IngramMicroCyberSecurity

Penetration testing

Tjänstebeskrivning

Version: 3.0

Innehållet

1. Inledning 2
2. Tjänstens syfte 2
3. Tjänstens omfattning 2
4. Tillvägagångssätt 3
5. Förutsättningar 4
6. Rapport 4
7. Leveransvillkor 4
8. Antaganden 5
9. Bilaga - A – vanliga frågor 6
10. Bilaga - B – Verktyg 7

1. Inledning

Penetrationstest (PT) är processen att utvärdera den nuvarande säkerhetsstatusen för ett system eller nätverk för att hitta sårbarheter som en angripare kan utnyttja för att få obehörig åtkomst till system och information. Denna process innefattar identifiering av säkerhetsbrister som kan uppstå på grund av felaktig konfigurationer av system eller applikation samt kända eller okända sårbarheter i hårdvaru- eller mjukvarusystem.

2. Tjänstens syfte

Syftet med ett penetrationstest är:

- Validera konfigurationer av IT-resurser och skapa en lista över kända sårbarheter i systemet eller applikationer och åtgärda dem innan de utnyttjas av illvilliga angripare.
- Simulera en riktig attack för att testa hållbarheten i organisationens befintliga försvarsmekanismer och motåtgärder.

3. Tjänstens omfattning

Tjänstens omfattar IT-resurser som inkluderar brandväggar, routrar, VPN, IDS/IPS, webbservrar, programservrar, databasservrar etc.

Penetrationstest ger inblick i organisationers nuvarande säkerhetsstatus och upptäcker möjligheten av att penetrera organisationens system och testa effektiviteten av den säkerhetsmekanismerna. Vi utför våra penetrationstester i två varianter:

- **External Basic Penetration Testing** (Extern penetrationstest)**:** Utförs på distans av vårt SOC-team. Målet är att identifiera och klassificera svagheterna samt penetrera en organisations IT-resurser som är publicerade mot Internet som webbservrar, nätverksgateways, VPN, e-postservrar och brandväggar.
- **Internal Basic Penetration Testing** (Intern penetrationstest)**:** Utförs inifrån organisationens interna nätverk, vanligtvis för att identifiera och klassificera hot och brister i det interna nätverket som utgörs av någon som redan har tillgång till organisationens nätverk, såsom en anställd, entreprenör eller gäst. Detta hjälper också en organisation att fastställa dess överensstämmelse med globala eller lokala policyer, standarder och förfaranden när det gäller informationssäkerhet, dataskydd och segmentering av nätverk.

I stället för att bara lista alla enskilda sårbarheter i varje IT-resurs, är vår metod att hitta systembrister i organisationen som leder till problem. Vi använder ofta en testmetodik i vårt arbete för att fokusera på problemens grundorsaker och prioriterar de viktigaste åtgärderna.

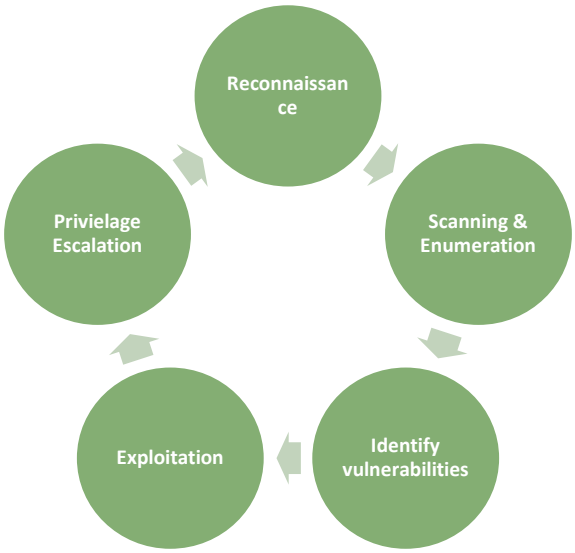
När vi utför penetrationstestet, begränsar vi oss till relativt säkra kontroller som är utformade för att begränsa eventuellt negativa effekter på organisationens produktionsmiljöer.

4. Tillvägagångssätt

För att leverera tjänsten penetrationstest kommer Ingram Micro att använda en kombination av automatiserade och manuella scanningsmetoder. I utförandet kommer används både kommersiella och kostnadsfria verktyg samt anpassade skript och applikationer som utvecklats av Ingram Micro.

Basic Penetration Testning processen består av följande steg:

- **Reconnaissance** (Rekognoscering) **:** samla in uppgifter eller information om målorganisationen. Uppgifterna samlas in för att bättre kunna planera attacken. Information som används i detta steg omfattar IP-adressintervaller, publika e-postadresser, webbadresser etc.
- **Scanning & Enumeration** (Skanning & Listning)**:** samla in mer information om system, applikationer och tjänster i organisationens nätverk. Information såsom typ och version av operativsystem, användarkonton, e-postadresser, serviceversion och utgivningsnummer är också insamlade.
- **Identify Vulnerabilities** (Identifiera sårbarheter)**:** baserat på informationen som samlats in i de två föregående faserna kommer vi att identifiera säkerhetsluckor i tjänster eller applikationer som körs i organisationens nätverk.
- **Exploitation** (Utnyttjande)**:** Använda redan tillgänglig eller skapa anpassade kod som kan användas för att utnyttja identifierade sårbarheter för att få tillgång till det system som testen utför mot.
- **Privilege Escalation** (Utökning av accessprivilegium)**:** I fall en säkerhetsbrist tillåter åtkomst endast på låg nivå, till exempel normal användaråtkomst med begränsade privilegier, kommer vi i detta steg att försöka få full administrativ åtkomst till systemet.



5. Förutsättningar

För att säkerställa ett lyckat och smidigt genomförande av tjänsten *Basic Penetration Test* måste vissa förutsättningar vara på plats enligt följande:

- **External Penetration Testning** (Penetrationstest av externa resurser)**:** IP-adresser för de resurser som skall inkluderas i testet.
- **Internal Penetration Testning** (Penetrationstest av interna resurser)**:** En virtuell maskin (VM) för att installera våra säkerhets verktyg som kommer att användas för att utföra skanningen och för att samla in data. Den virtuella datorn ska ha följande specifikation:
    - **Maskinvarukrav:** 8 GB RAM, 250 GB lagringsutrymme, 4 Core-processor.
    - **Behörigheter:** lokal administratörsbehörighet på den virtuella datorn.
    - **Nätverksåtkomst:** : VMen bör placeras i ett VLAN som har access till alla nätverkssegment och VLAN som ska vara med i testet. Dessutom bör den virtuella datorn vara tillgänglig från Internet så att Ingram Micros SOC-team kan komma åt via VPN eller fjärrskrivbord för att underlätta fjärrhantering och utförande av tjänsten.
    - **Programvara:** En image kommer att distribueras och skall installeras på ovan nämnda VM. Så snart imagen har installerats kommer den att be om aktiveringskod som kommer att tillhandahållas av Ingram Micros SOC-team. Som tillägg behöver VM stödja Nested Virtualization för att vi ska kunna använda andra virtuella image.

6. Rapport

Efter avslutat penetrationstest kommer en detaljerad rapport att skickas till beställaren som inkluderar följande:

- **Executive Summary** (Sammanfattning)**:** Sammanfattning av testresultatet med en bedömning samt en kortfattad redogörelse av hotbilden som organisationen utsätts för ur ett affärsperspektiv.
- **Findings** (Resultaten)**:** En detaljerad teknisk beskrivning av testresultatet med bevisningar.
- **Conclusions & Recommendations** (Slutsats & rekommendationer)**:** Det här avsnittet innehåller en sammanfattning av de problem som hittats under testet med eventuella rekommendationer för åtgärder.

7. Leveransvillkor

Tjänsten Basic Penetration Testing på ca 10 IT-resurser kan levereras inom 10 arbetsdagar efter angivet startdatum.
Testet påbörjas vid, av återförsäljare angivet, datum.

8. Antaganden

- Basic Penetration Testing kommer att utföras från Ingram Micro i Tyskland.
- Kunden kommer att tillhandahålla alla nödvändig information, i detta fall IP-adressintervall, VM och tillgång till VM för intern Basic Penetration Testing. Men för extern Basic Penetration Testing behövs enbart de publika IP-adresserna.
- Tester som genomförs utanför normala kontorstider kan medföra en ökad kostnad som måste godkännas av kunden i förväg. Automatiserade tester kan utföras utanför normala kontorstider om testen kan schemaläggas i förväg.
- Kunden är ansvarig för att anordna nödvändiga möten med relevanta intressenter för att framgångsrikt utföra tjänsten.
- Kunden är ansvarig för att ge feedback och/eller signera slutleveransen inom fem arbetsdagar efter att rapporten gjorts tillgänglig av Ingram Micro.
- Kunden ansvarar för att genomföra nödvändiga åtgärderna som rekommenderas i testrapporten.
- Ingram Micros SOC-team kommer att tillhandahålla dokumentation med nödvändiga åtgärdsförslag för eventuella funna brister.
- Ingram Micros SOC-team ansvarar inte för att fastställa/åtgärda någon av funna sårbarheterna utan endast för att tillhandahålla dokumentation för hur eventuella problem kommer kunna åtgärdas.

Kontakta oss

Har du frågor om vår tjänst **Penetration Testing** är du välkommen att kontakta oss på:

csec.nordics@ingrammicro.com eller +46-708-234740

Shawn Akrawi
Business Development Manager

Andreas Pantzar
Sales Specialist

9. Bilaga - A – vanliga frågor

Vad är en Penetration testning?

Penetrationstest, informellt kallad PenTest, är en attacksimulering mot datorsystem som söker säkerhetsluckor för att potentiellt får tillgång till systemfunktioner och information. Målet med penetrationstest varierar beroende på uppdragstyp, som godkänns av kund, för att hitta sårbarheter som kan utnyttjas av en angripare. Uppdragstagaren kommer att informera kunden om dessa sårbarheter tillsammans med rekommenderade åtgärder.

Hur utförs penetrationstestet?

Penetrationstest utförs vanligtvis med hjälp av en kombination av manuell och automatiserad teknik för att systematiskt kompromissa servrar, klienter, webbapplikationer, trådlösa nätverk och nätverksenheter (beroende på uppdragets omfattning och målsättning).

Vem utför penetration tester?

Vårt team innehåller högkvalificerade säkerhetsexperter med många års erfarenhet av sårbarhetsbedömning och penetrationstestning. Våra säkerhetsexperter håller globalt erkända säkerhetsuppgifter, inklusive men inte begränsat till Offensive Security Certified Professional (OSCP) och/eller GIAC Certified Penetration Tester (GPEN).

10. Bilaga - B – Verktyg

Ingram Micro använder en blandning av automatiserade och manuella test metoder för att upptäcka eventuella sårbarheter i ett nätverk. Vi använder oss av väl kända gratis samt kommersiella säkerhets verktyg. Vi använder bland annat följande applikationerna:

- **Maltego:** Ett verktyg som används vid penetrationstester samt i Public Discovery rapporter.
- **NMAP:** Ett nätverksskanner applikation som används för att mappa och lista nätverks enheter som är en del i ett penetrationstest.
- **Nessus:** En sårbarhetsskanner som används för att upptäcka sårbarheter och Malware som angripare kan använda för att ta sig in i ett nätverk. Nessus används som en del i sårbarhetsrapporter samt penetrationstester.
- **Qualys:** En nätverks och sårbarhetsskanner som används i Webbapplikationstester och vid penetrationstester.
- **Kali Linux distribution:** Ett operativsystem med hundratals verktyg som kan användas för alla typer av tester.
- **Burp Suit:** En webbaserad Proxy som används vid webbapplikationstester och vid webbpenetrationstester.
- **BeEF:** Används för webbtester som exploateringsverktyg.
- **OWASP proxy:** En lokal Proxy som används vid webb och mobilapplikationstester.
- **Metasploit:** Ett ramverk för penetrationstest som används för exploatering och i bedömning av penetrationstester efter exploatering.