Savarankiškų darbų užduotys

Užduotys atliekamos naudojant VMware ESXi 5.5 (6.0 ar 6.5) hypervizorių. Atlikus laboratorinį darbą, reikia parašyti ataskaitą, kurioje matytųsi darbų eiga (aprašas, ekrano nuotraukos) ir pasiektas rezultatas. Ataskaitos pabaigoje reikia pateikti darbo išvadas ir apibendrinimus. Užduoties numeris pasirenkamas pagal studento numerį grupės sąraše.

Laboratorinio darbo gynimui reikia paruošti 10 min. pristatymą, kuriame matytųsi kaip buvo atliktas darbas. **Darbas vertinamas 2 balais.**

1. **Užduotis**
   Virtualiose mašinose suaktyvinti SNMP tarnybą. Įtraukti virtualių mašinų stebėjimą į monitoringo sistemą ir stebėti jo parametrus. Monitoringo sistemą suinstaliuoti atskirame kompiuteryje arba kaip atskirą VM. Monitoringo sistemą pasirenkate patys Palyginti savo sukurtos monitoringo sistemos rezultatus su vidinės ESXi monitoringo sistemos rezultatais. Sukonfigūruoti ugniasienę taip, kad SNMP būtų prieinamas tik monitoringo serveriui.

2. **Užduotis**
   Sukonfigūruoti ESXi serveryje žurnalinių įrašų (log‘ų) rašymą į nuotolinį serverį (gali būti VM). Remiantis VMware Security Hardening rekomendacijomis, atlikti atitinkamą žurnalinių įrašų valdymo konfigūravimą. Atlikti ESXi ugniasienės konfigūravimą, kad log‘us galėtų pasiimti tik vienas nuotolinis serveris

3. **Užduotis**
   Sukonfigūruoti ESXi VMkernel portų grupę ir prijungti NFS saugyklą. NFS saugykla naudojant NFS 4.1 su Kerberos autentifikacija. Sukurti 3 direktorijas NFS serveryje su skirtingomis prieigos teisėmis. Taip pat NFS serveryje nurodyti leistinų prisijungimui IP adresų sritį. Suinstaliuoti NFS serverio saugykloje VM ir palyginti jos I/O našumą su VM, kuri suinstaliuota ESXi lokalių diskų saugykloje. Naudoti iOZone įrankį.

4. **Užduotis**
   Sukonfigūruoti ESXi serverio autentifikaciją taip, kad vartotojai ir jų teisės būtų skaitomos iš Microsoft AD serverio (šį serverį instaliuojate patys atskirame kompiuteryje arba kaip VM). Išanalizuoti duomenų srauto tarp ESXi ir AD saugumo grėsmes ir galimus pažeidžiamumus.

5. **Užduotis**
   Prie VM saugiai prijungti bendrintą Windows katalogą naudojant CIFS over SSH. Atlikti portų skenavimą (pvz. su WireShark) ir parodyti, kad duomenų perdavimas yra šifruotas. Palyginti CIFS over SSH saugumo aspektus su nešifruoto CIFS naudojimu.

6. **Užduotis**

   Sukonfigūruoti ESXi VMkernel portų grupę ir saugiai prijungti NFS saugyklą tarp ESXi ir NFS saugyklos realizuojant IPsec, VPN ar kitą technologiją. Atlikti portų skenavimą (pvz. su WireShark) ir parodyti, kad duomenų perdavimas yra šifruotas.

7. **Užduotis**

   VMware Player (galima naudoti ir VirtualBox) suinstaliuoti 2 VM, esančias vidiniame tinkle ir sukonfigūruoti VPN kanalą tarp jų. Programinę įrangą ir protokolą (PPTP, L2TP/IPSec, SSL) pasirenkate patys. Pademonstruoti VPN saugumą (pvz. su WireShark). Išanalizuoti VM CPU apkrovos ir tinklo pralaidumo priklausomybę nuo protokolo tipo siunčiant duomenis VPN kanalu ir be jo. Testavimui naudoti iperf įrankį. Testavimo rezultatai pateikiami grafikų pavidalu.

8. **Užduotis**

   ESXi serveryje suaktyvinti SNMP tarnybą. Įtraukti ESXi serverį į monitoringo sistemą ir stebėti jo parametrus. Monitoringo sistemą suinstaliuoti atskirame kompiuteryje arba kaip atskirą VM. Monitoringo sistemą pasirenkate patys. Palyginti savo sukurtos monitoringo sistemos rezultatus su vidinės ESXi monitoringo sistemos rezultatais. Sukonfigūruoti ugniasienę taip, kad SNMP būtų prieinamas tik monitoringo serveriui.

9. **Užduotis**

   Sukonfigūruoti iSCSI adapterį ir prijungti iSCSI du LUN‘us. Sukurti VMFS saugyklą apjungiant du iSCSI LUN. Naudoti CHAP autentifikaciją. iSCSI saugykla (*target*) kuriama atskirame kompiuteryje arba virtualioje mašinoje naudojant laisvai pasirenkamą programinę įrangą (pvz. Microsoft iSCSI Software Target 3.3 for Windows Server 2008 R2, iSCSI Cake, Starwind iSCSI ir t.t.). Naudodami WireShark įrankį paanalizuoti persiunčiamus duomenų paketus tarp ESXi ir iSCSI saugyklos.

10. **Užduotis**

    Parašyti skriptą, kuris parodytų ESXi serveryje veikiančias VM ir jų konfigūraciją, jas išjungtų, padarytų kopijas (klonuotų į kitą saugyklą) ir paleistų klonuotas VM. Analizuojant ESXi log failus parodyti, kad buvo užfiksuoti VM‘ų išjungimas ir paleidimas.

11. **Užduotis**

    Naudojant VMware vSphere Security Hardening Guide (ar kitą rekomendacinį vadovą) (https://communities.vmware.com/docs/DOC-21732) suprogramuoti automatinį ESXi serverio konfigūracijos saugos tikrinimo skriptą. Pateikti tikrinimo ataskaitą, ją argumentuotai paaiškinti. Skripto pagalba atlikti rekomenduojamus serverio konfigūravimo veiksmus, jį „kietinant“. Suinstaliuoti rinkoje egzistuojantį VM konfigūracijos saugos tikrinimo įrankį (pvz. CIS-CAT) ir palyginti gautus rezultatus.

12. **Užduotis**

    Sukonfigūruoti ESXi serverio autentifikaciją taip, kad vartotojai ir jų teisės būtų skaitomos iš Microsoft AD serverio (šį serverį instaliuojate patys atskirame kompiuteryje arba kaip VM). Išanalizuoti duomenų srauto tarp ESXi ir AD saugumo grėsmes ir galimus pažeidžiamumus.

13. **Užduotis**

    Parašyti skriptą, kuris parodytų ESXi serveryje veikiančias VM ir jų konfigūraciją, jas išjungtų, padarytų kopijas (klonuotų į kitą saugyklą) ir paleistų klonuotas VM. Analizuojant ESXi log failus parodyti, kad buvo užfiksuoti VM‘ų išjungimas ir paleidimas.

14. **Užduotis**

    Parašyti skriptą, kuris parodytų ESXi serverio konfigūraciją, jame veikiančios VM konfigūraciją, padidintų atminties ir CPU rezervaciją virtualiai mašinai, parodytų laisvos vietos kiekį duomenų saugykloje (datastore) ir virtualios mašinos failų užimamą kiekį saugykloje. Visą informaciją išvesti į atskirą (log) failą.

15. **Užduotis**

    Sukonfigūruoti ESXi serverio autentifikaciją taip, kad vartotojai ir jų teisės būtų skaitomos iš Microsoft AD serverio (šį serverį instaliuojate patys atskirame kompiuteryje arba kaip VM). Išanalizuoti duomenų srauto tarp ESXi ir AD saugumo grėsmes ir galimus pažeidžiamumus.

16. **Užduotis**

    Sugeneruoti DoS ataką į ESXi serverį (1 atvejis) ir į virtualią mašiną, esančią ESXi (2 atvejis). Atlikti tyrimą, kuris nustatytų ESXi veiksnumo priklausomybę nuo jo turimų resursų (CPU skaičiaus, RAM, tinklo pralaidumo). Išanalizuoti ESXi log‘us ir parodyti faktą, kad buvo įvykdyta DoS ataka prieš ESXi.

17. **Užduotis**

    Sukonfigūruoti ESXi serverio autentifikaciją taip, kad vartotojai ir jų teisės būtų skaitomos iš Microsoft AD serverio (šį serverį instaliuojate patys atskirame kompiuteryje arba kaip VM). Išanalizuoti duomenų srauto tarp ESXi ir AD saugumo grėsmes ir galimus pažeidžiamumus.

18. **Užduotis**

    Parašyti skriptą, kuris parodytų ESXi serveryje veikiančias VM ir jų konfigūraciją, jas išjungtų, padarytų kopijas (klonuotų į kitą saugyklą) ir paleistų klonuotas VM. Analizuojant ESXi log failus parodyti, kad buvo užfiksuoti VM‘ų išjungimas ir paleidimas.

19. **Užduotis**

    Virtualiose mašinose suaktyvinti SNMP tarnybą. Įtraukti virtualių mašinų stebėjimą į monitoringo sistemą ir stebėti jo parametrus. Monitoringo sistemą suinstaliuoti atskirame kompiuteryje arba kaip atskirą VM. Monitoringo sistemą pasirenkate patys Palyginti savo sukurtos monitoringo sistemos rezultatus su vidinės ESXi monitoringo sistemos rezultatais. Sukonfigūruoti ugniasienę taip, kad SNMP būtų prieinamas tik monitoringo serveriui.

20. **Užduotis**

    Sukonfigūruoti ESXi serveryje žurnalinių įrašų (log‘ų) rašymą į nuotolinį serverį (gali būti VM). Remiantis VMware Security Hardening rekomendacijomis, atlikti atitinkamą žurnalinių įrašų valdymo konfigūravimą. Atlikti ESXi ugniasienės konfigūravimą, kad log‘us galėtų pasiimti tik vienas nuotolinis serveris

21. **Užduotis**

    Sukonfigūruoti ESXi VMkernel portų grupę ir prijungti NFS saugyklą. NFS saugykla naudojant NFS 4.1 su Kerberos autentifikacija. Sukurti 3 direktorijas NFS serveryje su skirtingomis prieigos teisėmis. Taip pat NFS serveryje nurodyti leistinų prisijungimui IP adresų sritį. Suinstaliuoti NFS serverio saugykloje VM ir palyginti jos I/O našumą su VM, kuri suinstaliuota ESXi lokalių diskų saugykloje. Naudoti iOZone įrankį.

22. **Užduotis**

    Sugeneruoti DoS ataką į ESXi serverį (1 atvejis) ir į virtualią mašiną, esančią ESXi (2 atvejis). Atlikti tyrimą, kuris nustatytų ESXi veiksnumo priklausomybę nuo jo turimų resursų (CPU skaičiaus, RAM, tinklo pralaidumo). Išanalizuoti ESXi log‘us ir parodyti faktą, kad buvo įvykdyta DoS ataka prieš ESXi.

23. **Užduotis**

    Sukonfigūruoti ESXi serverio autentifikaciją taip, kad vartotojai ir jų teisės būtų skaitomos iš Microsoft AD serverio (šį serverį instaliuojate patys atskirame kompiuteryje arba kaip VM). Išanalizuoti duomenų srauto tarp ESXi ir AD saugumo grėsmes ir galimus pažeidžiamumus.

24. **Užduotis**

    Parašyti skriptą, kuris parodytų ESXi serveryje veikiančias VM ir jų konfigūraciją, jas išjungtų, padarytų kopijas (klonuotų į kitą saugyklą) ir paleistų klonuotas VM. Analizuojant ESXi log failus parodyti, kad buvo užfiksuoti VM‘ų išjungimas ir paleidimas.

25. **Užduotis**

    Sugeneruoti DoS ataką į ESXi serverį (1 atvejis) ir į virtualią mašiną, esančią ESXi (2 atvejis). Atlikti tyrimą, kuris nustatytų ESXi veiksnumo priklausomybę nuo jo turimų resursų (CPU skaičiaus, RAM, tinklo pralaidumo). Išanalizuoti ESXi log‘us ir parodyti faktą, kad buvo įvykdyta DoS ataka prieš ESXi.