CARNET

Metodologija provjere ranjivosti

CERT.hr-PUBDOC-2020-07-402

Sadržaj

1 Uvod

S ciljem unapređenja sigurnosti mreže i mrežom dostupnih servisa, CARNET poduzima različite akcije, između ostaloga i provjeru ranjivosti računalnih mreža članica CARNET-a. Provjera ranjivosti (engl. *vulnerability scanning*) je postupak u sklopu kojega se obavlja prikupljanje podataka o sigurnosnim problemima na računalima i drugim uređajima spojenima na Internet te uputama za njihovo uklanjanje. Cilj ovog dokumenta je opisati načine obavljanja provjere ranjivosti s posebnim osvrtom na uslugu Provjere ranjivosti koju CARNET nudi svojim ustanovama članicama.

2 Način provođenja provjere ranjivosti

Postupak provjere ranjivosti obuhvaća prikupljanje podataka o uređajima spojenima u pojedini segment mreže te njihovu kasniju interpretaciju s izradom odgovarajućeg izvještaja u kojemu su sadržane informacije o pronađenim sigurnosnim ranjivostima i preporukama za njihovo uklanjanje. Najčešće se za prikupljanje podataka koriste specijalizirani alati za provjeru ranjivosti (eng. *vulnerability scanneri*), računalni programi koji korištenjem različitih tehnika skeniraju uređaje u određenom IP rasponu mreže te na temelju tako prikupljenih podataka dolaze do informacija o topologiji i strukturi mreže, vrsti i tipu uređaja u mreži, inačici operativnog sustava uređaja, popisu otvorenih portova i sl. Prikupljenim podacima specijalizirani alati za provjeru ranjivosti pridružuje informacije o pronađenim ranjivostima, odnosno informacije o poznatim ranjivostima vezanima za određenu vrstu i tip uređaja, inačicu operativnog sustava, određeni TCP/UDP port i sl. te generira odgovarajući izvještaj.

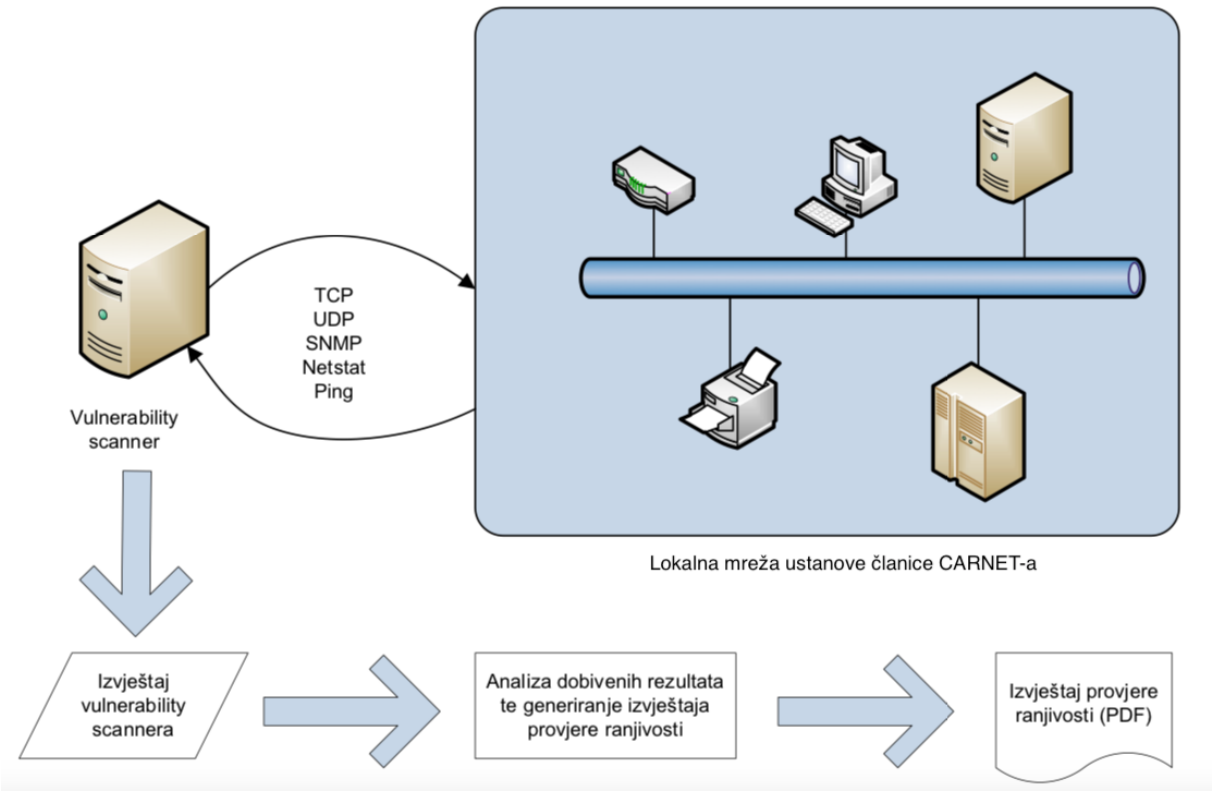
U postupku provjere ranjivosti računalne mreže Vaše ustanove korišten je Nessus® *vulnerability scanner*.

Nessus® je jedan od najpoznatijih alata za provjere ranjivosti (eng. *scanner)* koji putem skeniranja portova (eng. *portscan)* odnosno sondiranjem otvorenih portova računala iz pojedinog IP raspona, dolazi do informacija o pokrenutim servisima. U narednim koracima se, ovisno o konfiguraciji Nessusa® te podacima o vrsti i tipu pronađenih uređaja odnosno njihovih drugih značajki, provode dodatna testiranja kako bi se prikupili svi relevantni podaci o udaljenim uređajima odnosno utvrdilo postojanje određenih sigurnosnih ranjivosti. Nessus® trenutno podržava više od 140000 modula *(*eng. *plugin)* za otkrivanje različitih vrsta ranjivosti. Sam modul obično sadrži informacije o ranjivosti, uputu korisniku kako potvrditi postojanje određene ranjivosti te upute za uklanjanje iste.

3 O CARNET-ovoj usluzi provjere ranjivosti

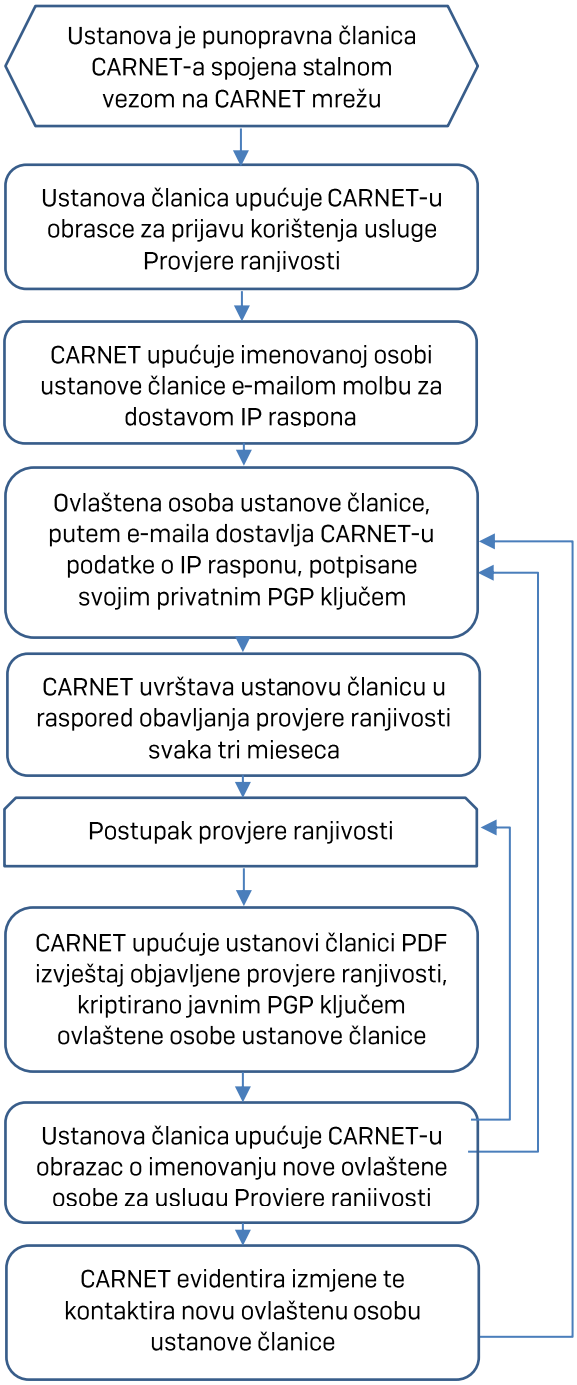
Usluga Provjere ranjivosti dostupna je svim punopravnim članicama CARNET-a, te je njezin cilj pomoći ustanovama članicama u uspješnijem održavanju lokalnih mreža i povećanju sigurnosti CARNET mreže u cjelini. Korištenjem usluge pojedina ustanova članica na periodičkoj bazi, u pravilu svaka tri mjeseca, dobiva PDF izvještaj o provjeri ranjivosti koji sadržava cijeli niz informacija o ranjivostima pronađenima na uređajima u IP rasponu koji joj pripada te načinima njihovog uklanjanja.

Sam postupak provjere ranjivosti, odnosno skeniranja mreže ustanove članice CARNET provodi korištenjem alata Nessus®, te po potrebi i drugih alata, uz izričitu pisanu suglasnost ustanove. Ustanova se prije svakog skeniranja obavještava o planiranom terminu skeniranja mreže ustanove. Nakon završenog skeniranja obavlja se analiza dobivenih rezultata nakon čega se generira PDF izvještaj koji sadrži sve relevantne informacije o obavljenom postupku provjere ranjivosti. Na ~~*Slika 1*~~*Slika 1* je shematski prikazan postupak obavljanja provjere ranjivosti.



Slika 1 Shematski prikaz postupka provjere ranjivosti

Kako bi ustanova članica postala korisnikom usluge Provjere ranjivosti, koju obavlja Nacionalni CERT, potrebno je prijaviti se za korištenje usluge pisanim putem tj. slanjem obrazaca poštom na adresu koja se nalazi na web stranici[1], odnosno pri dnu obrasca. U obrascu kojim se imenuje ovlaštena osoba za komunikaciju s Nacionalnim CERT-om potrebno je navesti ID PGP ključa ovlaštene osobe te se isti mora nalaziti na nekom od poslužitelja javnih ključeva (npr. http://hkps.pool.sks-keyservers.net). Oba obrasca moraju biti potpisana od strane zakonskog predstavnika ustanove (dekan ili ravnatelj) te ovjerena pečatom ustanove. Nakon prijave za korištenje usluge, imenovanoj osobi će se e-mailom uputiti molba za dostavom IP segmenta ustanove članice koje je potrebno podvrgnuti postupku provjere ranjivosti. Ovlaštena osoba šalje podatke e-mailom koji potpisuje svojim privatnim PGP ključem. Nakon dostave ovih podataka ustanova se uvrštava u planove obavljanja provjere ranjivosti, u pravilu, svaka tri mjeseca. Nakon svakog pojedinog postupka provjere ranjivosti generira se pripadajući PDF izvještaj koji se u šifriranom obliku (koristeći PGP) upućuje putem e-maila imenovanoj kontakt osobi.



Slika 2 Hodogram provjere ranjivosti

Ovlaštena osoba ustanove članice može u bilo kojem trenutku dostaviti promjenu podataka o IP rasponima slanjem e-maila potpisanog svojim privatnim PGP ključem. Promjena PGP ključa moguća je isključivo pisanim putem uz potpis zakonskog predstavnika ustanove te ovjereno pečatom ustanove. Ustanova članica dužna je obavijestiti CARNET o promjeni ovlaštene osobe za usluge Provjere ranjivosti pisanim putem tj. slanjem obrasca o imenovanju poštom.

[1] https://www.cert.hr/provjera_ranjivosti/carnet_provjera_ranjivosti/

4 Zaključak

Bitno je imati na umu da je briga o sigurnosti bilo kojeg IT sustava kontinuirani proces, te je stalno nužno ulagati energiju kako bi se ta sigurnost održala na zadovoljavajućoj razini. Korištenje usluge Provjere ranjivosti te primjenom preporučenih postupaka za uklanjanje uočenih ranjivosti je jedan od koraka na ovom putu. Trenutkom izrade izvještaja Provjere ranjivosti on je već na određeni način zastario. Naime, s obzirom na brz i strelovit razvoj informatičke industrije, svakodnevno dolazi do pojave novih ranjivosti, te je uvijek iznova potrebno osmišljavati nove načine za zaštitu informacija i sustava. Briga o sigurnosti IT infrastrukture je kontinuirana aktivnost koju nikada ne možemo smatrati završenom.

5 Literatura

1) Javni web CARNET-a – provjera ranjivosti: http://www.carnet.hr/provjera_ranjivosti/ustanove_clanice (srpanj, 2020.)

2) Informacije o Nexpose-u: https://www.rapid7.com/products/nexpose/ (srpanj, 2020.)

3) Wikipedija – *vulnerability scanner*: http://en.wikipedia.org/wiki/Vulnerability_scanner (srpanj, 2020.)

4) Popis popularnih *vulnerability scannera*: http://sectools.org/vuln-scanners.html (srpanj, 2020.)

5) Popis web *vulnerability scannera*: http://sectools.org/web-scanners.html (srpanj, 2020.)