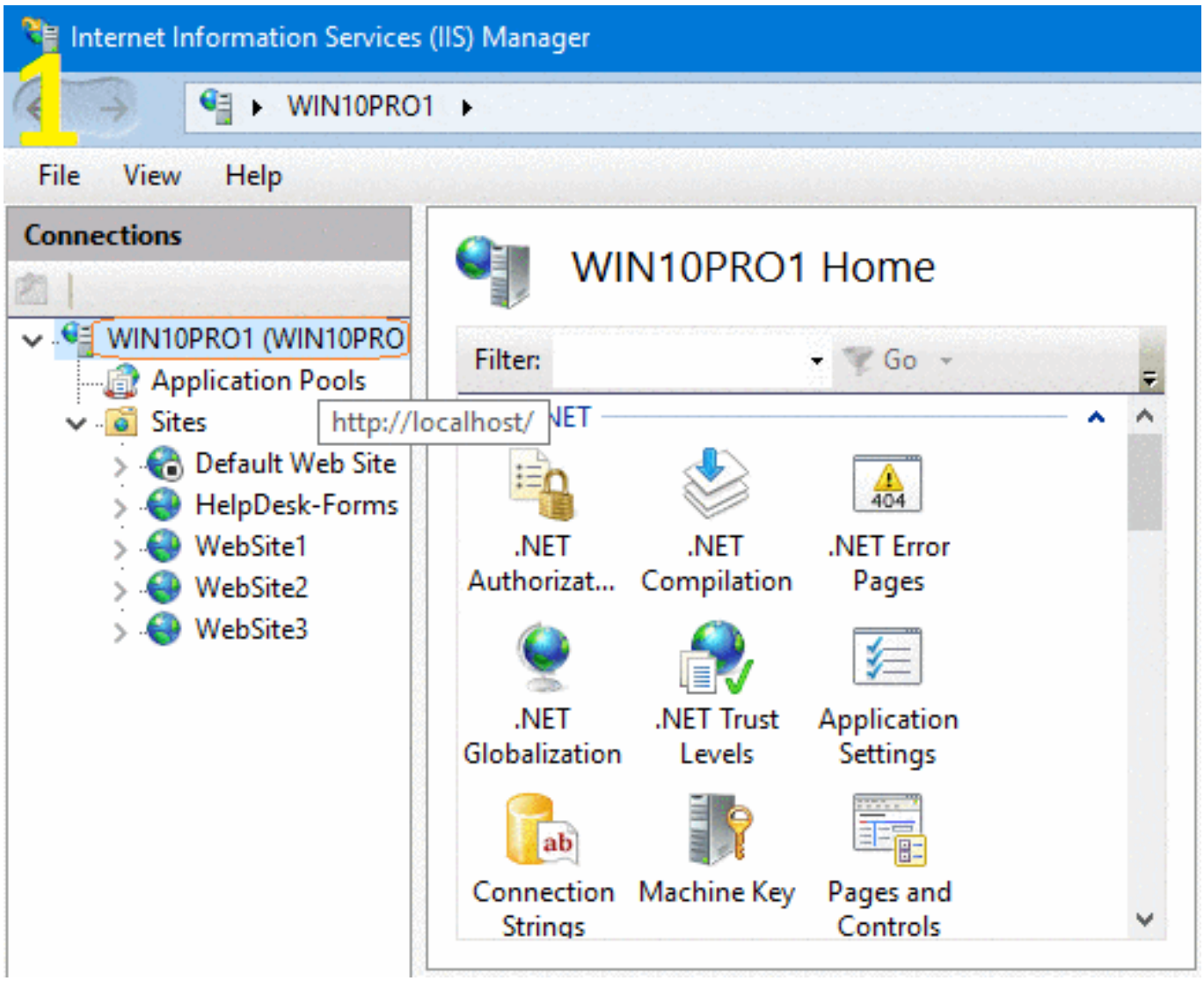
Internet Information Services i Anonymous/Basic autentikacija

U prošlom smo članku [1] iskoristili činjenicu da je Desetka opremljena najsuvremenijom inačicom Internet Information Services web servera, pa smo podigli nekoliko TLS-om zaštićenih web mjesta na istoj IP adresi i portu. Na kraju smo se sjetili da bi bilo dobro propuštati do naših web usluga samo one osobe koje se prethodno identificiraju posredstvom neke vjerodajnice. Poput svakog boljeg web servera, IIS omogućuje nekoliko načina autentikacije – od prastare username/password kombinacije do sve prisutnijih osobnih digitalnih certifikata. Poželimo li se poigrati sa svakom od raspoloživih autentikacija, skoknut ćemo u Programs and Features te narediti instalaciju stavke Security kao cjeline.

Potom u IISManu, kako je animacijom prikazano, pogledamo što sve možemo iskoristiti. Active Directory Client Certificate metoda sugerira da je autentikacija certifikatima moguća samo ako je IIS član domene, no daleko je to od istine. Ni na koji način Microsoftov web server ne ovisi o Windows domeni, samo je adminima lakše administrirati IIS instalacije ako ih uključe u domenu.

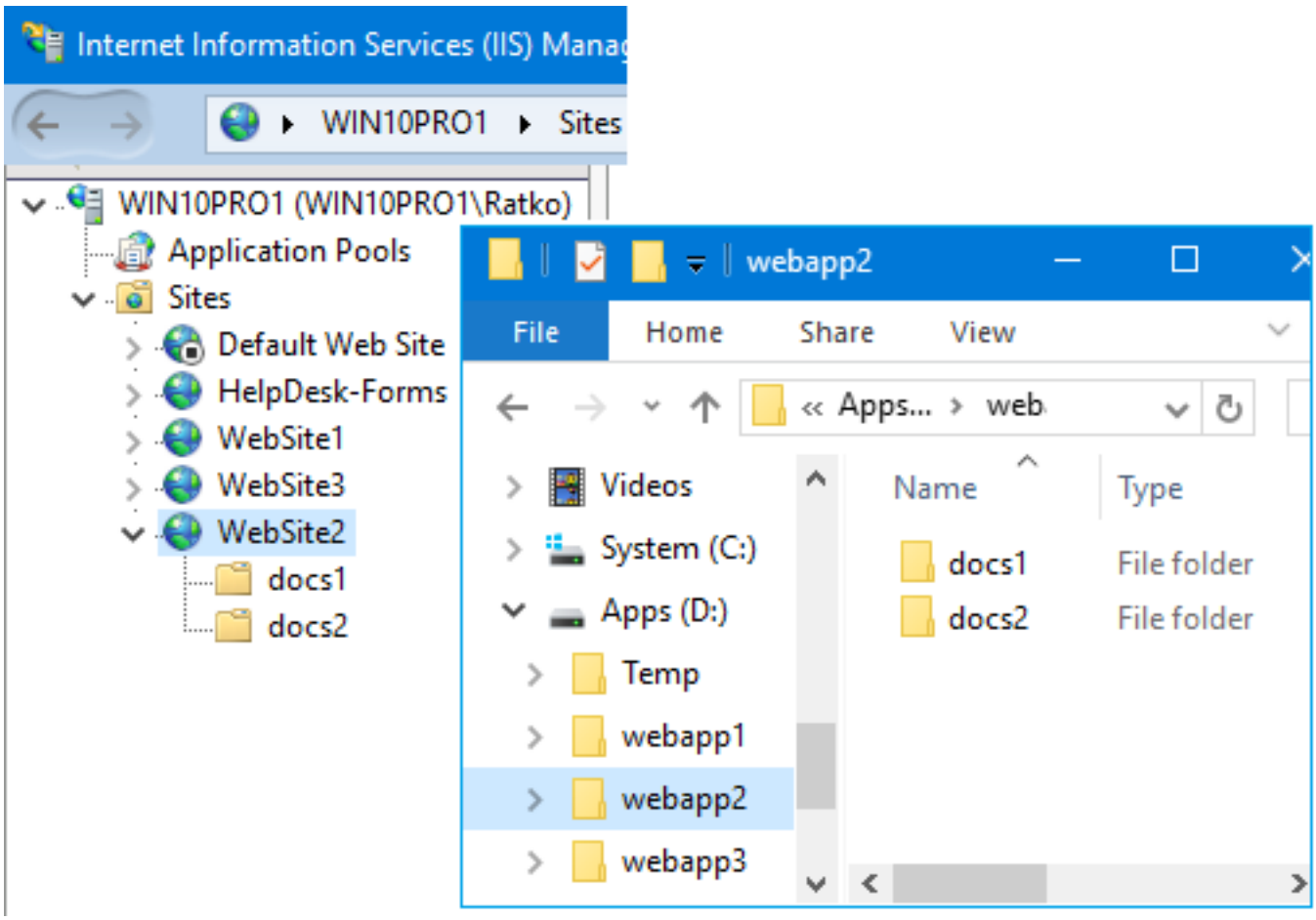


Fokusirat ćemo se na Basic autentikaciju (vidi RFC 7617) jer je primjenjiva i za privatne i za javne web sajtove. Dodatno, funkcionalna je bez obzira na klijentski operativni sustav ili browser. Jedinu stvarnu slabost ove autentikacijske metode – prenosi vjerodajnicu u čitljivom obliku - već smo otklonili primjenom TLS poslužiteljskih certifikata. Usput, sve rečeno važi i za Forms Authentication, ali nju ne možemo postaviti bez programiranja, što je prevelik zalogaj za većinu nas sistemaca.

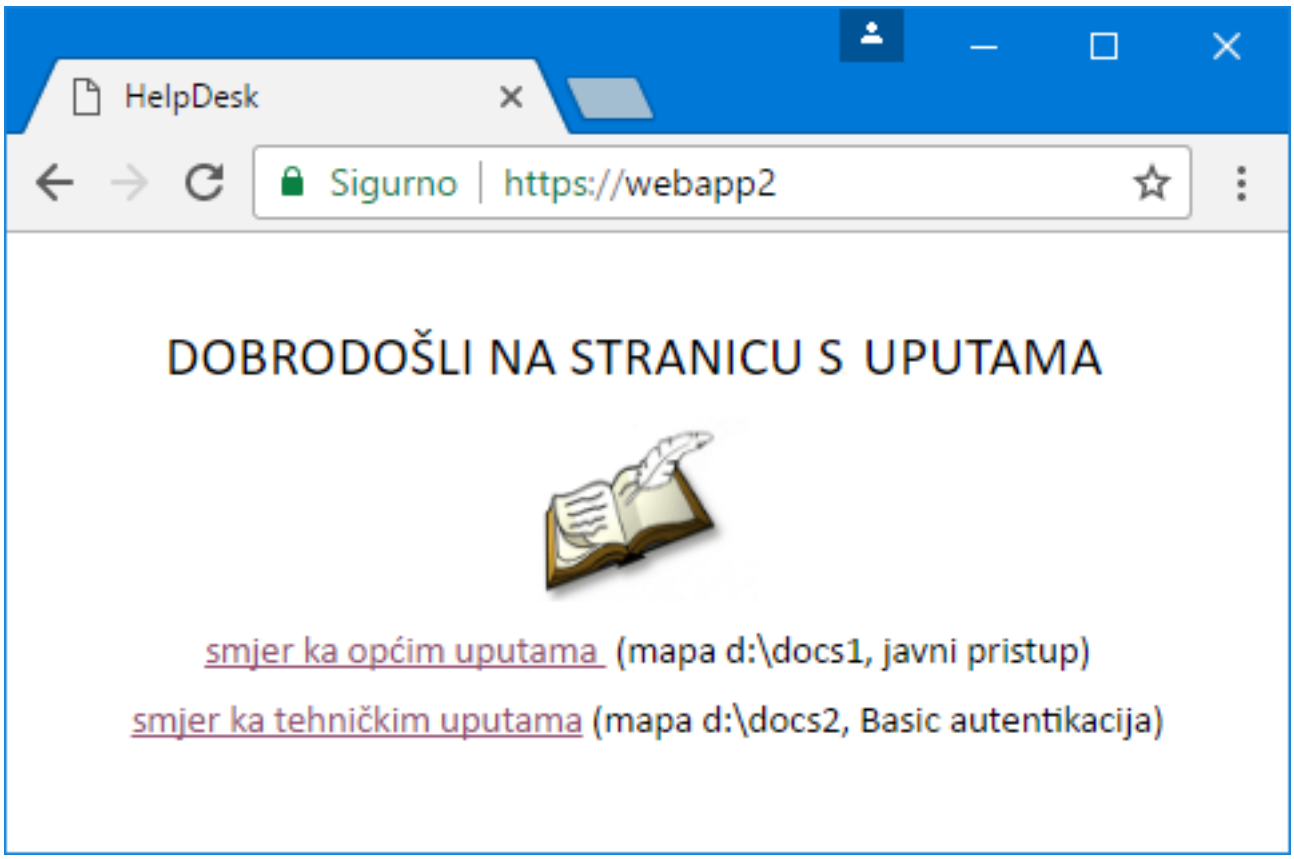
U nastojanju da što bolje oponašamo stvarnu situaciju, Basic autentikaciju kombinirat ćemo s anonimnim pristupom... i tako dolazimo do sasvim realnog scenarija: WebSite2 pretvoriti u biblioteku uputa za download, s time da upute za korisnike moraju biti općedostupne (bez autentikacije), dok je pristup tehničkim uputama moguć samo ovlaštenim osobama, dakle, onima koji se predstave nama prihvatljivom username/password vjerodajnicom.

Prvi korak: Na stanici sa IIS-om kreiramo korisnika korisnik1. Neka ostane u grupi Users jer ta grupa defaultno ima pravo čitanja na NTFS razini. Utoliko, po pitanju autorizacije smo mirni jer autenticirani korisnik neće moći mijenjati, brisati ili dodavati dokumente.

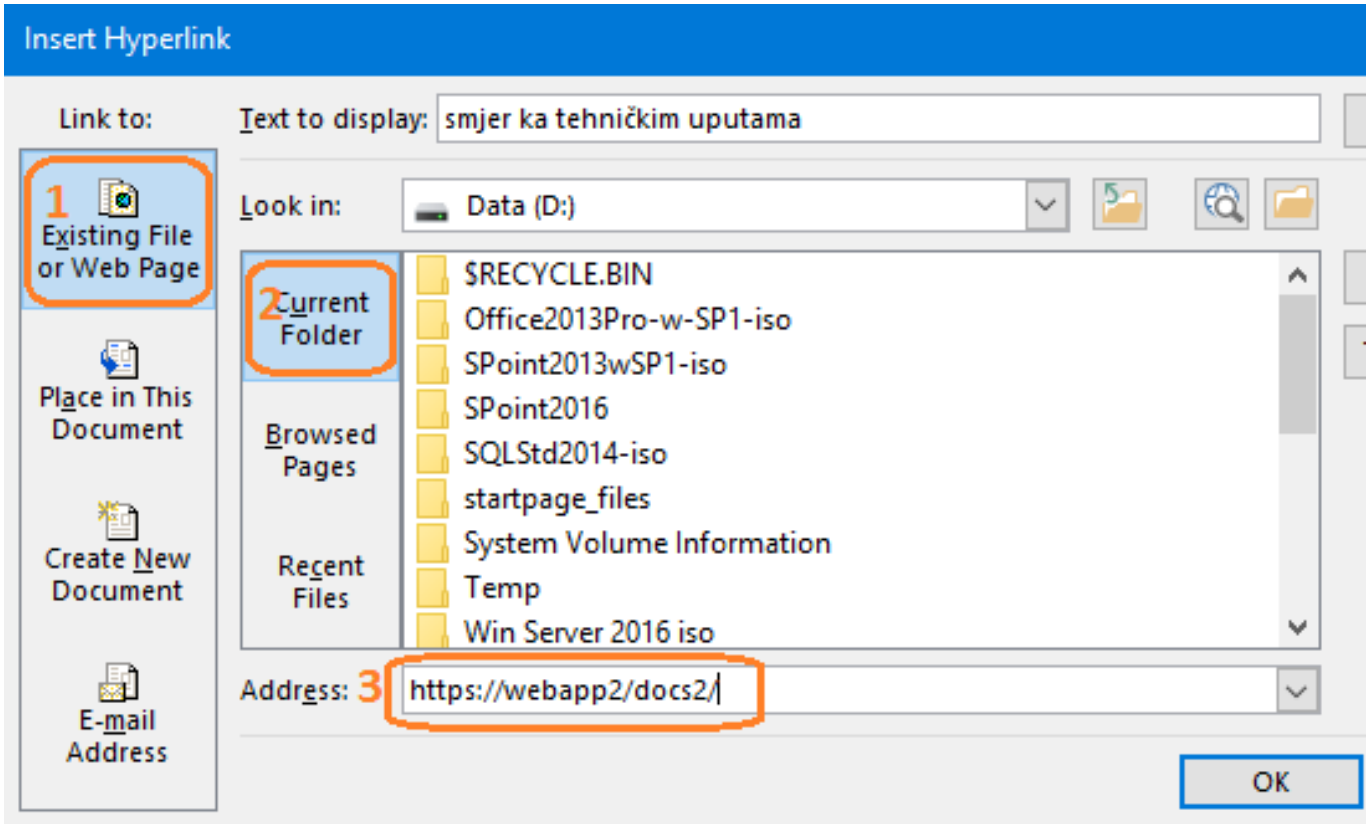
Drugi korak: U d:\webapp2\ kreiramo mape docs1 i docs2; u svaku mapu kopiramo par dokumenata-uputa. Niže je slikovni prikaz tih mapa u IISManu i Windows Exploreru.



Treći korak: Zadatak ne možemo realizirati „aplikacijom„ startpage.txt, stoga ćemo iskoristiti Word ili sličan mu alat kojime možemo kreirati statičku HTML stranicu s linkovima ka javno dostupnom sadržaju (taj će biti u mapi docs1) i sadržaju za kojega se je potrebno autenticirati (mapa docs2). Stranica poput ove na narednoj slici ispunit će sve naše potrebe. Naravno da je potrebna i sličica, po mogućnosti animirana, ta moramo misliti i na estetski doživljaj posjetitelja, zar ne?! :o)



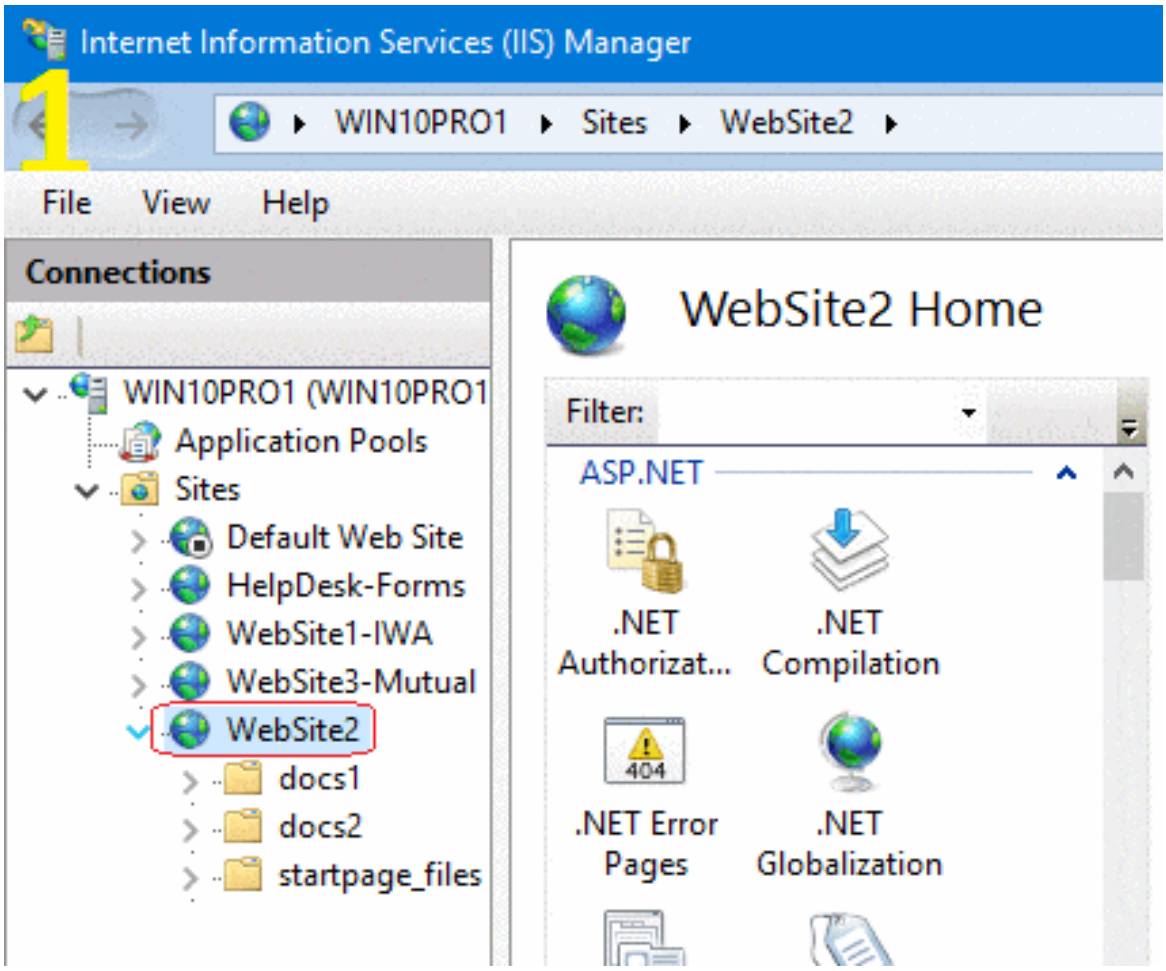
Kako u Wordu konvertirati tekst u HTML link? Srećom, jednostavno: označimo izraz, desni klik i naredba Hyperlink. Prvi ćemo link usmjeriti na mapu docs1 a drugi na docs2; na narednoj slici upravo radimo link ka mapi docs2.



Kad ovaj dokument spremimo kao startpage.htm, Word kreira dokument i prateću mapu s XML-ovima u kojima je opis stranice; oba sadržaja moramo kopirati u d:\webapp2\. Nakon toga se

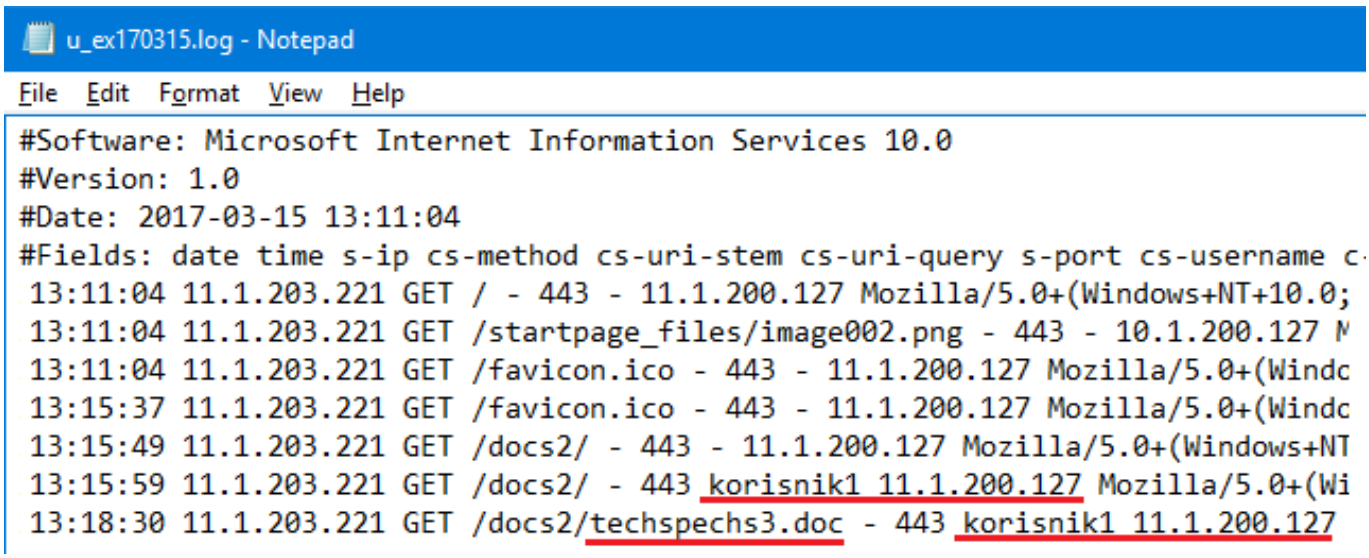
prihvatimo IISMana pa za website2, kroz applet Default Document, postavimo startpage.htm kao prvu stranicu.

Četvrti korak: Od ranije nam je na WebSite2 uključena Anonymous metoda pristupa. Ovu vrstu pristupa kontrolira sam IIS posredstvom svog računa IUSR koji, blago nama, kao član grupe Users također po defaultu ima samo prava čitanja i skidanja sadržaja biblioteke. Mapa docs1 će to naslijediti. Trebamo, znači, na mapi docs2 isključiti anonimni pristup a uključiti Basic autentikaciju. U tome će nam pomoći naredna animacija.



Navedene operacije rezultirat će pojavljivanjem web.config datoteka u mapama docs1 i docs2 – to IIS radi za nas. Zavirite u te fajlove i odmah ćete shvatiti o čemu je riječ. IIS često rastereću administratora, tako je i sada samo što ipak moramo sakriti te konfiguracijske datoteke kako ne bi zbunjivale klijente. Naime, korisnik će ih kroz preglednik vidjeti u popisu dokumenata, ali, budući da ih IIS štiti, umjesto uvida u njihov sadržaj dobit će poruku o grešci. Sakrivanje dodjeljivanjem atributa hidden odradimo ili naredbom Attrib ili iz Windows Explorera, lagan poslić.

Peti korak: S druge stanice – Windows ili Linux - možemo se spojiti na https://webapp2, te klikom na prvom linku pristupiti sadržaju mape docs1 (općim uputama). Klik na linku za tehničke upute izazvat će pojavljivanje autentikacijskog okvira; ulogiramo li se kao korisnik1 moći ćemo pristupiti sadržaju mape docs2 i skidati upute. Jasno, zato što je naša konekcija zaštićena TLS-om, i vjerodajnica i podaci su enkriptirani.
Praćenje aktivnosti korisnika defaultno je uključeno, logovi su u %SYSTEMDRIVE%/inetpub/logfiles, u mapama W3SVCn, gdje je n redni broj (ID) web mjesta kako je prikazano u IISManu kad kliknemo na stavci Sites u lijevom oknu IISMana. Zahvaljujući Basic autentikaciji vidimo koji se korisnik, kad, od kuda... spojio na biblioteku s tehničkim uputama i što je skinuo.



Kako vidimo, dovoljno je slijediti korake izložene u dva omanja članka da bismo podigli potpuno djelatan i razumno zaštićen web server kojeg smo dobili zajedno s Windows OS-om. No, jedno je metodom step-by-step aktivirati osnovne funkcionalnosti web servera a drugo je razumjeti spomenute i još brojnije nespomenute značajke, zajedno s međuzavisnostima... utoliko, ocijenite li IIS vrijednim poneke implementacije, svakako se za početak zbližite s kategorijama poput **Application Pools** i **Virtual Directories**.

sub, 2017-04-08 10:22 - Ratko Žižek**Kuharice:** Windows [2]
Kategorije: Servisi [3]
Vote: 0

No votes yet

story_tag: autentikacija [4]
IIS [5]
windows [6]

Source URL: https://sysportal.carnet.hr/node/1733

Links
[1] https://sysportal.carnet.hr/node/1728
[2] https://sysportal.carnet.hr/taxonomy/term/18
[3] https://sysportal.carnet.hr/taxonomy/term/28
[4] https://sysportal.carnet.hr/taxonomy/term/74
[5] https://sysportal.carnet.hr/taxonomy/term/75
[6] https://sysportal.carnet.hr/taxonomy/term/76