Windows OS - od mita do stvarnosti

Postoje dvije predrasude o Windows OS-u koje su, zahvaljujući dugogodišnjem nekritičkom prenošenju „s koljena na koljeno“ (što pisanom što govornom riječju), dosegle razinu mita, postajući time neupitne, samorazumijevajuće:
a) Windows OS je nesiguran, što ga čini nepodesnim za primjenu u sigurnosno iole zahtjevnijim situacijama, posebno onima koje uključuju Internet konekcije.

b) za dijeljenje mapa i pisača na Windows OS-u potrebna je gomila TCP/UDP portova, od kojih su neki sigurnosni problem, što Windows OS čini nepoželjnim za tu ulogu.

Izvorište oba mita nalazi se u davnoj prošlosti - informatičkim mjerilom mjereno, dakako – kada su windoze uistinu imale opisane slabosti. No, Windows 2000, i sve kasnije edicije, eliminiraju slabost (b), a sa pojavom Windows Server 2003 (i kasnijim desktop inačicama) i prva tvrdnja (a) postaje sve diskutabilnija. Da, ranjivosti i danas postoje, ta svi smo bolno svjesni toga, ali Windows OS je u tome ravnopravan drugim popularnim OS-ovima. Puno indikatora potvrđuju tu tezu, niže je samo jedan, ali reprezentativan (kompletan članak je na http://www.softpanorama.org/Commercial_linuxes/Security/top_vulnerabilities.shtml):

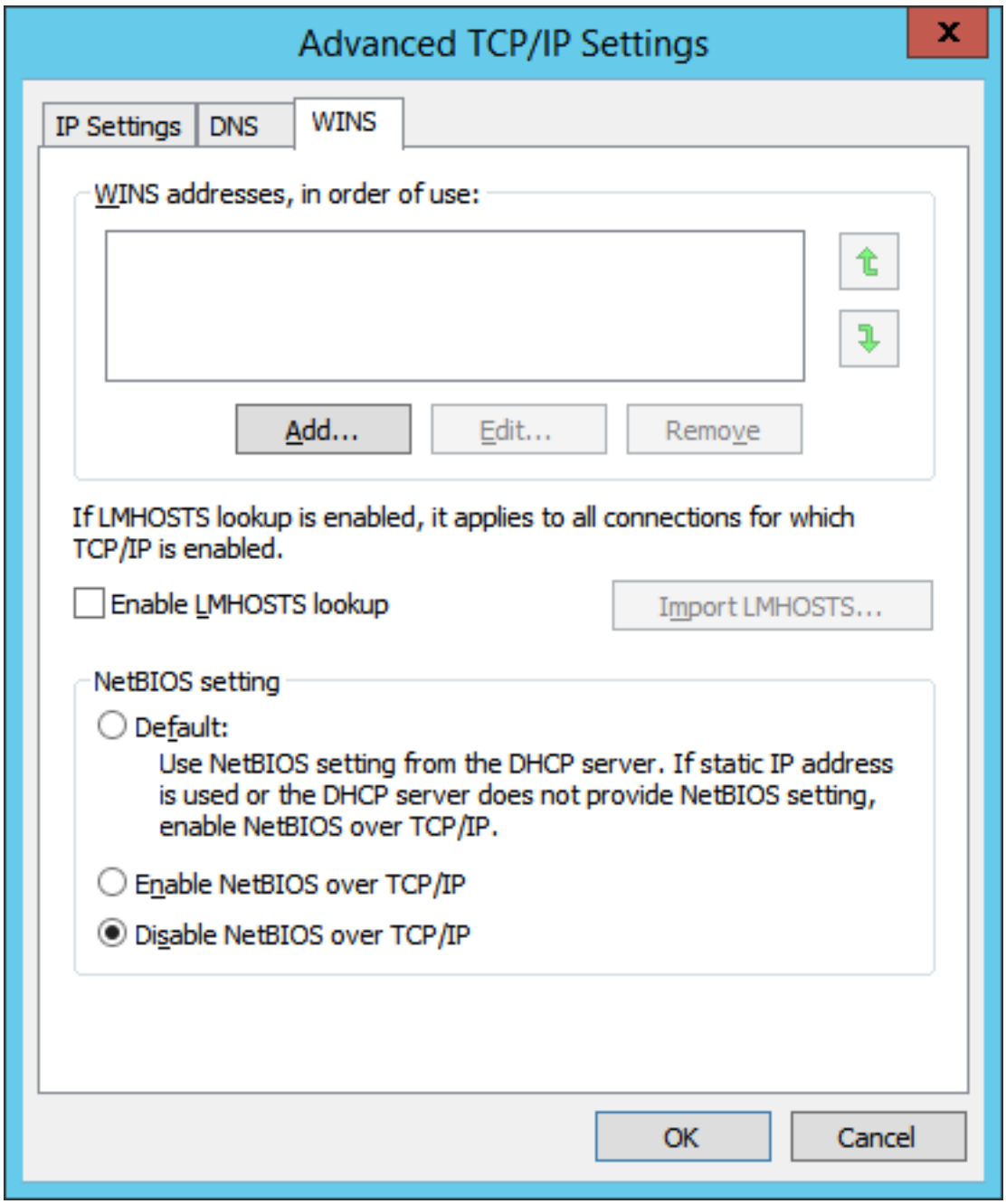
According the U.S. Government’s database of computer security vulnerabilities maintained by the National Institute of Standards and Technology (http://icat.nist.gov) as of April 15, 2004, there have been more High Severity (remotely exploitable) vulnerabilities found in the Linux operating system than in Microsoft Windows.

Autori također navode da je prednost Unix/Linux platforme u tome što se konkretna instalacija može bolje osigurati u smislu zaštite od provala s mreže i/ili ugnježđivanja zlonamjernog softvera. No, raspoloživi potencijali su jedno a njihova iskorištenost „na terenu“ drugo, pa u praksi, na veliko zadovoljstvo cyber kriminalaca, imamo tek polovično fortificirane unixoidne instalacije. Tako da, nakon vaganja „pro et contra“ možemo zaključiti da je jedini stvarni nedostatak Windows OS-a u odnosu na Linux/Unix kao njegovu pravu konkurenciju, veća izloženost Windowsa računalnim virusima i crvima. Što, opet, ima povijesne razloge – nešto od toga naći ćemo u spomenutom članku – no, svejedno, to je objektivno stanje.

Kako to biva, ljudi se emocionalno vežu ne samo za živa stvorenja nego i za stvari, ideologije.... pa i tehnologije. Utoliko, nekome se rečeno neće svidjeti, naći će tucet zamjerki ali meni se, sa dosadašnjima spoznajama i iskustvima, gore izloženo čini istinitim.

Prijeđimo sada na mit o problematičnom dijeljenju mapa i pisača na windozama.
Suvremene edicije Windowsa rabe SMB3 protokol za dijeljenje mapa i pisača. Pri tome, Windows računalo koje na mreži oglašava svoje resurse, može prihvatiti klijentske konekcije na jedan od dva načina:
- SMB over TCP/IP, pri čemu se rabe portovi TCP/UDP 445
- NetBIOS over TCP/IP, kad se rabe portovi TCP 139 i 137 te UDP 137 i 138

Od Windowsa 2000, na WINS kartici (eno je pod Properties TCP/IP protokola na mrežnoj kartici), možemo isključiti NetBIOS over TCP/IP, čime se efektivno zatvaraju gore spomenuti NetBIOS portovi, a Windows računalo normalno nadalje prihvaća i opslužuje klijentske konekcije kroz TCP 445. WINS kartica je idealno konfigurirana ako odgovara nižoj slici.



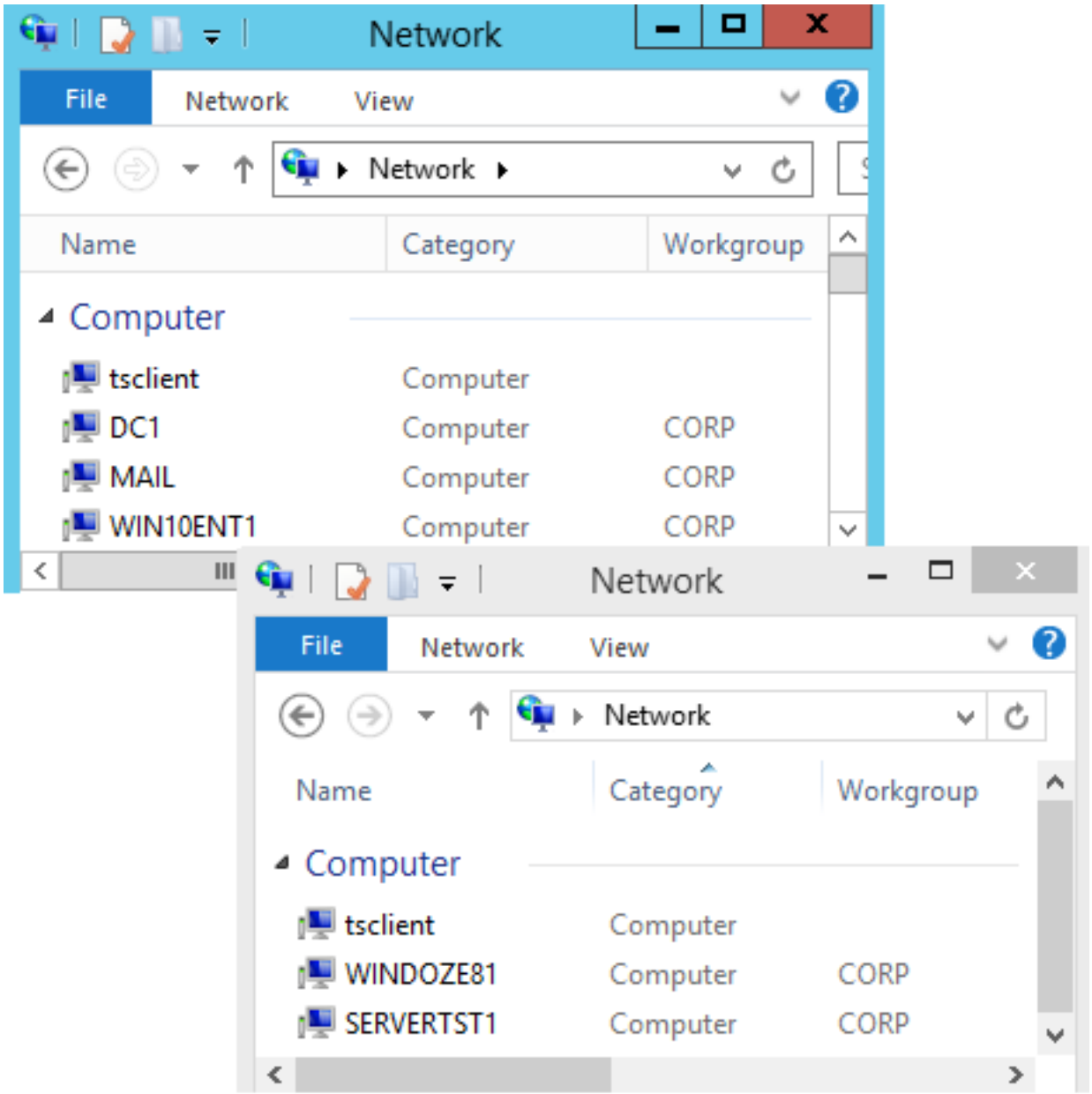
Nasuprot uvriježenom mišljenju, ovime nismo otklonili nekakvu ranjivost jer je servis koji sluša na ozloglašenom portu TCP 139 odavno temeljito prerađen, znači, otporan je na napade koji su ga svojevremeno „proslavili“ kao sigurnosnu rupu. Ipak, možemo reći da smo smanjili manevarski prostor napadaču jer smo iz igre izbacili četiri porta. Znamo kako to ide u računalnoj sigurnosti – neka softverska komponenta sama po sebi ne mora biti ranjiva, ali može poslužiti kao izvor informacija za oblikovanje strategije napada. A može, bome, i sama postati sigurnosni problem; praksa nas podučava kako ono što se godinama smatralo sigurnim postane ranjivo, štoviše, da je godinama bilo ranjivo dok je istovremeno vrednovano kao uzor sigurnosti.

Isključivanje NetBIOS-a na Windows računalima ni po čemu se neće negativno odraziti na funkcionalnost dijeljenja i uporabe mapa i pisača, čak i na segmentiranom LAN-u (routanoj internoj mreži). Ujedno smo značajno smanjili broadcaste po mreži i omogućili finije filtriranje prometa na mrežnoj opremi, što će jako razveseliti mrežare. Naposljetku, možemo „umiroviti“ i WINS servis, ako smo ga ranije dignuli kako bismo omogućili korisnicima Windows računala na segmentiranoj mreži nesmetanu uporabu Network preglednika.

Možemo reći da smo na dobitku, barem na tehničkoj razini. Potencijalni problem su korisnici

Windows računala jer ipak moraju promijeniti neke navike, ponekad i sami informatičari.

Što se tiče korisnika, nakon isključivanja NetBIOS protokola, na routanom LAN-u Network preglednik može prikazati samo one članove domene ili radne grupe koji su na istom subnetu. Na nižoj slici vidimo “razlomljenu“ domenu Corp – računala unutar istog mrežnog segmenta međusobno se vide, ali ne vide sabraću s one strane routera. Nepripremljenim korisnicima će to svakako otežati rad.

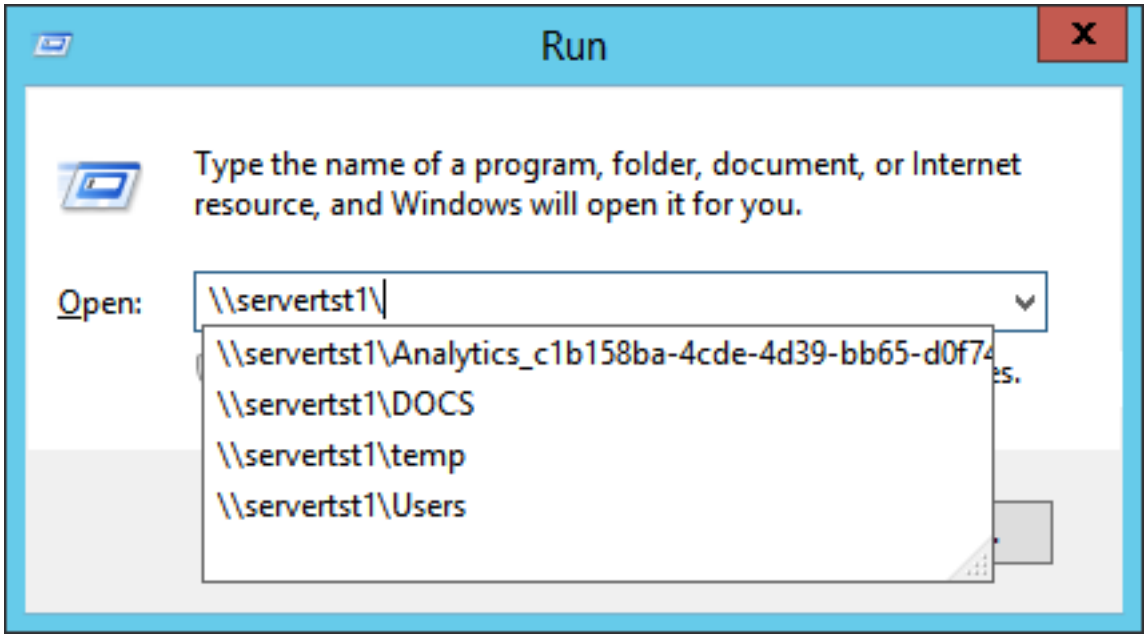


Može li korisnik računala Win10Ent1 vidjeti računala prisutna na drugom mrežnom segmentu domene, poput Servertst1 i Windoze81, i bez NetBIOS podrške? Može, samo se treba poslužiti naredbom Search Active Directory, koja se nalazi na kartici Network unutar preglednika Network, vidi gornju sliku. To je izvedivo zbog povezanosti Active Directory sustava sa DNS servisom. Ta povezanost korisniku ujedno omogućuje ono najvažnije: spajanje na neki dijeljeni resurs uporabom NetBIOS (single-label) imena ciljnog računala - znači, kako je i navikao - bez obzira nalazi li se to računalo s ove ili s one strane routera. Možemo, znači, na klijentu Win10Ent1 iskoristiti naredbe Map network drive ili Net use i putanjom \\servertst1\docs spojiti se na share Docs servera. Niža slika nam pokazuje da je klijentsko računalo NetBIOS imenu cilja dodalo primarni DNS sufiks i upitalo DNS koja je IP adresa tog računala. Potom se računala dogovaraju o prijenosu podataka (TCP i SMB handshake); uočite da je port cilja TCP 445.

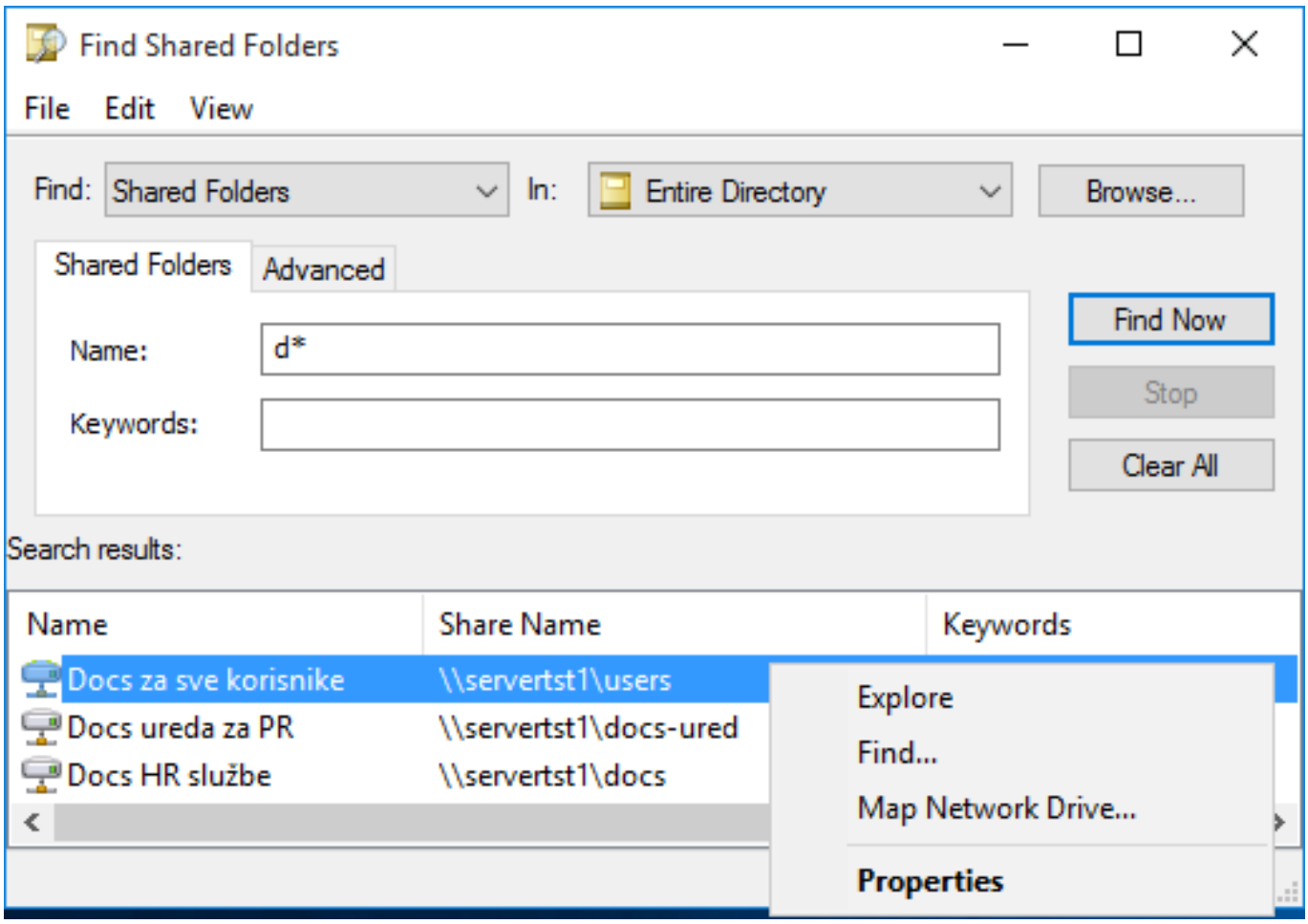
No.	Source	Destination	Protocol	Length	Info
675	.127	.139	DNS	78	Standard query 0x02f1 A servertst1.corp.hr
676	.139	.127	DNS	94	Standard query response 0x02f1 A 101.5.47.
677	.127	.55	TCP	66	49872→445 [SYN, ECN, CWR] Seq=0 Win=8192 Len
678	.55	.127	TCP	66	445→49872 [SYN, ACK, ECN] Seq=0 Ack=1 Win=81
679	.127	.55	TCP	54	49872→445 [ACK] Seq=1 Ack=1 Win=1051136 Len=
680	.127	.55	SMB	213	Negotiate Protocol Request
681	.55	.127	TCP	60	445→49872 [ACK] Seq=1 Ack=160 Win=131328 Len
682	.55	.127	SMB2	306	Negotiate Protocol Response
683	.127	.55	SMB2	166	Negotiate Protocol Request
684	.55	.127	SMB2	306	Negotiate Protocol Response
685	.127	.55	SMB2	1884	Session Setup Request
686	.55	.127	TCP	60	445→49872 [ACK] Seq=505 Ack=2102 Win=131328
687	.55	.127	SMB2	315	Session Setup Response
688	.127	.55	SMB2	164	Tree Connect Request Tree: \\servertst1\docs

Gornji primjer nam sugerira da se u stvari transparentno rabe DNS imena. U ispravno podešenom DNS-u te, dakako, Windows računalu, tajna je nesmetane uporabe dijeljenih resursa na Windows mreži sa disabliranim NetBIOS protokolom.

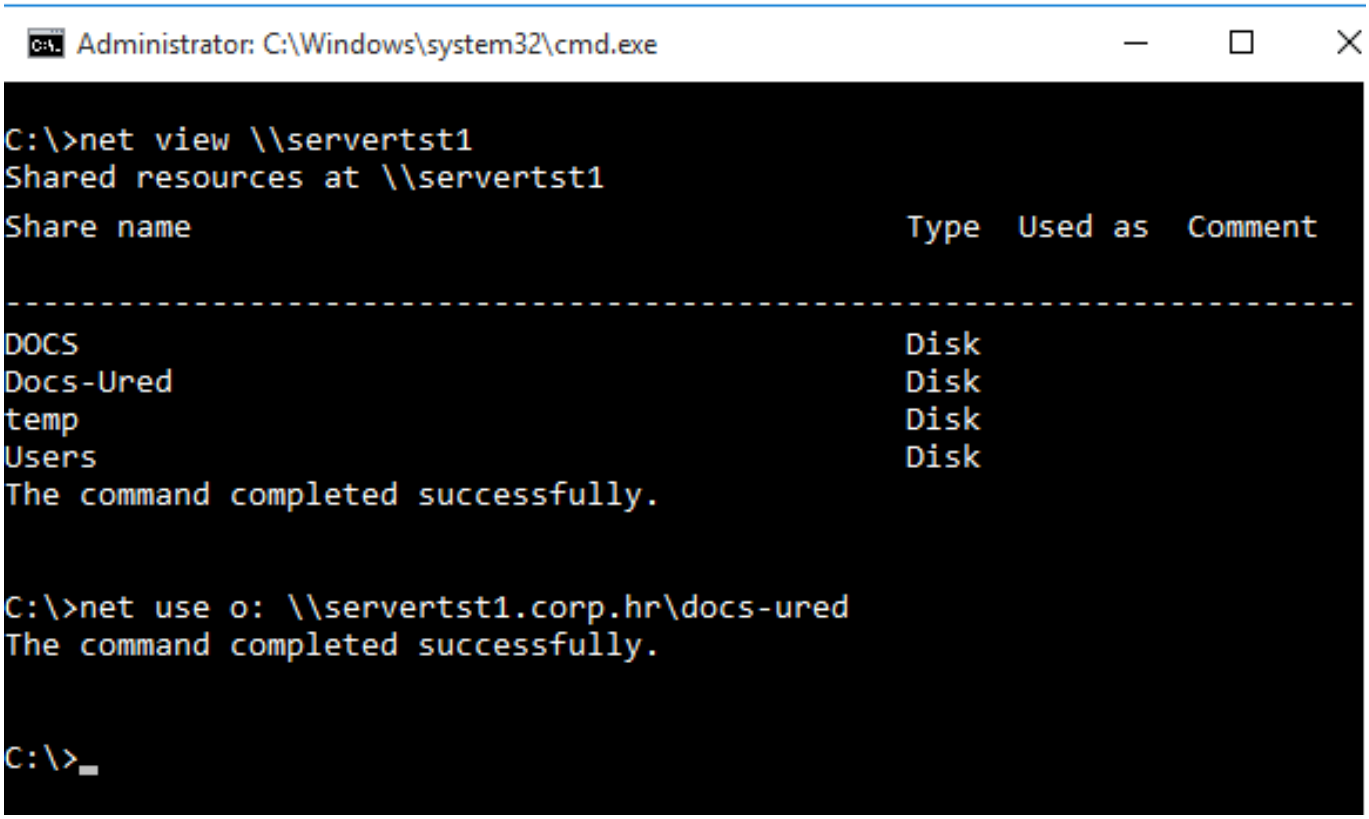
Pogledajte kako možemo, posredstvom naredbe Run, rabeći samo NetBIOS ime cilja, vidjeti sve dijeljene mape na računalu Servertst1 a potom se, dakako, spojiti na ciljnu mapu: nakon zadnjeg backslasha pričekamo sekundu – dvije i pojavit će se popis dijeljenih mapa kojima je taj server domaćin.



Što ako ne znamo ime ciljnog servera? Prisjetimo sa da Active Directory, „prirodno stanište“ Windows računala, omogućuje oglašavanje dijeljenih mapa i pisača. Rabeći maloprije spomenutu naredbu Search Active Directory (na kartici Network unutar preglednika Network, a dade se i postaviti na Desktop), možemo pristupiti bilo kojem domenskom dijeljenom resursu, kako to radimo na nižoj slici.



Naravno, pristup dijeljenim resursima možemo riješiti i raznim shortcutima, skriptama i sličnim tehnikama. Korisnicima su takva rješenja najpraktičnija jer imaju pripremljenu radnu okolinu. Niže je primjer uporabe NET* naredbi iz komandne linije, kako vidimo, i nakon disabliranja NetBIOS-a možemo se njima okoristiti, rabeći pritom i kratka i dugačka imena računala.

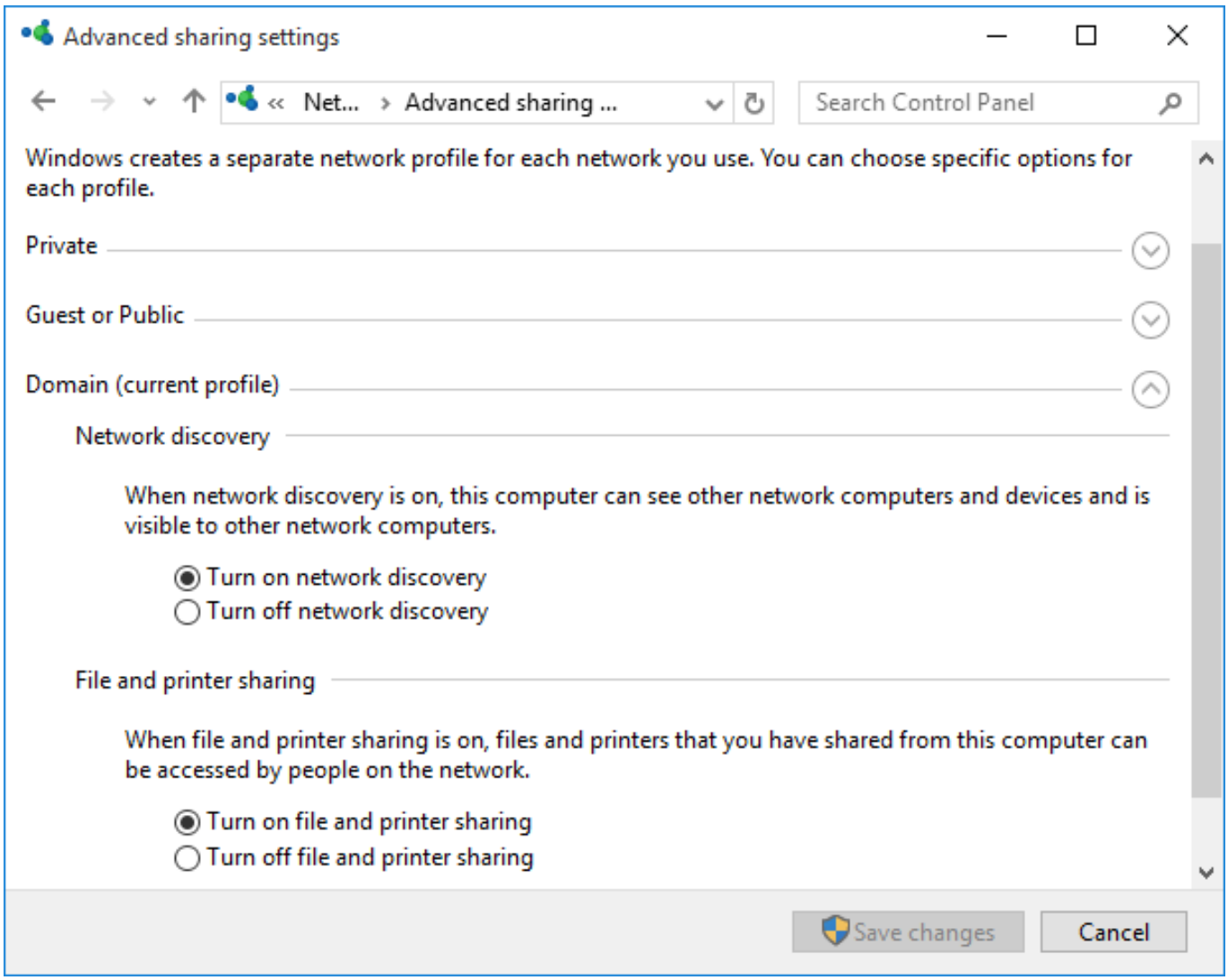


Kako stojimo s routanim LAN-om po kojem su raspršena domenska i nedomenska Windows računala, k tomu sa onemogućenim NetBIOS protokolom? U toj situaciji je neizbježna uporaba FQDN imena, posljedično, jako je važno znati ispravno podesiti ne samo DNS servere nego i DNS postavke na Windows računalima, posebno se to odnosi na sufikse pretraživanja i automatsko prijavljivanje u DNS. U ovoj situaciji korisnici upadaju u probleme, jasno, ako ih mi sistemci nismo pravovremeno educirali ili im pripremili radno okruženje.

U složenijim tehnološkim okolinama (više foresta, nepovezane interne DNS hijerarhije, postojanje NetBIOS aplikacija) resolving imena računala možemo unaprijediti primjenom GlobalNames DNS zona; samo spominjem jer ta tema probija okvir ovog članka, jednako kao obrada banalnosti poput uporabe lokalne Hosts za resolving.

Kad mi sistemci postajemo problem? Ne ovladamo li finesama Windows mreže u mjeri dovoljnoj da radna sredina o kojoj brinemo – i ljudi i računala i servisi - bezbolno nastavi obavljati svoje posliće bez NetBIOS protokola, e, tada smo mi problem, a ne „te gluuupe windoze“. Brzopletim ukidanjem NetBIOS-a pojave se razne greške i nedoumice, krenu brzinska rekonfiguriranja svega i svačega, krene gunđanje... i situacija se riješava vraćanjem NetBIOS-a u igru jer „gle, bez njega ipak ne radi“.

Ako Windows računalo bez NetBIOS-a ne nudi ili odbija rabiti dijeljene resurse, osnovno je provjeriti Advanced sharing settings (vidi nižu sliku), TCP/IP postavke na mrežnoj kartici, stanje lokalnog vatrozida te, svakako, stanje lokalnih servisa. Dovoljno je zaustaviti „sada nepotreban“ servis TCP NetBIOS Helper da izazovemo gadan problem... Probajte!



Važno je upamtiti: NetBIOS over TCP/IP nije samo mrežni protokol za dijeljenje datoteka i mapa, na što smo se mi trenutno fokusirali; njegov je zadatak i registracija imena računala (i nekih njegovih servisa) na lokalnoj mreži, te prevođenje imena računala u IP adresu, štoviše, NetBIOS je i API za klijent/server aplikacije. Ukidanjem NetBIOS-a onemogućit ćemo rad aplikacija koje o njemu ovise. Tih aplikacija danas ima jako malo jer sam Microsoft odavno sustavno radi na zamjenjivanju NetBIOS-a modernijim tehnologijama, ali postoje. Načelno, što je infrastruktura složenija, potrebno je više planiranja i testiranja. No, uvijek se možemo opredijeliti za opciju selektivnog isključivanja NetBIOS-a, npr. na Windows instalacijama u DMZ, i sl.

Još par riječi o SMB protokolu, jer njime se prenose podaci između domaćina dijeljenih resursa i klijenata. Pouzdan je, robustan, čak i vrlo siguran jer od Windows Server 2012 / Windows 8 sav SMB promet možemo enkriptirati na domaćinu, deenkriptira se na klijentu. No, sigurnosno gledano, mnogo možemo postići i bez enkripcije ako u Local Security Policy windoza uključimo opcije:

Digitally sign communication (posebno za SMB server i SMB klijenta)
Do not allow anonymous enumeration of SAM accounts and shares
Restrict anonymous access to Named Pipes and Shares

Znači li to da ispravno podešena Windows računala mogu kombinacijom SMB + port 445 razmjenjivati podatke i preko Interneta? Dvije su prepreke: prva je ISP, koji po navici blokira SMB promet (defaultno je SMB promet onemogućen i na xDSL routerima), druga je brbljivost porta TCP 445, naime, on skenerima poput Nessusa isporuči informaciju o nekolicini RPC lokalnih servisa, zajedno sa imenom računala. Nessus, doduše, procjenjuje da je Risk factor = None, no zašto bismo potencijalnom napadaču davali bilo kakvu informaciju „na tacni“. Stoga je VPN pravo rješenje za

simpatizere metode „SMB-over-Internet“. Ali budimo realni - postoji bezbroj načina za dijeljenje datoteka i pisača preko Interneta, ne mora to biti baš SMB protokol.

pon, 2015-11-30 16:02 - Ratko Žižek**Kuharice:** Windows [1]
Kategorije: Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1586

Links
[1] https://sysportal.carnet.hr/taxonomy/term/18
[2] https://sysportal.carnet.hr/taxonomy/term/30