IT WORKS FOR YOU ?

Audit Infrastructura

Scanare Vulnerabilitati

Teste de penetrare

Politici de securitate

Despre noi

Echipa de securitate IT a companiei FROSTWOLF este formata din specialisti cu peste 15 ani de experienta in domeniul securitatii IT. Detinem o multitudine de certificari internationale care acopera intreaga arie de servicii si echipamente :

MCP, MCSE, CISSP, LPIC-2, VCAP5-DCD, CCIE (RS,DC)

Condusa de un manager cu peste 20 de ani experienta in domeniul IT, FROSTWOLF ofera, pe langa servicii premium, siguranta, calitate, seriozitate, implicare si dinamism clientilor sai.

INTRODUCERE

Securitatea Cibernetica

Audit
Prevent
Secure

Intr-o lume a calculatoarelor, in care informația este preponderent digitală, accesul la informații a devenit atat o necesitate cât si un pericol. Securizarea informației se face pe mai multe nivele : infrastructură, echipamente de rețea, access fizic, protecție impotriva virusilor, malware-ului, ransomware-ului, protecție a mailului, echipamente mobile si licențiere corecta a software-urilor.

Serviciile noastre reprezinta evaluarea internă a securității sistemelor informatice a clientului pentru a oferi asigurare managementului companiei că sunt îndeplinite cerințele tehnice și organizatorice privind protejarea sistemelor informatice și că riscurile semnificative la adresa confidențialității, integrității și disponibilității datelor și operațiunilor companiei sunt identificate și ținute sub control.

Raportul de audit va conține o listă de propuneri făcută de către echipa de audit în vederea creşterii nivelului de securitate al sistemelor operate de client. Aceste propuneri se fac pe baza rezultatelor obţinute în urma testelor de securitate şi constau în implementarea unor controale noi de securitate sau în corectarea aplicării unor controale deja existente.

DESCRIEREA ETAPELOR PROCESULUI DE AUDIT

Etapa I. Analiza iniţială a sistemului ţintă – este o etapă iniţială obligatorie în care se colectează informaţii despre sistemul ce urmează a fi testat şi despre aşteptările responsabililor privind nivelul de securitate. Are următoarele sub-etape de parcurgere:

- Identificarea sistemului ţintă – sub-etapă în care se definesc la nivel primar perimetrul şi elementele componente ale sistemului ţintă.
- Identificarea documentelor de bune practică utilizabile ca referință pentru evaluarea nivelului de securitate
- Analiza configuraţiei sistemului ţintă – sub-etapă în care se studiază documentaţia sistemului şi se strâng informaţii de la personalul tehnic pentru a putea defini o imagine detaliată a arhitecturii şi modului de funcţionare a sistemului ţintă.

Etapa II. Proceduri de testare a securităţii sistemelor informatice – etapă a procesului de testare în care se proiectează şi se pune în aplicare setul de teste asupra sistemului ţintă. Implică parcurgere următoarelor sub-etape:

- Alegerea instrumentelor şi tehnicilor de testare – proces de selecţie şi proiectare a testelor în funcţie de specificul sistemului ţintă.
- Derularea testelor de securitate – punerea în aplicare efectivă a testelor de securitate.

Livrabile:

- Acord privind domeniul și obiectivele activităților de testare
- Rezultate brute ale activităților de testare

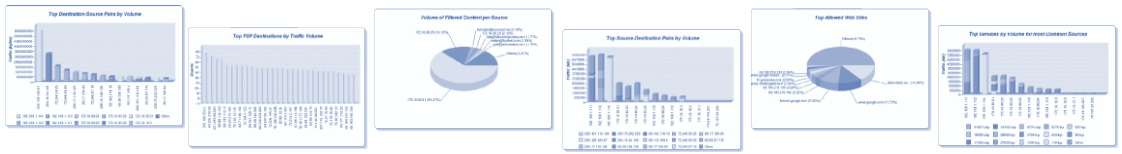
DESCRIEREA ETAPELOR PROCESULUI DE AUDIT

Etapa III. Proceduri de analiză a rezultatelor testării – interpretarea şi analiza rezultatelor testelor de securitate efectuare în etapa anterioară. Principale activităţi ale acestei etape constau în:

- Raportarea vulnerabilităţilor tehnice descoperite în urma scanărilor de securitate.
- Propuneri de îmbunătăţire a sistemului de securitate bazate pe vulnerabilităţile şi neconformităţile descoperite în urma derulării testelor de securitate.
- Elaborarea raportului final al testării securităţii sistemului informatic.

Livrabile:

- Raport de audit
- Plan de măsuri pentru remedierea riscurilor de securitate identificate



OBIECTIVELE PROCESULUI DE AUDIT

- Identificarea și delimitarea elementelor sistemului ce urmează a fi testat;
- Analiza sistemului ţintă din punct de vedere arhitectural şi al modului de configurare;
- Inventarierea instrumentelor de testare disponibile şi definirea unor criterii de selecţie în vederea efectuării testelor de securitate; proiectarea unor paşi de execuţie în efectuarea testelor de securitate;
- Obţinerea acordului proprietarilor / responsabililor de resurse pentru efectuarea testelor;
- Execuţia testelor de securitate în conformitate cu paşi stabiliţi la proiectarea fazei de testare;
- Evaluarea rezultatelor testelor de securitate în vederea identificării vulnerabilităţilor şi elementelor ce nu sunt conforme cu cerinţele;
- Determinare, în colaborare cu beneficiarul, a unui set complet de mecanisme şi măsuri de securitate care să permită eliminarea vulnerabilităţilor şi reducerea astfel a riscurilor de securitate și a unui plan de implementare a acestora.

DOCUMENTE DE REFERINȚĂ PENTRU SERVICIILE DE EVALUARE

Standarde și ghiduri ce vor fi folosite ca referințe în planificarea activităților de audit sunt următoarele:

- ISO/IEC 27007:2011: Information technology -- Security techniques -- Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2011 Information technology -- Security techniques -- Guidelines for auditors on information security controls
- Standarde ISACA:
  - S2 Independence
  - S5 Planning
  - S6 Performance of Audit Work
  - S13 Using the Work of Other Experts
- Ghiduri ISACA:
  - G1 Using the Work of Other Auditors
  - G8 Audit Documentation
- Metodologii de audit tehnic:
  - Open Source Security Testing Methodology Manual (OSSTM)
  - Information System Security Assessment Framework (ISSAF)
- SR ISO/CEI 27001:2006: Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe

ANALIZA INITIALA

Identificarea sistemului ţintă

Efectuarea de teste de securitate presupune selectarea unui sistem, sau unui grup de sisteme, care să fie subiectul – sistemul ţintă – a acestor teste. Identificarea sistemului ţintă presupune inventarierea tuturor entităţilor care fac parte din cadrul sistemului selectat şi delimitarea graniţelor fizice şi logice ale sistemului.

Identificarea cerinţelor iniţiale

Pentru sistemul ţintă trebuie să fie cunoscute cerinţele de securitate în uz la momentul proiectării şi efectuării testelor de securitate. Cerinţele de securitate identificate vor include toate elementele de securitate definitorii pentru funcţionarea sistemului provenite din reglementări legale (legi sau dispoziţii în vigoare), regulamente de funcţionare interne (politici, proceduri sau strategii organizaţionale) sau cerinţe tehnice de bună practică (parametrii optimi de configurare şi funcţionare).

Analiza configuraţiei sistemului ţintă

Proiectarea testelor de securitate şi selectarea instrumentelor tehnice de verificare a securităţii sistemului informatic sunt fundamentate pe analiza arhitecturii şi configuraţiei curente a tuturor componentelor aferente sistemului ţintă ales.

Analiza configurației va lua în calcul următoarele elemente: topologii de interconectare; versiuni ale programelor de bază (sisteme de operare, programe utilitare şi servicii ale sistemului de operare); programe de aplicaţii; mecanisme de securitate în uz (politici de securitate, instrucţiuni sau regulamente de utilizare, patch-uri de securitate, aplicaţii de securitate, mecanisme de autentificare a utilizatorilor etc.).

Analiza configuraţiei sistemului ţintă stă la baza selectării instrumentelor de testare necesare proiectării verificării de securitate.

PROCEDURI DE TESTARE A SECURITĂŢII SISTEMELOR INFORMATICE

1. Alegerea instrumentelor şi tehnicilor de testare

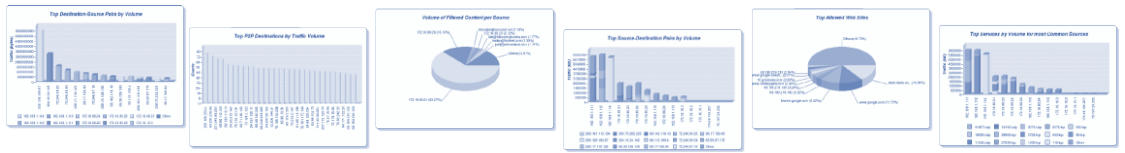
În funcție de specificul sistemelor identificate în domeniul de evaluare, instrumentele de testare automată pot include, fără a se limita la: Nmap, Nessus, Nexpose, MBSA, Accunetix, Instrumente și proceduri dezvoltate de personalul de evaluare

2. Auditul de infrastructura
   A. Analiza topologiei de reţea
   B. Analiza configuraţiei sistemelor
      a) Analiza sistemelor de tip ruter, firewall, IDPS
      b) Analiza sistemelor de tip server de aplicație
      c) Analiza sistemelor de tip server de email
      d) Analiza sistemelor de tip server de baze de date
      e) Analiza sistemelor de tip server DNS
      f) Analiza altor sisteme de tip server
   C. Analiza funcţionării mecanismelor de securitate existente
   D. Testarea instruirii şi a cunoaşterii regulilor de securitate

DERULAREA TESTELOR DE SECURITATE

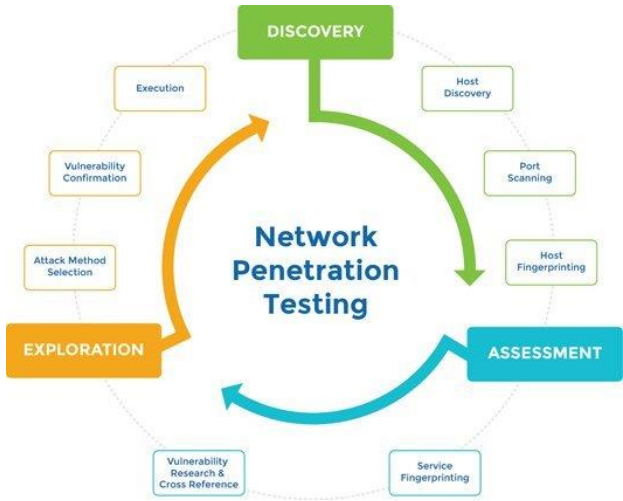
Având în vedere varietatea instrumentelor şi tehnicilor de testare a securităţii se pot identifica mai multe categorii de astfel de teste:

1. Teste de verificare a arhitecturii de reţea
2. Scanarea sistemelor în vederea identificării serviciilor de reţea
3. Scanarea de vulnerabilităţi a calculatoarelor din retea
4. Scanarea de virusi/malware/ransomware a calculatoarelor din retea
5. Analiza serviciilor de reţea (DNS, DHCP etc)
6. Scanarea serviciilor care ruleaza pe servere
7. Analiza configuratiilor echipamentelor active de retea
8. Testarea accesului la echipamentele Wireless
9. Evaluarea conexiunii la internet si redundața acesteia



TESTELE DE PENETRARE

Evaluarea internă a securității va fi complementată prin efectuarea de **teste de penetrare** care se bazează pe încercarea unor scheme cunoscute de penetrare a sistemelor de calcul prin intermediul slăbiciunilor de securitate a serviciilor de reţea identificate. Nu este necesară cunoaşterea detaliilor de acces (parole de acces); se imită comportamentul maliţios al unui atacator extern. Aceste teste pot perturba activitatea sistemelor de calcul în uz.



Testele de penetrare pot oferi următoarele beneficii:

- Testarea reţelei utilizând aceeaşi metodologie şi aceleaşi instrumente ca şi atacatorii;
- Verificarea vulnerabilităţilor existente;
- Mergând în profunzimea problematicii vulnerabilităţilor existente, se arată cum pot fi exploatate acestea pentru atacarea sistemelor;
- Demonstrarea faptului că vulnerabilităţile nu există numai la nivel teoretic;
- Oferă doza de realism necesară abordării problemelor de securitate.
- Permit testarea procedurilor şi a riscului reprezentat de factorul uman (prin tehnici de social engineering).

PROCEDURI DE ANALIZĂ A REZULTATELOR TESTĂRII

1. Raportarea vulnerabilităţilor

În urma efectuării testelor de securitate trebuie să se facă o colectare a informaţiilor brute generate de instrumentele de lucru utilizate în vederea analizei şi documentării nivelului actual de securitate şi identificarea vulnerabilităţilor la nivel de sistem ţintă. Analiza rezultatelor testului de securitate trebuie să se concretizeze într-un raport de securitate care să detalieze toate aspectele (negative sau pozitive) evidenţiate de efectuare testelor de securitate.

2. Propuneri de îmbunătăţire a sistemului de securitate

Raportul de analiză a rezultatelor testelor de securitate trebuie să conţină propuneri de îmbunătăţire a sistemului de securitate pentru sistemul ţintă în corelaţie cu aspectele negative dezvăluite de efectuare testelor asupra sistemului ţintă. Recomandările de îmbunătăţire a sistemului de securitate pot proveni din necesitatea de a contracara vulnerabilităţi tehnice cunoscute (soluţii tehnice disponibile) sau din necesitatea diminuării riscurilor de securitate generate de vulnerabilităţi noi (la care nu se cunosc rezolvări tehnice imediate şi trebuie concepute soluţii temporare de prevenire a unor incidente de securitate).

3. Raportul final de audit