Engineer

Penetrasjonstest

🔓 et godkjent angrep som viser om sårbarheter kan utnyttes

Hva det er

En penetrasjonstest, ofte forkortet til *pentest*, er sikkerhetstesting der testerne etterligner virkelige angrep for å finne veier rundt sikkerhetsmekanismene i en applikasjon, et system eller et nettverk. NISTs tekniske veiledning for testing og vurdering av informasjonssikkerhet, SP 800-115, påpeker at dette ofte betyr å gjennomføre ekte angrep mot ekte systemer og data, med de verktøyene og teknikkene angripere selv bruker. Den kortere definisjonen i SP 800-53 Rev. 5, NISTs katalog over tiltak for sikkerhet og personvern, legger til at de som tester, vanligvis arbeider innenfor bestemte rammer, og det er nettopp det som skiller en test fra et angrep: testen er godkjent, avgrenset og skriftlig avtalt før den begynner.

Det som skiller den fra annen sikkerhetstesting, er målet. En sårbarhetsskanner sammenligner det den ser, med beskrivelser av kjente svakheter og rapporterer hva som kan finnes der. Den som utfører en penetrasjonstest, prøver å utnytte svakheten. SP 800-115 sier forskjellen rett ut: skannere sjekker bare om en sårbarhet kan finnes, mens angrepsfasen i en penetrasjonstest utnytter den for å bekrefte at den faktisk finnes. De fleste tester ser også etter kombinasjoner, altså svakheter i ett eller flere systemer som sammen gir mer tilgang enn hver av dem ville gitt alene.

OWASPs *Web Security Testing Guide* (WSTG) påpeker at teknikken også er kjent som *black-box testing* eller etisk hacking. Teamet tester utenfra, uten å kjenne målets indre virkemåte, og opptrer slik en angriper ville gjort, selv om det ofte får én eller flere gyldige brukerkontoer.

To valg former hver test. Det første er utgangspunktet. En ekstern test starter utenfor nettverket med lite mer enn adressene som inngår i omfanget; en intern test starter innenfor, vanligvis med tilgangen til en vanlig ansatt, og prøver å

klatre videre derfra gjennom eskalering av privilegier. Det andre er hvem som vet om testen. SP 800-115 kaller åpen testing for *white hat*-testing: den skjer med IT-personalets kjennskap og samtykke. Skjult testing, eller *black hat*-testing, skjer uten at IT-personalet vet om det, men med full kjennskap og tillatelse fra toppledelsen.

SP 800-115 deler arbeidet i fire faser og legger til i en fotnote at dette er én av mange akseptable måter å gruppere det på. I planleggingen avtales reglene, ledelsens godkjenning dokumenteres og målene fastsettes; selve testingen begynner i kartleggingen. Kartleggingen samler informasjon om målet, skanner det og sammenligner funnene med sårbarhetsdatabaser, blant dem den amerikanske NVD, og med testernes egen kunnskap. Angrepsfasen, som veiledningen kaller kjernen i enhver penetrasjonstest, prøver å utnytte hver mulig svakhet. Når en vellykket utnyttelse gir ny tilgang, går testerne tilbake til kartleggingen fra den nye posisjonen. Rapporteringen går parallelt med de tre andre fasene og ender med en rapport som lister opp sårbarhetene som ble funnet, vurderer risikoen ved dem og forklarer hvordan de kan utbedres. Andre metoder deler det samme arbeidet annerledes: *Penetration Testing Execution Standard* (PTES), som WSTG regner blant sine referansemetodikker, har sju faser, fra avklaringene før oppdraget til rapporteringen.

Bruk begrepet i en beslutning

Bruk «Hva er en penetrasjonstest?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Kontoer, passord og tilganger ordnet slik at folk har nøyaktig den tilgangen jobben krever, og de som slutter, mister den samme dag.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Skrev 1 000 RBAC-regler for å sikre Linux-servere — 1,000 tilgangsregler skrevet for å tette et sikkerhetshull

Skrev 1 000 RBAC-regler for å sikre Linux-servere Ta kontakt →

Hvorfor det er viktig

En skanners rapport er en liste over muligheter. Noen av dem lar seg ikke utnytte i ditt oppsett, og en skanner kan ikke se en svakhet som ingen har beskrevet, eller en som bare oppstår når to tilsynelatende harmløse svakheter brukes sammen. En penetrasjonstest svarer på et annet spørsmål: hva kan en angriper faktisk gjøre her, og hvor langt kan vedkommende komme? SP 800-115 nevner hva den ellers kan vise: hvor godt et system tåler reelle angrepsmønstre, hvor dyktig en angriper må være, hvilke ytterligere mottiltak som vil hjelpe, og om forsvarerne oppdager angrepet og reagerer på det.

Derfor veier funnene tungt også hos folk som aldri leser rapporter fra skannere. Et funn som viser at en utenforstående uten konto leste kundetabellen, er et bevis, ikke en sannsynlighet. SP 800-115 beskriver penetrasjonstesting som en iterativ prosess der minimal tilgang brukes til å skaffe større tilgang, og en god rapport viser den kjeden steg for steg, slik at rettelsen kan bryte den i det billigste leddet.

Den samme realismen gjør testen kostbar og risikabel. NIST kaller den arbeidskrevende, sier at den krever stor ekspertise, og advarer om at systemer kan bli skadet eller satt ut av spill under testen; erfarne testere reduserer den risikoen, men den kan aldri fjernes helt. Mye av det en tester gjør, for eksempel å angripe systemer for å kompromittere dem, er aktiviteter som organisasjonens egne retningslinjer vanligvis forbyr. Det er derfor spillereglene for testen finnes, på engelsk *rules of engagement* (ROE): et dokument, avtalt før testen begynner, som gir testteamet fullmakt til å utføre bestemte aktiviteter og ingenting utover dem.

Den er også én teknikk blant flere, ikke en dom i seg selv. WSTG observerer at mange team bruker penetrasjonstesting av webapplikasjoner som sin primære teknikk for sikkerhetstesting, og argumenterer for at den verken bør være den primære eller den eneste. Webapplikasjoner er nesten alltid skreddersydde, så å teste dem utenfra ligner mer på forskning enn på å finne kjente svakheter i standardprodukter, og testen kommer sent i utviklingsløpet, når design og kode allerede ligger fast. Der kildekoden ikke er tilgjengelig, legger veiledningen til, er en penetrasjonstest klart bedre enn ingen testing i det hele tatt.

Hyppigheten følger av kostnaden. SP 800-115 antyder at det, på grunn av den høye kostnaden og den mulige påvirkningen, kan være tilstrekkelig å teste en organisasjons nettverk og systemer én gang i året, med regelmessig og lettere skanning imellom. Noen standarder krever det også direkte: WSTG påpeker at PCI DSS, betalingskortbransjens standard for datasikkerhet, definerer sitt eget krav til penetrasjonstesting, som omfatter både ekstern og intern testing.

Slik ser det ut i praksis

Det meste av en penetrasjonstest avgjøres før testerne rører målet. Vedlegg B i SP 800-115 er en mal for spillereglene, med avsnitt om formål og omfang, deltakerne og tidsplanen, hvordan partene kommuniserer og når testingen stanses, hvilke systemer som er med og hvilke som er unntatt, hvilke aktiviteter som er tillatt og forbudt, hvordan testdata håndteres, hvordan resultatene

rapporteres, og en side med underskrifter. En nedkortet versjon for en ekstern test av en nettbutikk kunne sett slik ut. Den er skrevet for denne artikkelen, og navn og adresser er hentet fra områdene som er reservert for dokumentasjon.

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

Formål         Finne hvilke svakheter en utenforstående kan utnytte, og
               hvor langt hver av dem fører.
Mål            203.0.113.10–203.0.113.20, eierskap kontrollert i WHOIS
Unntatt        203.0.113.15 (betalingsleverandør, ikke vår å teste)
               Alle tredjepartstjenester butikken kaller
Kontoer        To kundekontoer og én supportkonto
Tidsrom        3.–14. november, 19.00–06.00 CET, utenom salgstoppene
Testernes IP   Bare 198.51.100.7 og 198.51.100.8
Tillatt        Utnytte en bekreftet svakhet for å vise virkningen; lese
               data som tilhører testkontoene; laste opp én merket testfil
               som fjernes ved avslutning
Forbudt        Tjenestenekt; endre eller slette kundedata; sosial
               manipulering; fysisk inntrenging
Stans          Butikken går ned, ekte kundedata blir synlige, eller det
               er tegn på en ekte inntrenger: stopp, ring
               sikkerhetsansvarlig
Gjenoppta      Bare etter skriftlig beskjed fra sikkerhetsansvarlig
Testdata       Sensitive; bare på testteamets bærbare, slettes 30 dager
               etter sluttrapporten
Rapportering   Daglig statusnotat; sluttrapport innen ti arbeidsdager
Signert        Leder for testteamet; informasjonssikkerhetssjef
```

Hver linje svarer på et spørsmål som SP 800-115 reiser. Veiledningen sier at man før testingen begynner skal kontrollere at hver offentlige adresse på mållisten tilhører organisasjonen, og viser til registreringsdata i WHOIS for det. Den foreslår å teste et nettsted i drift om kvelden heller enn i de travleste forretningstimene. Den ber om adressene testerne arbeider fra, slik at administratorene kan skille testtrafikk fra et ekte angrep. Listen over systemer som ikke skal berøres, kaller den en *exclude list*, og den sier at reglene bør angi kriterier for å stanse testen og en prosess for å gjenoppta den. Den spør også hva som skal skje hvis testerne finner en faktisk inntrenger: skal testingen stoppe, når kan den starte igjen, og hvem avgjør det? Som et minimum signerer lederen for testteamet og toppledelsen, og bekrefter dermed at de forstår omfanget og grensene for det.

Under slike regler følger angrepsfasen mønsteret WSTG beskriver for SQL-injeksjon. En skanning av søkesiden i butikken avdekker en mulig svakhet. Det første beviset er en databasefeil når et enkelt anførselstegn skrives inn i

søkefeltet. Deretter sender testeren spesiallaget inndata som endrer grammatikken i spørringen, og regner svakheten som bekreftet først når spørringen returnerer data den ikke burde. Hvis de dataene inkluderte økten til supportkontoen, kunne testeren gå inn som support, se seg om derfra, og rapporten ville vise hele veien: ett ufiltrert felt, én lekket økt, og supportens innsyn i alle bestillinger.

En slik test kommer i tillegg til andre kontroller, ikke i stedet for dem. Artikkelen om et løpende program for sikkerhetsskanning fra grunnleggerens arbeid for NextMariner beskriver statisk analyse, dynamisk testing mot en kjørende instans og kontroll av avhengigheter, alt automatisert, og ved siden av automatiseringen skriftlige sikkerhetsrevisjoner, blant annet en trusselmodell og en vurdering opp mot OWASP-testveiledningen. Siden gir også begrunnelsen for den kombinasjonen: skannere finner de problemklassene noen allerede har beskrevet, og en trusselmodell er der problemene som er spesifikke for én plattform, får et navn.

Hvor det går galt

Testing uten skriftlig fullmakt. Et muntlig «bare kjør på» fra en teamleder dekker ikke angrep som selskapets retningslinjer forbyr, og beskytter verken testerne eller dem som bestilte testen. Skriv spillereglene først, og la lederen for testteamet og toppledelsen signere dem før testteamet sender den første trafikken.

Testing av adresser som ikke er dine. En målliste kopiert fra et gammelt diagram kan inneholde adresser som nå tilhører noen andre, og på delte plattformer står andre kunder rett ved siden av deg. Kontroller at hver offentlige adresse i omfanget tilhører organisasjonen, slik SP 800-115 ber om, og før opp hver tredjepartstjeneste ved navn på listen over unntak.

En skanning solgt som penetrasjonstest. En skannerrapport med ny forside lister opp muligheter, ikke bevis. Be om bevis på utnyttelse for hvert funn: hva testeren gjorde, hvilken tilgang det ga, og hva det neste steget ville vært.

Penetrasjonstesten som eneste sikkerhetstesting. En enkelt test ser et utvalg av risikoene, på ett tidspunkt og utenfra. WSTG plasserer trusselmodellering i designfasen, gjennomgang og analyse av kildekode under utviklingen

og penetrasjonstesting i testfasen som følger. Bruk alle sammen, og bruk penetrasjonstesten til å bekrefte det de tidligere kontrollene ikke kunne avdekke.

Ingen regel for å stanse. Hvis testerne tar ned en tjeneste i drift eller finner tegn på en ekte inntrenger, og ingen har avtalt hvem som stanser testen og hvem som starter den igjen, må folk improvisere under press. Skriv kriterier for stans, en ringeliste og en prosess for å gjenoppta testen inn i spillereglene.

Resultatene behandlet som vanlige data. En rapport fra en penetrasjonstest er et kart over hva en motstander kan utnytte, og SP 800-115 sier at testresultater bør behandles som sensitive. Avtal før testen begynner hvordan funn samles inn, overføres, oppbevares og slettes, og begrens hvem som får hele rapporten.

Funn lukket uten ny test. En rettelse kan være delvis, eller havne et annet sted enn svakheten. WSTG kaller testing som prøver å utnytte sårbarheter funnet i tidligere gjennomganger, for fokusert penetrasjonstesting, og påpeker at den viser om bestemte svakheter faktisk er rettet i koden som er i drift. Kjør den opprinnelige utnyttelsen på nytt mot hver rettelse før funnet lukkes.

Forventningen om at en skjult test finner alt. Ifølge SP 800-115 undersøker skjult testing hvilken skade en motstander kan gjøre; den tester ikke alle sikkerhetstiltak og finner ikke alle sårbarheter, og den kommer som regel inn gjennom de mest grunnleggende svakhetene. Velg en åpen test når målet er dekning, og en skjult når målet er å finne ut om forsvarerne merker noe.

Les mer

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment — NISTs veiledning for å planlegge og gjennomføre sikkerhetstester, med de fire fasene i en penetrasjonstest og en mal for spillereglene.
- OWASP Web Security Testing Guide v4.2: Introduction — hvor penetrasjonstesting hører hjemme ved siden av gjennomgang og kildekodeanalyse, og hvorfor den ikke bør være den eneste teknikken.
- OWASP WSTG v4.2: Penetration Testing Methodologies — en kort oversikt over PTES, PCI DSS-veiledningen, PTF, NIST SP 800-115 og OSSTMM.

- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations — NISTs katalog over tiltak for sikkerhet og personvern, der tiltak CA-8 dekker penetrasjonstesting og spillereglene for den.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er en penetrasjonstest?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/penetration-test/