
ETIČKO
HAKOVANJE

ŠTA JE ETIČKO HAKOVANJE ?

- Etičko hakovanje odnosi se na legalno i dobroćudno prodiranje u računarske sisteme kako bi se testirala njihova bezbednost i eventualno otkrile ranjivosti.
- To je ustvari radnja koju sprovodi stručnjak u oblasti IT tehnologija, specijalista za računarsku bezbednost koji svojom aktivnošću vrši ocenu koliko je vaša kompanija izložena rizicima, koliko je ranjiva i otporna - detektuje ranjivosti i greške u sistemu, uređaju ili bilo kom programu.

White Hat (Etički) hakeri

- White Hat hakeri su stručnjaci za informacionu bezbednost koji koriste svoje znanje i veštine kako bi pomogli organizacijama u zaštiti svojih informacionih sistema. Oni sarađuju sa vlasnicima sistema kako bi pronašli i otklonili ranjivosti, pre nego što to učine zlonamerni napadači. Etički hakeri često koriste metode i alate slične onima koje koriste "black hat" hakeri, ali njihov cilj je poboljšanje bezbednosti, a ne eksploatacija ranjivosti.

Organizacije širom sveta angažuju white hat hakere kako bi testiralei svoje sisteme i aplikacije i, kako bi se osiguralei da su njihovi podaci i korisnici zaštićeni. Etičko hakovanje obuhvata različite aspekte kao što su:

- **Testiranje proboja (penetration testing):** Ovo podrazumeva simulaciju napada na računarske sisteme kako bi se identifikovale ranjivosti i preporučile odgovarajuće mere zaštite.
- **Revizija bezbednosti:** Etički hakeri procenjuju politike i procedure organizacija kako bi osigurali da su one u skladu sa standardima industrije i zakonodavstvom.
- **Obuka i svest o bezbednosti:** Etički hakeri često obučavaju zaposlene u organizacijama kako bi ih naučili da prepoznaju i izbegnu potencijalne pretnje, kao što su phishing napadi.

Black Hat (Neetički) hakeri

- **Black Hat hakeri su pojedinci koji se bave neovlašćenim prodiranjem u računarske sisteme i mreže, sa ciljem krađe, sabotaže ili iznuđivanja. Oni koriste svoje veštine za ličnu korist, bez obzira na štetu koju mogu naneti drugima. Black hat hakeri često koriste sofisticirane alate i tehniku kako bi ostali neotkriveni i ostvarili svoje zlonamerne ciljeve. Neki od najčešćih ciljeva black hat hakera uključuju:**

- **Krađa podataka:** Black hat hakeri često ciljaju organizacije kako bi ukrali osetljive informacije, kao što su finansijski podaci, lični identifikacioni podaci ili korporativne tajne.
- **Finansijske prevare:** Nelegalno pristupanje bankovnim računima, kreditnim karticama ili drugim finansijskim instrumentima kako bi se preusmerila sredstva ili izvršile neovlašćene transakcije.
- **Ransomware:** Ovo je zlonamerna vrsta softvera koji šifruje podatke žrtve i zahteva otkupninu kako bi se podaci oslobodili. Black hat hakeri često koriste ransomware kako bi iznudili novac od pojedinaca ili organizacija. Jedan od primera ransomware napada je bio napad na Republički Geodetski Zavod sredinom prošle godine.
- **Distribuirani napadi odbijanja usluge (DDoS):** Ovi napadi se koriste za preopterećenje mrežnih resursa ili usluga, što može dovesti do pada sistema ili mreže. Cilj ovih napada može biti nanošenje štete konkurenciji, iznuđivanje ili aktivizam.

ETIČKO HAKOVANJE KAO PROFESIJA

- Dok se etičko hakovanje uvek ne smatra "glamuroznom" karijerom, ono nudi mnoge mogućnosti za stručnjake iz oblasti informacione bezbednosti. Etički hakeri mogu raditi kao konsultanti, zaposleni u korporacijama ili čak kao članovi vladinih agencija. Industrija informacione bezbednosti brzo raste, a potražnja za etičkim hakerima se povećava kako se organizacije sve više oslanjaju na tehnologiju i internet.