禪

مقدمه دوره رایگان CEH

آموزش رایگان دوره CEH V10: چگونه هکر کلاه سفید شویم

~~Hacker~~
Ethical Hacker
CEH

مبحث امنیت و هک یکی از داغترین موضوعات دنیای فناوری است که فرصتهای شغلی متعدد و دستمزد خوبی عاید متخصصان میکند. البته در برخی موارد متخصصان حوزه شبکه دستمزدهای بیشتری دریافت میکنند . با این حال، آشنایی با روشهای شناسایی بدافزارها و رخنههای یک سیستم کمک میکند ضعفهای سامانهای که از آن استفاده میکنید را شناسایی کنید و در حالت ایدهآل شغلی در یک سازمان یا شرکت بزرگ پیدا کنید . برای تبدیل شدن به یک هکر کلاه سفید چه کاری باید انجام دهیم؟ آیا در مورد دوره CEH اطلاعی دارید؟

چگونه یک هکر کلاه سفید شویم؟

روشهای مختلفی برای تبدیل شدن به یک هکر کلاه سفید وجود دارد، اما استانداردترین و قانونیترین روشی که پیش روی شما قرار دارد یادگیری مباحث منطبق با دورههای بینالمللی است . دورههای مختلفی برای آموزش مباحث امنیت وجود دارند که تقریبا هر یک پیشنیاز دوره دیگری است . بهطور مثال، شخصی که دوست دارد یک هکر شود، در ابتدا باید دورههای Network+ و Security+ را گذارنده باشد، زیرا بخش اعظمی از مباحث مربوط به هک مرتبط با مباحث شبکه هستند و اگر به درستی ندانید DHCP، DNS، آدرس آیپی چیست، شبکههای بیسیم چه هستند و... به توفیق چندانی نمیرسید . دوره Security+ به این دلیل نیاز است که دانشجو باید با مباحث تئوری امنیت آشنا باشد و بداند بدافزار چیست، باجافزار چیست، نفوذ به چه معنا است و...

بیشتر مباحث دوره سکوریتی پلاس جنبه تئوری دارند و در حقیقت پیشنیازی برای دوره حرفهایتر گواهی

هک اخلاقی (**CEH**) سرنام Certified Ethical Hacker هستند. در کنار **CEH** دورههای امنیتی دیگری به شرح زیر وجود دارند :

- ISC2-CISSP
- پکیج (Security+, CEH, CISSP)
- Offensive Security-PWK - Penetration Testing with Kali Linux
- EC-Council-CHFI: Computer Hacking Forensics Investigator
- EC-Council-ECSA: EC-Council Certified Security Analyst
- SANS-SANS SEC، ISACA-CISM: Certified Information Security Manager
- (CSIRT)
- GCIH: GIAC Certified Incident Handler
- SANS-SANS SEC 487 (OSINT)

هر یک از این دورهها مباحث مختلف امنیت را آموزش میدهند . جالب آنکه سیسکو نیز دورههای امنیتی مختلفی دارد که در فهرست یاد شده به آنها اشاره نکردیم .

پیشنیاز سومی که کمک میکند در حوزه امنیت موفق شوید تسلط بر یک زبان برنامهنویسی است . در برخی موارد لازم است اسکریپتهایی بنویسید یا برخی از دستورات را به شکل برنامه آماده کنید یا در حالت عالیتر به عنوان یک متخصص شناسایی آسیبپذیریهای مستتر در نرمافزارها در یک شرکت مشغول به کار شوید. تسلط بر یک زبان برنامهنویسی به شما کمک زیادی میکند . شما میتوانید هر زبانی را به عنوان پایه کار خود انتخاب کنید، اما صحبت فوق نباید اینگونه تعبیر شود که اگر زبان کوتلین یا زبان آر را یاد گرفتهام دیگر مشکلی در این زمینه ندارم . باید زبانی انتخاب کنید که بتوانید در صورت لزوم به شکل کاربردی در زمینه امنیت از آن استفاده کنید . بیشتر کارشناسان زبان پایتون را پیشنهاد میدهند که ساده است و قابلیتهای مختلفی دارد، البته به شخصه و با توجه به اینکه سی پلاسپلاس اولین زبانی بود که به شکل جدی از آن استفاده کردم، سیپلاسپلاس را ترجیح میدهم .

دوره **CEH** چیست؟

دوره **CEH** یا هکر اخلاقمدارد (قانونمند) یکی از معتبرترین دورههای آموزش نفوذ و تست نفوذ است که شرکت EC-Council آنرا ارائه میکند . در این دوره مباحثی همچون تست نفوذ به شبکه و امنیت شبکه بررسی میشود. این دوره به افراد آموزش میدهد که چگونه از ابزارها و روشهایی که هکرها برای نفوذ به سامانهها استفاده میکنند برای شناسایی ضعفها و آسیبپذیریهای سیستمی استفاده کنند و به شرکتها در بهبود مکانیزم امنیت دفاعی کنند . به عبارت دقیقتر، اگر مباحث دوره **CEH** را به خوبی یاد بگیرید، به راحتی میتوانید یک شغل خوب در حوزه امنیت پیدا کنید . دوره **CEH** در آموزشگاههای مختلف به شکلهای مختلفی آموزش داده میشود که همراه با مباحث تئوری و عملی است . طول این دوره 40 تا 60 ساعت است و مدرس سعی میکند روش استفاده از ابزارهای مختلف را به دانشجو آموزش دهد . بهطور استاندارد، آموزشگاهها باید مجهز به آزمایشگاههایی باشند تا دانشجو به شکل عملی مباحث تئوری را روی سامانهها اجرا کند و بتواند بدون مشکل از تکنیکها و ابزارها برای شناسایی رخنهها استفاده کنند .

مطلب پیشنهادی

فهرست آموزشگاههای معتبر امنیت و شبکه در تهران

آموزشگاه های شبکه و امنیت شبکه در تهران + قیمت دورههای شبکه

[illegible]

[illegible]

[illegible] **CEH** [illegible]

[illegible] **CEH** [illegible] EC-Council [illegible] 1 [illegible] 600 [illegible] 40 [illegible] 60 [illegible] CEH 312-50 [illegible] CEH [illegible] 18 [illegible] 270 [illegible] 140 [illegible] 50-312 [illegible] 125 [illegible] 4 [illegible] 18 [illegible]

- Introduction to ethical hacking
- Footprinting and reconnaissance
- Scanning networks
- Enumeration
- System hacking
- Malware threats
- Sniffing
- Social engineering

- Denial of service
- Session hijacking
- Hacking web servers
- Hacking web applications
- SQL injection
- Hacking wireless networks
- Hacking mobile platforms
- Evading IDS, firewalls, and honeypots
- Cloud computing
- Cryptography

[illegible]

[illegible] 2026 [illegible] 28 [illegible] 7 [illegible] 2017 [illegible] 95 [illegible].

[illegible]



IT [illegible]

[illegible]

[illegible] **CEH** [illegible]

[illegible] Windows server 2019 [illegible] Network+ [illegible] Python [illegible] **CEH** [illegible] **10** [illegible] **CEH** [illegible]:

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible]
5. [illegible]
6. [illegible]
7. [illegible]
8. [illegible]
9. [illegible]
10. [illegible]

11. [illegible]
12. [illegible]
13. [illegible]
14. [illegible]
15. [illegible] (EISA)
16. [illegible]
17. [illegible]
18. [illegible]
19. [illegible]
20. [illegible]
21. [illegible]
22. [illegible]
23. [illegible]
24. [illegible]
25. [illegible]
26. [illegible] (HIPAA)
27. [illegible] Sarbanes Oxley (SOX)
28. [illegible] WHOIS، DNS [illegible]
29. [illegible] TCP [illegible] TCP، [illegible] SoftPerfect [illegible] Nmap، [illegible] NetBIOS، [illegible]
30. [illegible] NSLookup [illegible] DNS [illegible] SNMP، LDAP، NTP، SMTP [illegible]
31. [illegible]
32. [illegible]
33. [illegible] Sniffing [illegible]
34. [illegible] DHCP [illegible] MAC [illegible] DHCP (DHCP) [illegible] DHCP [illegible] DHCP [illegible] DHCP [illegible] ARP [illegible] ARP [illegible] DNS [illegible] DNS [illegible] Wireshark [illegible] DNS
35. [illegible]
36. [illegible]
37. [illegible] Kali Linux [illegible] DoS / DDoS [illegible] DoS / DDoS [illegible] DoS / DDoS
38. [illegible] OSI [illegible]
39. [illegible] ARP ، ICMP [illegible] TCP / IP [illegible] Spoofing، UDP [illegible] IPSec [illegible]
40. [illegible] SSH، [illegible]
41. [illegible]
42. [illegible] IIS [illegible] DoS / [illegible] DDoS، [illegible] DNS

43. [illegible] DNS [illegible]
44. [illegible]
45. [illegible] SQL [illegible] SQL [illegible] SQL [illegible]
46. [illegible] Wi-Fi [illegible] WEP [illegible] WPA [illegible] WPA2 [illegible] Wi-Fi [illegible]
47. [illegible] OWASP [illegible] 10 [illegible] iOS [illegible] (MDM) [illegible] BYOD [illegible]
48. [illegible] (IoT) [illegible] IoT [illegible] 10 [illegible]
49. [illegible]
50. [illegible] Cloud Computing [illegible] NIST Cloud [illegible]
51. [illegible] Sniffing Network [illegible] XSS Attack [illegible] Session Riding [illegible] (DNS) [illegible]
52. [illegible]
53. [illegible] (DES) [illegible] (AES) [illegible]
54. [illegible] RC4 RC5 RC6 [illegible]
55. [illegible] RSA [illegible]
56. [illegible] Digest [illegible] (SHA) SSH (Shell Secure) [illegible]
(PKI) [illegible]
57. [illegible] (CA) SSL [illegible] TLS SSL ([illegible]) [illegible]

[illegible] **CEH** [illegible] [illegible] [illegible]

%D8%B4%D9%88%DB%8C%D9%85