Autentikacija na Linux Desktop AAI@EduHr identitetom

Na javnim računalima koja koriste pretežito studenti nalaze se instalirani Windows XP, a prijava se vrši putem Pgine sa AAI@EduHr identitetom. Ta se računala uglavnom koriste za pretraživanje Interneta, pristup servisu e-učenja, pisanje seminarskih radova i slično. U povodu najave prekida službene podrške za Windows XP 8.travnja 2014, 11 godina nakon njihove pojave, postavlja se pitanje: Što sa starijim hardwareom nakon isteka podrške?. Uglavnom se radi o računalima koja jedva zadovoljavaju minumum ili su ispod minumuma hardverskih zahtijeva koje traže Windows 7 il 8. Može li instalacija nekog "laganog" Linux desktop sustava produžiti vijek korištenje takvih računala? Trebalo bi samo naći adekvatan način autentikacije poput Pgine na Windowsima kojim bi se studenti, djelatnici fakulteta prijavljivali sa AAI@EduHr identitetom.

Za "lagani" Linux klijent probno su odabrane distribucije Xubuntu 13.04 i AntiX-13: 13.1. Xubuntu 13.04 je verzija popularne Ubuntu distribucije s manje zahtijevnim, laganim Xfce grafičkim sučeljem. AntiX-13 13.1 je prilagođena distribucija Debiana koja pri instalaciji nudi Wheezy (Stable), Testing i Sid (Unstable) varijantu. Odlučili smo se za Wheezy s Fluxbox grafičkim sučeljem. Praktički nakon instalacije imate sve potrebno za neko uredsko, multimedijalno računalo. Ostaje nam prilagoditi prijavu na GUI sučelje putem AAI@EduHr identiteta.

Prvi dio rješenja problema daje dokument Što je to spona? [1] gdje se poglavlju "Autentikacija osnovnih servisa putem AAI@EduHr" preporučuje korištenje modula pam_radius za autentikaciju korisnika. Jer kako dokument objašnjava koristi se posredni način putem kojeg RADIUS server kontaktira LDAP server.

Instalirajmo potrebni PAM modul na Linux klijent paket (Debian i Ubuntu) :

```
 # apt-get install libpam-radius-auth
```

U konfiguraciji na freeradius serveru u datoteci */etc/freeradius/clients.conf* dodamo javni IP klijenta kojeg koristi Pgina iza kojeg imamo lokalne klijente u tom slučaju javna računala.

```
client 161.53.***.** {
      secret          = NekaTajna
      shortname   = pgina-klijent
}
```

Nakon unosa obavezno napraviti ponovo pokretanje RADIUS servera:

```
#/etc/init.d/freeradius restart
```

Na strani Linux klijenta kako uputa kaže treba unijeti konfiguracijsku datoteku */etc/pam_radius_auth.conf* redak:

```
#  There are 3 fields per line in this file.  There may be multiple
#  lines.  Blank lines or lines beginning with '#' are treated as#  comments, and are
 ignored.  The fields are:
#
```

```
#  server[:port] secret [timeout]
161.53.***.*:1812    NekaTajna          3
#
#  the port name or number is optional.  The default port name is
#  "radius", and is looked up from /etc/services The timeout field is
#  optional.  The default timeout is 3 seconds.
```

Slijedi podešavanje konfiguracije PAM modula koji se nalazi */etc/pam.d* direktoriju. Kao što uputa "Spona što je to?"govori u datoteci */etc/pam.d/common-auth* možemo zadati da se svi servisi autenticiraju putem RADIUS-a. U našem slučaju to nije potrebno pošto želimo samo GUI prijavu pomoću RADIUS-a, ostali servisi nam ne trebaju.

U tom slučaju to je kod Xubuntu 13.04 konfiguracijska datoteka */etc/pam.d/lightdm* ili kod AntiX-13: 13.1. */etc/pam.d/slim*. U oba slučaja napravite slijedeće:

Zakomentirajte redak

```
#@include common-auth
```

i dodajte dva nova na sam vrh:

```
#%PAM-1.0
auth sufficient pam_radius_auth.so
auth required pam_unix.so try_first_pass
```

Nakon ovog unosa probamo se testno prijaviti svojim AAI@EduHr identitetom, upit dolazi do servera što znači da je upit ispravo proslijeđen ali dolazi do greške koju pronalazimo u */etc/freeradius/radius.log* logu našeg servera.

```
Mon Jul 8 11:44:54 2013 : Auth: Login incorrect ( [ldap_aai] Bind as user failed): [p
pucko@simet.hr] (from client pgina-klijent port 2277 cli ns.simet.lan)
```

Postoji logično objašnjenje koje se iz RADIUS loga ne može isčitati ali je očekivano da korisnik iz AAI imenika na Linux klijentu ima svoj home direktorij te se nalazi u */etc/passwd* i u */etc/shadow* koje sistem ne pronalazi i odbija prijavu. Za korisnički home direktorij postoji rješenje u obliku modula zvanog *pam_mkhomedir.so*.Koji služi za kreiranje korisničkih home direktorija ako ne postoje na početku prijave.Dozvoljava prijavu korisnika iz centralne baze u našem slučaju LDAP imenika.Podrazumijevano sadrži kopiju */etc/skel* direktorija kojeg koristi *useradd* program.

Traženu opciju o obliku retka unosimo u konfiguraciju */etc/pam.d/lightdm* i */etc/pam.d/slim*.

```
#%PAM-1.0session
   session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
   auth sufficient pam_radius_auth.so
   auth required pam_unix.so try_first_pass
```

No to je samo dio posla,što sa korisnicima kojih nema u */etc/passwd* te */etc/shadow*?Ovdje primjenimo malo "prljave igre" i mašte.Mogli bi ih dopisati ručno u obje datoteke no da li će to raditi?Tko će ručno ukucati stotine i tisuće korisnika u traženom obliku u konfiguraciju. Srećom iz kontakta sa kolegom Ivanom Icom Rakom koji mi je preporučio kao referencu dokument "*Spona što je to?*" dobivam bingo odgovor u kratkom vremenu."Moglo bi se to dobiti skriptom iz LDAP imenika".

Velika zahvala ovim putem kolegi Raki koji je s nama podijelio 2 skripte:

ldap2passwd.pl [2]

[2] ldap2shadow.pl [3]

Skripte pokrenemo na našem Linux klijentu

```
#./ldap2passwd.pl >> /etc/passwd
#./ldap2shadow.pl >> /etc/shadow
```

i one nam generiraju korisničke podatke pogodnog oblika koje onda sktipta automatski editira u */etc/passwd* i */etc/shadow* .

Primjer izgleda dijela ispisa iz skripte *ldap2passwd.pl* :

```
mmaric@simet.hr:x:1001:1001:Marko Mari?:/home/mmaric@simet.hr:/bin/bash
jjuric@simet.hr:x:1002:1002:Jurica Juri?:/home/jjuric@simet.hr:/bin/bash
pperic@simet.hr:x:1003:1003:Pero Peric:/home/pperic@simet.hr:/bin/bash
ppucko@simet.hr:x:1004:1004:Pucko Puckovi?:/home/ppucko@simet.hr:/bin/bash
```

Primjer izgleda dijela ispisa skripte *ldap2shadow.pl*.

```
mmaric@simet.hr:*:::::::
jjuric@simet.hr:*:::::::
pperic@simet.hr:*:::::::
ppucko@simet.hr:*:::::::
```

Nakon unosa korisnika u */etc/passwd* i */etc/shadow* prijava na sistem funkcionira korisnik dobiva svoj Desktop i korisnički direktorij,svi sretni i zadovoljni.:)To se vidi u */var/log/freeradius/radius.log* kao u primjeru.

```
Thu Aug 22 08:53:01 2013 : Auth: Login OK: [ppucko@simet.hr] (from client pgina-
klijent port 2922)
```

Poslije prijave na Xubuntu 13.04 ima problema sa odjavom korisnika sa sistema zbog čega nam se ipak kao bolja opcija pokazao AntiX-13: 13.1.Koji je većini sistemaca koji administriraju uglavnom Debian vjerovatno i bolji izbor. Nije mi se loša činila ideja da korisnike na prijavnom ekranu čeka neka obavijest o načinu prijavljivanja. Za to možemo iskoristiti zajedničku grafičku login temu.Treba napraviti temu sa nekim grafičkim editorom i jednostavno zamjeniti:

```
#cp mojaTEMA.jpg /usr/share/slim/themes/antiX/background.jpg
```

Moj primjer:

Time smo završili osnovno podešavanje i dobili poprilično živahan sistem sa obzirom na starost hardwarea na kojem se pokreće.Ilustracija prikazuje opterećenja pri pokrenutom video streamingu.

Dobili smo siguran i personalizirani način prijave korisnika koristeći se AAI imenikom ustanove na sustav koji će i dalje zadovoljavati sigurnosne standarde u smislu nadogradnji. A eto i odgovora na pitanje može li Linux na desktopu zamijeniti Windowse XP. :)

čet, 2013-08-22 13:09 - Goran Šljivić**Kuharice:** Linux [4]
Kategorije: Preglednici [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1309

Links
[1] http://www.aaiedu.hr/docs/spona.pdf
[2] https://sysportal.carnet.hr/system/files/ldap2passwd.txt
[3] https://sysportal.carnet.hr/system/files/ldap2shadow.txt
[4] https://sysportal.carnet.hr/taxonomy/term/17
[5] https://sysportal.carnet.hr/taxonomy/term/27