Dnevnik rada

1. tjedan (10.10.2017. - 17.10.2017.)

Dosadašnji rad

Održađen prvi sastanak sa mentorom i asistentima te dobivena tema “Pokretanje izoliranih ranjivih mrežnih servisa na Windows serveru za CTF zadatke”. Proučio sam malo više o tome te sam razgovarao sa jednim od asistenata kako ću realizirati zadanu temu i dogovorio za sastanak uživo kako bi mi razjasnio sve nejasnoće.

Daljnji koraci

Do sastanka (koji je u petak) proučiti zadatak koji mi je poslao asistent te proučiti sve nejasne elemente zadatka. Pronaći par sličnih zadataka te ih probati riješiti.

---

2. tjedan (17.10.2017 - 24.10.2017.)

Dosadašnji rad

Proučio sam zadatak koji mi je poslao asistent te ga uspio riješiti. Proučio sam python kod te shvatio kako funkcionira. Nije mi bilo jasno kako prokrenuti program kao servis na windowsu.

Na sastanku s asistentom shvatio sam poantu zadatka te me uputio što i kako dalje.

Daljnji koraci

Proučiti programe Inetd, XInetd te WinInetd koji omogučuju internet servise te za svaki konfigurirani servis “slušaju” zahtjeve korisnika koji se povezuju.

---

3. tjedan (24.10.2017. - 31.10.2017.)

Dosadašnji rad

Naučio sam raditi sa programima inetd te xinetd te kako staviti određeni program na mrežu tako da ostali korisnici koji su spojeni na tu mrežu mogu pristupiti tom programu. Najviše sam se mučio sa shvaćanjem kako konfigurirati xinetd.config u kojem se treba upisati ip adresa, port, protokoli itd., ponajviše zato što još nisam bio upoznat sa svim navedenim jer komunikacijske mreže imam tek ovaj semestar. Za sada sam radio na kali linuxu.

Daljnji koraci

Prebaciti se na Windows te probati istu stvar. Pitati asistenta te proučiti kako napraviti izolirani sustav.

---

4. tjedan (31.10.2017. - 7.11.2017.)

Dosadašnji rad

Isprobao WinInetd te se dogovorio sa asistentom kako raditi implementirani sustav. Ideja je sljedeća. Staviti rješenja dva različita zadatka u dvije tekstualne datoteke sa ovlastima za dva različita korisnika. Time bi osigurali da korisnik koji riješi jedan zadatak ne može pročitati rješenje drugog zadatka niti ga brisati/modificirati.

Daljnji korac

Pokušati sve gore navedeno napraviti sa WinInetd-om koji bi u konfiguraciji trebao imati podršku za korisnike.

---

5. tjedan (7.11.2017. - 14.11.2017.)

Dosadašnji rad

Napisan plan projekta i predan na fer web.

Daljni koraci

Poslje međuispita izvesti sve navedeno u 4. tjednu.

6./7. tjedan - Međuispiti

---

8. tjedan (2.12.2017. - 9.12.2017.)

Dosadašnji rad

Proučio sam kako pisati konfiguracijski file wininetd.conf. Uspio sam pokrenuti servis wininetd koji je vidljiv u Task Manageru. Napravio sam jednostavan program (program.exe, ispisuje sa stdina na stdout) na kojeg cu se pokušati spojiti sa drugog računala. Dao sam mu port za kojeg sam prije toga provjerio je li slobodan sa netstat-om. Kada pokrenem wininetd –debug, uspije ga staviti na mrežu. Tu sam imao problem jer wininetd u konfiguracijskom file-u prilikom dodjele puta do datoteke program.exe iz nepoznatih razloga izbriše zadnji znak te se u konfiguracijsku datoteku mora dodati još

jedan znak na kraj kako ne bi došlo do pogreške (c:\program.exee → c:\program.exe). Na istom računalu sa drugog terminala naredbom nc (netcat) koja kao parametre prima IP adresu i port zadajem vlastitu IP adresu (ipconfig) te unaprijed određeni port. Sa terminala na kojem je pokrenut wininetd –debug se vidi da se klijent spojio sa određenom ip adresom i portom, ali na klijentskom računalu (netcat) se ne pokreće zadani program odnosno ne ispisuje ono što bi trebalo.

Daljni koraci

Probati na kućnoj mreži istu stvar sa dva različita računala. Riješiti problem na koji sam naišao. Ukoliko ne uspijem, javiti se asistentu.

---

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

From:
http://studentski-izvjestaji.zesoi.fer.hr/ - **Studentski izvještaji**

Permanent link:
http://studentski-izvjestaji.zesoi.fer.hr/doku.php?id=studenti:roko_grubelic:rg_dnevnik&rev=1515606979

Last update: **2023/06/19 16:20**