Informatikai technológiák laboratórium 2.
(BMEVIMIA429)

Komplex alkalmazási környezetek felderítése és menedzsmentje
(Mérési feladatok)

Szatmári Zoltán
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

2011. szeptember 26.

1. Mérési feladatok

A korábbi üzemeltetőjétől dokumentáció és előismeretek nélkül kaptunk egy informatikai infrastruktúrát. Ezt a rendszert kell a továbbiakban felügyelnünk és újabb szolgáltatásokat üzembe helyeznünk rajta.

Idegen gépek scannelése éles infrastruktúrán nem megengedett, hálózat elleni támadásnak minősül, kitiltást vonhat maga után. A mérés során mindenki a saját infrastruktúrájával foglalkozzon, más hallgatók mérésének megzavarása, infrastruktúrájának piszkálása jegylevonást von maga után.

1.1. A mérési infrastruktúra

A Lenovo gépen adott 4 virtuális gép, melyek a mérési infrastruktúrát alkotják. Ezek közül az egyik egy Windows XP operációs rendszerrel felszerelt gép, ami a kliens szerepét fogja betölteni. A többi (VM1-3), Debian Linux 5.0 (Lenny) operációs rendszert futtató gép alkotja a szolgáltatást, amit meg kell vizsgálunk és további előzetes információnk nincs róla.

Fontos tudnivaló, hogy a virtuális gépek „linked clone" technikával készültek és a futtatásukhoz az alapul vett virtuális gépek elérési útjának megadása is szükséges. A Windowsos gép a Windows XP SP3 Base virtuális gépen alapul, míg a linuxos gépek a ITLabLinuxBase image alapján készültek. A gépek indulásakor az alapul vett virtuális gépek elérési útvonalát megkérdezhetik.

A virtuális gépekre a feladatok elvégzéséhez szükséges eszközök előre telepítve vannak, így a mérés során csupán a megismert eszközök megfelelő

felhasználása a feladat. A kliens gép fontosabb mérést támogató szoftverei és **jótanácsok a méréshez**:

- Putty: SSH és Telnet kliens.

  A Telnet üzemmód a *Connection Type*: *RAW* beállítással érhető el. Célszerű az '*Close windows on exit* opciót is *Never* értékre állítani, hogy a kimenetet megtekinthessük.

- WinSCP
- Firefox
- Zenmap
- Wireshark

A mérés során célszerű az egyes feladatpontok szövegét figyelmesen végigolvasni és csak utána végrehajtani, különben fontos információk kerülhetik el a figyelmünket. Javasolt a kliens gépen teljes képernyős üzemmódban dolgozni, ahonnan a többi kiszolgáló SSH kapcsolaton kersztül elérhető lesz. Többször szükséges lesz egy-egy konfigurációs állomány minimális módosítása. Ha a keresett opciót nem találjuk benne, akkor bátorkodjunk segítséget keresni az Interneten!

A mérés értékelése a leadott jegyzőkönyv alapján történik, az elvégzett feladatok és a **jegyzőkönyv formai követelményei** alapján. A mérés során az utolsó feladatblokk (Monitoring) részleges vagy teljes elkészítése, a jeles osztályzathoz szükséges, de ezen kívül opcionális.

1.2. Infrastruktúra elindítása

A mérés első feladata az infrastruktúra beüzemelése. Indítsuk el a hoszt gépen a kliens, majd egyenként a 3 darab ITLab virtuális gépet a VMware Workstation alkalmazás segítségével és jegyezzük fel, amit így külső szemmel a konzolok alapján az infrastruktúránkról meg tudunk állapítani.

A mérés során az infrastruktúra topológiáját papíron fogjuk elkészíteni és figyeljünk annak folyamatos karbantartására. Az ábrán rögzítsük az egyes gépek adatait, hiszen ezen paraméterekre a mérés során folyamatosan szükségünk lesz.

1.3. Infrastruktúra felderítése

Az elindított infrastruktúráról sajnos eddig kevés információval rendelkezünk, a virtuális gépre nem tudtunk bejelentkezni. A feladat első fele az infrastruktúra lépésről-lépésre történő felderítéséről szól.

1. A mérésvezető által megadott adatokkal lépjünk be a kliens számítógépre és állapítsuk meg, hogy jelenleg milyen hálózathoz csatlakozunk.

2. Végezzük el a megfigyelt hálózaton az infrastruktúra felderítését a tanult eszközzel a „Ping Scan" eljárást használva! (Időtakarékossági okokból elegendő a 255.255.252.0 alhálózati maszkkal jelölt alhálózatban vizsgálódni) Milyen információkat gyűjthetünk ezzel a módszerrel?

3. Azon hosztok esetében, melyek a saját mérési infrastruktúránkat alkotják, állapítsunk meg, „Quick scan" vizsgálat során, hogy milyen szolgáltatások futnak rajtuk!

4. Milyen hálózati topológiát lehet az eddig megismert adatok alapján felrajzolni? A mellékletben található diagramot kiegészítve alkossa meg az infrastruktúra modelljét, mely az eddig megismert információkra épül!

5. A hoszt gépen vizsgáljuk meg a Virtuális gépeink VMware hálózati beállításait és tegyünk módosítási javaslatot arra nézve, hogyan tudnánk az infrastruktúránk eddig nem ismert részeit is felderíteni? A mérésvezetővel konzultálva hajtsuk végre a szükséges módosításokat! Figyeljünk arra, hogy a hálózati módosítások által érintett gép(ek) esetén a hálózati paraméterek frissüljenek. Legegyszerűbben ezt a virtuális gép hálózati adapterének letiltásával, majd engedélyezésével érhetjük el.

6. A módosítások után megismerhető információk alapján futtassunk egy újabb felderítést „Intense Scan" eljárást használva. Egy újabb diagram formájában készítsük el a infrastruktúra modelljét, vegyük fel a friss paramétereket az ábrához. (Célszerű a Zenmap programot újraindítani, ezáltal tiszta környezetet kapunk benne.)

7. Amennyiben már minden külső forrásból elérhető információ rendelkezésünkre áll, akkor a mérésvezető által kiosztott adatokkal lépjünk be a virtuális gépekre és támasszuk alá az eddigi megállapításainkat a gépeken elérhető tényleges információkkal.

8. Milyen egyéb szolgáltatásokat tudunk azonosítani a gépeken? Röviden ismertessük mindegyik gépet az általa nyújtott szolgáltatások szemszögéből és állapítsuk meg a teljes infrastruktúra célját! A továbbiakban

a kiszolgálókat az elsődleges funkciójuk alapján elnevezve fogjuk hivatkozni.

9. Az itlab.hu domain nevet sajnos még nem jegyezte be a hatóság, de már most, a bejegyzés előtt szeretnénk webalkalmazást fejleszteni. A VM1 gép *hosts* fájlában állítsuk be helyesen az adatbázisszerver `sql.itlab.hu` hoszthoz tartozó IP címét.

10. A megismert információkat felhasználva a mérési segédletben bemutatott SMTP esettanulmányt csináljuk végig. A VM1 gép rendelkezik SMTP szolgáltatással. Küldjünk `Telnet` segítségével ezen keresztül elektronikus levelet a `root@vm1.itlab.hu` címre! A levél megérkezését ellenőrizhetjük a VM1 gépen a `/var/mail/mail` fájl tartalma alapján, ahol alapértelmezetten a *root* felhasználó levelei tárolódnak. (A levelezőszerver SPAM védelem miatt kis késleltetéssel jelentkezik be, így nehezítve az „Early speaker"-nek nevezett sietős spammerek életét. Várjunk türelemmel! A levél tartalmi részében (a DATA kulcsszó után) ne foglalkozzunk a fejléccel, csak valami gyors, rövid tartalmat küldjünk.)

1.4. Webszolgáltatás

A megismert infrastruktúrában a webkiszolgálás jelentős szerepet játszik, de a jelenlegi szolgáltatás beállításaiban hibák lehetnek. Feladatunk egy egyszerű PHP webalkalmazás majd egy WordPress blog üzembe helyezése. A művelet során a megismert diagnosztikai módszerekkel állapítsuk meg a hibák okait és hárítsuk el azokat.

11. Teszteljük a VM1 gép webkiszolgálását a kliens gépről kiindulva. A szerver IP címe alapján kérjük le az ott kiszolgált weboldalt. Türelmesen várjuk meg a végeredményt! Mit tapasztalunk?

12. Korábbi ismereteinket felhasználva fogalmazzuk meg mi a különbség a kapott hibaüzenet és a HTTP 404-es hibaüzenet között?

13. A Wireshark eszközzel vizsgáljuk meg, milyen hálózati forgalmat tapasztalunk. Állítsuk be úgy az eszközt, hogy csak a webkiszolgáláshoz kapcsolódó csomagokat gyűjtse össze. Határozzuk meg, hogy mi lehet az előbb tapasztalt hiba oka és hárítsuk azt el. Indokoljuk döntésünket! A WireShark eszköz indulásakor a VmWare WorkStation felveti, hogy a hálózati kártya beállításait nem tudja módosítani. Ezt az üzenetet hagyjuk figyelmen kívül, mert a feladat alapbeállításokkal is elvégezhető.

14. A webszolgáltatás működését kliens oldalon különböző módszerekkel tudjuk ellenőrizni. Soroljunk fel ezek közül néhányat, és ne feledkezzünk meg arról sem, hogy nem minden kliens rendelkezik grafikus felülettel! Egy konzolos módszert próbáljunk is ki!

15. Vizsgáljuk meg a webszerver beállításait és állapítsuk meg, milyen virtuális kiszolgálókat (Virtualhost) üzemeltet!

16. Tekintsünk meg a kliens böngészőjében két ilyen oldalt! Mit tapasztalunk? Keressünk megoldást a problémára és tegyük meg a szükséges beállításokat.

17. Az így már működőképes webkiszolgálás hálózati forgalmát vizsgáljuk meg a Wireshark eszközzel és mutassuk be a hálózati forgalom elemzése alapján *virtualhosting* a működési elvét.

18. Ellenőrizzük egy előre telepített webalkalmazás működését és töltsük be a böngészőbe az alapértelmezett (IP címen elérhető) virtualhost alatt elérhető `konyvek.php` oldalt. Az esetleges lassabb reakciót türelemmel várjuk meg. Mi a hibajelenség oka? Oldjuk fel a problémát! Kiinduláshoz segítséget találhatunk az alapértelmezett virtualhost phpinfo.php oldalán. (Figyeljünk arra, hogy a probléma többrétű is lehet, nem biztos, hogy egy opció módosításával megoldható.)

19. A webalkalmazás kódjában vizsgálódva megtalálhatjuk az adatbáziscsatlakozáshoz használt felhasználót és jelszót. A VM1 gépről lekérve a `http://vm1.ip.cim/phpmyadmin/` URL-el elérhető tartalmat, a népszerű webes adatbázis menedzsment felülethez jutunk. Az adatbázisban a `konyv` táblába helyezzünk el néhány példa adatot, majd vizsgáljuk meg, hogy a webalkalmazásban is megjelent-e!

20. Telepítsük fel az infrastruktúránkra a WordPress blogmotort. A működéséhez hozzunk létre saját adatbázist saját felhasználóval és egy wp.itlab.hu virtualhostot. A virtualhostot az előzőek mintájára az Apache konfigurációs mappájában a `sites-available` mappa alatt hozzuk létre, majd az `a2ensite vhost.neve` utasítással engedélyezzük. (Az adatbázis létrehozásához szükséges *root* jelszót a mérésvezetőtől kapjuk meg.) A WordPress blogmotor telepítéséhez segítséget találunk az Interneten vagy a letöltött csomagban is. A sikeres telepítés után publikáljunk egy bejegyzést, demonstrálva a helyes működést. (A WordPress letöltését a http://static.inf.mit.bme.hu/wp.tar.gz címen tegyük meg, mert különben a WordPress szerver lelassulhat a mérés során)

1.5. Rendszermonitorozás

A megismert szolgáltatások egy részéhez előre beállított monitoring rendszer üzemel, melyet szeretnénk kiterjeszteni a webes szolgáltatásra is. A következő feladatok során vizsgáljuk meg a monitoring rendszer működését és a felmerülő hibákat hárítsuk el!

21. A kliens gépen tekintsük meg a Nagios rendszer webes felületét, tekintsük meg a *Service Details* oldalt. Vizsgáljuk meg és vessük össze a topológia ábránkkal, hogy milyen szolgáltatásokat monitorozunk a jelenlegi állapotban.

22. Vizsgáljuk meg a szerver oldalon a központi Nagios monitoring beállításait és a hosztok beállításainál javítsuk ki az IP cím beállításokat! A beállítások módosítása és a monitoring szerver újraindítása után vizsgáljuk meg a webes felületen, hogy helyesen működik-e a monitoring funkció! Az állapotlekérdezések időzítve vannak, azok hamarabb elvégzését a szolgáltatások részletező oldalán a *Rescedule* opcióval kérhetjük. Milyen hibát tapasztalunk? Hárítsuk el a problémát!

23. A webszerveren fut már az NRPE ágens, de a központi monitoring rendszer konfigurációs beállításai nincsenek felkészítve a webszerver monitorozására. Vegyük fel a webszervert új hosztként és állítsuk be rajta, hogy az alapvető NRPE-n keresztül elérhető szolgáltatásokat monitorozzuk. (Ne felejtsük el a Nagios szerveralkalmazást újraindítani!)

24. Tekintsük meg a Nagios webes felületén az előző lépésben tett módosítások eredményét. Keressük meg a hiba okát és javítsuk ki!

25. A webszerveren definiáljunk saját monitoring feladatot, mely azt vizsgálja, hogy a korábban telepített WordPress blog wp-settings.php állományát tudja-e valaki írni. Ha igen, akkor a „CRITICAL” riasztást kell adni, különben „OK” legyen a szolgáltatás állapota. Módosítsuk az NRPE és a központi monitoring rendszer beállításait, hogy ez a paraméter is megjelenjen a webes felületen.