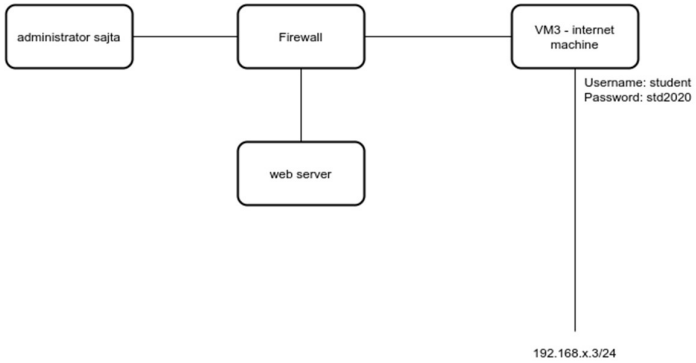
Заштита рачунарских система и мрежа
практични део испита – јун 2020

Компанија X има веб сајт преко кога води евиденцију о студентима неког факултета. Познато је да компанија X има додељен опсег адреса 10.0.2.0/24 и да користи *firewall* за заштиту интерне ИТ инфраструктуре за коју се претпоставља да изгледа као на слици. Познато је да администратор сајта ажурира исти из локалне мреже фирме врло често и периодично. Познато је да је администратор неискусан и да користи исте лозинке за приступ различитим системима.



Ви сте нападач чији је крајњи циљ да приступи рачунару администратора на интерној мрежи фирме. Имате могућност ssh и vnc приступа једном рачунару на интернету са адресом 192.168.x.3/24, са којег може да се изврши напад. Креденцијали за ssh приступ су student/std2020. Лозинка за vnc приступ је iblabvnc, а порт по којем се приступа 5901 (као на досадашњим лабораторијским вежбама).
Потребно је да урадите следеће:

1. Откријете адресу и порт на којем ради веб сервер, као и остале отворене портове на њему – 5 поена
2. Откријете корисничко име и лозинку за ssh приступ на веб сервер – 20 поена
3. Промените IP филтер на веб серверу тако да се омогући vnc логовање директно на веб сервер, али само са рачунара којим се приступа преко VPN (тако да се не иде кроз интернет рачунар) – 3 поена (vnc сервер је потребно стартовати командом vncserver)
4. Откријете адресу администраторовог рачунара – 2 поена
5. Откријете лозинку корисника admin на веб серверу – 10 поена.

Име и презиме студента: _____
Број индекса: _____

Питање	Одговор	Број поена
Адреса веб сервера:		
Портови који су отворени на веб серверу		
Корисничко име и лозинка за приступ веб серверу		
Промењен IP филтер (попуњава наставник)		
Адреса администраторовог рачунара		
Лозинка корисника admin		
УКУПНО		