Dnevnik rada

1. tjedan (9.4.2018 - 16.4.2018.)

Dosadašnji rad

Dogovoren sastanak sa asistentom. Proučio sam kako se rade “Access Pointovi” preko androida.

Daljnji koraci

Na sastanku se dogovoriti koji bi bio radni plan.

---

2. tjedan (26.3.2018 - 2.4.2018.)

Dosadašnji rad

Na sastanku se dogovorio sa asistentom da ću za početak napravirti open-vpn server na debianu u virtualnoj mašini. Uspio sam to napraviti uz manje probleme.

Daljnji koraci

Spojiti se preko android uređaja na server te riješiti problem sa spajanjem preko javne ip adrese.

---

3. tjedan (2.4.2018. - 9.4.2018.)

Dosadašnji rad

Uspio sam se spojiti na server preko android uređaja koristeći aplikacije OpenVPN Connect i SSHJuice. Server sam napravio koristeći tutorial https://www.cyberciti.biz/faq/how-to-install-and-configure-an-openvpn-server-on-debian-9-in-5-minutes/. Također sam morao forwardirat port 1194. Također kako ne bih stalno morao mijenjati postavke servera i mijenjati postavke routera zbog javne dinamičke IP adrese koristio sam dinamički dns preko kojeg sam napravio domenu koja će uvijek poazivati na moju javnu IP adresu. https://www.noip.com/remote-access.

Daljnji koraci

Ostvariti slanje mrežnog prometa sa androida na open-vpn server.

4. tjedan (9.4.2018. - 16.4.2018.)

Dosadašnji rad

Par grešaka se ostvarilo ovaj tjedan. Naime mogu dobiti ssh pristup računalu preko mobitela, ali ne mogu ići na internet preko mobitela kada sam spojen na openVPN server. Nakon čitanja raznih foruma te mijenjanja postavka firewalla, mijenjanja konfguracijskih datoteka openVPN-a (server.conf, client.ovpn) nisam uspio rijepiti problem. Uspio sam si samo “pokvariti” debian te više ne mogu na internet s njim te nakon pokušaja na Linux Mintu koji nije na VirtualBoxu ni na njega se više nisam u mogućnosti spojiti. Ovaj tjedan još probati riješiti problem, ukoliko ne pitati asistenta.

Daljnji korac

Riješiti problem.

5. tjedan (16.4.2018. - 23.4.2018.)

Dosadašnji rad

Problem je uspješno riješen. Server radi, preko mobitela se može spojiti na njega te se ima pristup internetu. No prilikom spajanja žrtve iliti drugog Android uređaja ili računala, on nema pristup internetu. Nakon istraživanja saznao sam da Android bez rootaima zaštitu za slanje podataka. Naime ako je uređaj spojen na VPN server te se na njega preko hotspota, žice ili bluetootha spoji žrtva, Android neće podatke proslijeđivat VPN serveru iz sigurnosnih razloga.

“”Android does not allow tethered devices access to the VPN tunnel. This is a deliberate choice forced by Android for security reasons. For instance, when using VPN to access your employer’s network, they might not want your friends and family there. Also a VPN tunnel shared with others wouldn’t really be a private network anymore”

https://safeandsavvy.f-secure.com/2016/09/23/how-to-create-a-portable-hotspot-on-android-with-vpn-on/

Također sam naišao na github raspravu u kojoj su također pokušali zaobići navedenu zaštitu no nisu uspjeli.

https://github.com/schwabe/ics-openvpn/issues/34

Daljni koraci

Pisati rad te se javiti asistantu za daljnje upute.

6./7. tjedan - Međuispiti

---

8. tjedan (7.5.2018. - 14.5.2018.)

Dosadašnji rad

Pisanje samog rada do trenutka do kojeg sam došao. Trenutno imam 22-ije stranice ukupno. Sastao sam se s asistentom koji je rekao da napišem rad do kud sam stigao te mi je dao ideju za drugačiji napad. Ideja je da napravim DNS server na koji ću se spojiti preko Android uređaja te kada se žrtva spoji na moj Android uređaj preusmjeravat će se na odabrane IP adrese koje sam naveo pri postavkama DNS servera.

Daljni koraci

Napraviti DNS server, testirati metodu te napisati do kraja završni rad.

---

9. tjedan (9.12.2017. - 16.12.2017.)

Dosadašnji rad

Uspio sam riješiti problem od prošlog puta. Wininetd radi normalno bez definiranog usera. Kod stavljanja usera u wininetd.config te pokretanja wininetd-a javljao se error. Jedan od errora sam uspio riješiti tako da sam debuggiro wininetd.c,našao grešku koja se javlja pozivom funkcije LogonUserA te nakon proučavanja greške na internetu našao riješenje. Naime u Windowsima treba otići u Local Security Policies (Start → Run → secpol.msc → Local Policies → User Rights Assignment → Log on as batch job) te dodati usera kojeg smo upisali u konfiguracijskoj datoteci u Log on as batch job. Nakon toga pojavila se nova greška ([wininetd] unable to create process as user: cmdln='c:\pr.exe' user='Roko' err='A required privilege is not held by the 'lient.) Nakon mnogo googlanja i debuggiranja nisam uspio otrkiti problem te sam se obratio mentoru.

Daljni koraci

Čekati odgovor mentora te nastaviti dalje prema njegovim uputama.

---

10. tjedan (16.12.2017. - 23.12.2017.)

Dosadašnji rad

Uz mentorovu pomoć, dosta googlanja i debuggiranja uspio sam riješiti problem od prošlog puta. Razlog pogreške je poziv funkcije *CreateProcessAsUserA* u wininetd.c datoteci. Greška koju Windowsi bacaju je **ERROR_PRIVILEGE_NOT_HELD A required privilege is not held by the client**. Na na linku https://msdn.microsoft.com/en-us/library/windows/desktop/ms682429 koji mi je proslijedio mentor piše sljedeće : *CreateProcessAsUser function must have the **SE_INCREASE_QUOTA_NAME** privilege and may require the **SE_ASSIGNPRIMARYTOKEN_NAME** privilege if the token is not assignable*. Riješenje sam našao na sljedećem linku: https://stackoverflow.com/questions/1475577/createprocessasuser-error-1314 . Naime, uz dodavnje usera u security policies → **Logon as batch job**, također treba usera ili grupu usera dodati u Local

Policies → User Rights Assignement → **Replace a process level token**. Nakon dodavanja usera (u mojem slučaju Roko) wininetd radi te uspjevam pristupiti servisu sa drugog računala.

Daljni koraci
Napraviti više usera kojima ću dati različite ovlasti za pristupanje određenim datotekama te pokušati pristupiti datotekama sa drugog računala.

---

11. tjedan (23.12.2017. - 30.12.2017.)

Dosadašnji rad
Za početak sam dodao dva usera : User1 i User2. To sam učinio na sljedeći način. Pokrenuo sam run.exe preko starta te upisao **lusrmgr.msc** nakon čega sam stisnuo Ok. Otvorio se prozor **Local Users and Groups.** Nakon toga sam kreirao dva usera tako što sam odabrao Users, desni klik na prazan prostor te New User. Odabrao sam username i password te spremio oba usera. Zatim sam na isti način napravio novu grupu koju sam nazvao Projekt u koju sam dodao oba usera. Nakon toga sam otišao u Security Policies te dodao grupu u **Logon as a batch job** i u **Replace a process level token**. Nakon toga sam napisao program u c-u koji prima put do određene datoteke te na stdin ispisuje njen sadržaj. Program sam dodao u wininetd.conf sa dva različita usera na sljedeći način:

202 User1:1234 c:\program.exe
203 User2:12345 c:\program.exee

Zatim sam napravio dvije tekstualne datoteke različitog sadržaja i imena (user1.txt, user 2.txt). Korisniku User1 dao sam dozvolu da pročita datoteku user1.txt, a onemogućio da pročital ili piše u datoteku user2. Obrnuto sam napravio za Usera2. Navedeno sam napravio na sljedeći način. Desni klik na user1.txt, klik na Security tab te klik na edit. Tu sada klikom na određenog usera promijeniti ovlasti koje ima nad tom datotekom. Nakon pokretanja wininetd-a te spajanjem na određeni port (recimo npr. 202) sa drugog računala zaista mogu pročitati što se nalazi u datoteci user1, a ne mogu pročitati što se nalazi u datoteci user2.

Moj zadatak je uspio.

---

12. tjedan (30.12.2017. - 6.12.2017.)

Dosadašnji rad
Napravljene su i postavljene kompletne upute sa slikama na mojoj stranici http://studentski-izvjestaji.zesoi.fer.hr/lib/exe/fetch.php?media=studenti:roko_grubelic:pokretanje_izoliranih_ranjivih_mreznih_servisa_na_windows_serveru_za_ctf_zadatke.pdf

Otvorio sam github account, napravio novi repozitorij u koji sam stavio svoj program koji prima put do datoteke i njen sadržaj ispisuje na stdout te kompletne upute na engleskom kako se koristi wininetd na Windowsima. https://github.com/rockymus/wininetd