WSTG bemærker, at mange teams bruger penetrationstest af webapplikationer som deres primære teknik til sikkerhedstest, og argumenterer for, at den hverken bør være den primære eller den eneste. Webapplikationer er næsten altid skræddersyede, så at teste dem udefra ligner mere forskning end jagt på kendte fejl i standardprodukter, og testen kommer sent i udviklingsforløbet, når design og kode allerede ligger fast. Hvor kildekoden ikke er tilgængelig, tilføjer vejledningen, er en penetrationstest klart bedre end slet ingen test.

Hyppigheden følger af prisen. SP 800-115 foreslår, at det på grund af de høje omkostninger og den mulige påvirkning kan være nok at teste en organisations netværk og systemer én gang om året, med regelmæssig og lettere scanning ind imellem. Nogle standarder kræver den også direkte: WSTG nævner, at PCI DSS, betalingskortbranchens standard for datasikkerhed, har sit eget krav om penetrationstest, som omfatter både ekstern og intern test.

Sådan ser det ud i praksis

Det meste af en penetrationstest bliver afgjort, før testerne rører målet. Bilag B i SP 800-115 er en skabelon til spillereglerne med afsnit om formål og omfang, de involverede personer og tidsplanen, hvordan parterne kommunikerer, og hvornår testen standses, hvilke systemer der er med, og hvilke der er undtaget, hvilke handlinger der er tilladt og forbudt, hvordan testdata håndteres, hvordan

resultaterne rapporteres, og en side med underskrifter. En forkortet udgave til en ekstern test af en webshop kunne se sådan ud. Den er skrevet til denne artikel, og navne og adresser stammer fra de intervaller, der er reserveret til dokumentation.

```
SPILLEREGLER: ekstern test af shop.example.com

Formål          Find ud af, hvilke fejl en udefrakommende kan udnytte, og
                hvor langt hver af dem fører.
Mål             203.0.113.10 til 203.0.113.20, ejerskab tjekket i WHOIS
Undtaget        203.0.113.15 (betalingsudbyder, ikke vores at teste)
                Alle tredjepartstjenester, som shoppen kalder
Konti           To kundekonti og én supportkonto
Tidsrum         3. til 14. november, kl. 19.00 til 06.00 CET, uden for de
                travleste handelstider
Testernes IP    Kun 198.51.100.7 og 198.51.100.8
Tilladt         At udnytte en bekræftet fejl for at vise følgerne; at
                læse data, der tilhører testkontiene; at uploade én
                mærket testfil, som fjernes til sidst
Forbudt         Overbelastningsangreb; ændring eller sletning af
                kundedata; social engineering; fysisk adgang
Stop            Nedbrud i den kørende shop, rigtige kundedata i syne eller
                tegn på en rigtig indtrænger: stop og ring til den
                sikkerhedsansvarlige
Genoptag        Kun efter skriftlig besked fra den sikkerhedsansvarlige
Testdata        Fortrolige; ligger på testteamets bærbare og slettes 30
                dage efter den endelige rapport
Rapportering    Daglig statusnote; endelig rapport inden ti arbejdsdage
Underskrevet    Testteamets leder; informationssikkerhedschefen
```

Hvert punkt besvarer et spørgsmål, som SP 800-115 rejser. Vejledningen siger, at man skal kontrollere, at hver offentlig adresse på mållisten tilhører organisationen, før testen begynder, og peger på registreringsdata i WHOIS til formålet. Den foreslår at teste et site i drift om aftenen frem for i de travleste forretningstimer. Den beder om de adresser, testerne arbejder fra, så administratorer kan skelne testtrafik fra et rigtigt angreb. Den kalder listen over systemer, der ikke må røres, for en exclude list, altså en undtagelsesliste, og siger, at spillereglerne skal rumme kriterier for at standse testen og en procedure for at genoptage den. Den spørger også, hvad der skal ske, hvis testerne støder på en rigtig indtrænger: skal testen stoppe, hvornår må den fortsætte, og på hvis bemyndigelse? Som minimum skriver testteamets leder og den øverste ledelse under på, at de forstår omfanget og dets grænser.

Med spilleregler som disse følger angrebsfasen det mønster, som WSTG beskriver for SQL-injection. En scanning af shoppens søgeside finder tegn på en mulig fejl. Det første bevis er en databasefejl, når der skrives et enkelt anførselstegn i søgefeltet. Testeren sender derefter tilrettelagt input, der ændrer grammatikken i SQL-forespørgslen, og regner kun fejlen for bekræftet, når den returnerer data, den ikke burde. Hvis de data rummede supportkontoens session, ville testeren kunne gå ind som support og se sig om igen derfra, og rapporten ville vise hele vejen: ét ufiltreret felt, én lækket session, ét supportoverblik over alle ordrer.

En test som denne står ved siden af andre kontroller, ikke i stedet for dem. Artiklen om et løbende sikkerhedsscanningsprogram fra grundlæggerens arbejde for NextMariner beskriver statisk analyse, dynamisk test mod en kørende instans og tjek af afhængigheder, der kører automatisk, sammen med skriftlige sikkerhedsgennemgange, heriblandt en trusselsmodel og en vurdering op mod OWASP's testguide. Siden giver også grunden til den kombination: scannere finder de typer problemer, som nogen allerede har beskrevet, og det er i en trusselsmodel, at de problemer, der er særlige for netop én platform, får et navn.

Hvor det går galt

Test uden skriftlig tilladelse. Et mundtligt »bare gå i gang« fra en teamleder dækker ikke angreb, som virksomhedens politik forbyder, og det beskytter hverken testerne eller dem, der bestilte testen. Skriv spillereglerne først, og få testteamets leder og den øverste ledelse til at underskrive dem, før der sendes nogen trafik.

Test af adresser, der ikke er jeres. En målliste, der er kopieret fra et gammelt diagram, kan rumme adresser, som i dag tilhører nogen andre, og på delte platforme står andre kunder lige ved siden af jer. Kontrollér, at hver offentlig adresse i omfanget tilhører organisationen, som SP 800-115 anbefaler, og sæt hver tredjepartstjeneste på undtagelseslisten ved navn.

En scanning solgt som penetrationstest. En scannerrapport med en ny forside oplister muligheder, ikke beviser. Bed om dokumentation for udnyttelse ved hvert fund: hvad testeren gjorde, hvilken adgang det gav, og hvad det næste skridt ville have været.

Penetrationstesten som eneste sikkerhedstest. En enkelt test ser et udsnit af risiciene, på ét tidspunkt og udefra. WSTG placerer trusselsmodellering i designfasen, kodegennemgang og kildekodeanalyse under udviklingen og penetrationstest i testfasen bagefter. Brug dem alle, og lad penetrationstesten bekræfte det, de tidligere kontroller ikke kunne.

Ingen regel for at stoppe. Hvis testerne lægger en kørende tjeneste ned eller finder tegn på en rigtig indtrænger, og ingen har aftalt, hvem der standser testen, og hvem der sætter den i gang igen, improviserer folk under pres. Skriv stopkriterier, en telefonkæde og en procedure for genoptagelse ind i spillereglerne.

Resultaterne behandles som almindelige data. En rapport fra en penetrationstest er et kort over, hvad en modstander kan udnytte, og SP 800-115 siger, at testresultater bør behandles som fortrolige. Aftal, hvordan fund indsamles, sendes, opbevares og destrueres, før testen begynder, og begræns, hvem der får den fulde rapport.

Fund lukkes uden en gentest. En rettelse kan være delvis eller ramme et andet sted end fejlen. WSTG kalder test, der forsøger at udnytte sårbarheder fundet i tidligere gennemgange, for fokuseret penetrationstest og bemærker, at den viser, om bestemte fejl faktisk er rettet i den kode, der kører. Kør det oprindelige angreb igen mod hver rettelse, før fundet lukkes.

En forventning om, at en skjult test finder alt. Ifølge SP 800-115 undersøger skjult test, hvor stor skade en modstander kan gøre; den tester ikke hver kontrol og finder ikke hver sårbarhed, og den kommer som regel ind gennem de mest basale svagheder. Vælg en åben test, når målet er dækning, og en skjult, når målet er at finde ud af, om forsvarerne opdager angrebet.

Læs mere

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment — NIST's vejledning i at planlægge og udføre sikkerhedstest, med de fire faser i en penetrationstest og en skabelon til spillereglerne.
- OWASP Web Security Testing Guide v4.2: Introduction — hvor penetrationstest passer ind ved siden af gennemgang og kildekodeanalyse, og hvorfor den ikke bør være den eneste teknik.
- OWASP WSTG v4.2: Penetration Testing Methodologies — et kort overblik over PTES, vejledningen fra PCI DSS, PTF, NIST SP 800-115 og OSSTMM.

- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations — NIST's katalog over sikkerheds- og privatlivskontroller, hvor kontrol CA-8 dækker penetrationstest og spillereglerne for den.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er en penetrationstest?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/penetration-test/