

د ایتیکل هکینگ زده کړه!

Ketabton.com

لیکوال : رحمان علی 2024

- د ایتیکل هیکینگ بنسټیز مفاهیمو زده کړه؟
- د وسایلو او تخنیکونو په اړه معلومات؟
- د قانوني چوکاټونو او اخلاقي محدودیتونو پوهه؟
- د سیستمونو او شبکو امنیتي ازموینې زده کړه

لومړی : د ایتیکل هیکینگ بنسټیز مفاهیمو زده کړه؟

ایتیکل هیکینگ (اخلاقي هیکینگ) د سیستمونو او شبکو د زیانمنو ټکو موندلو لپاره قانوني او اخلاقي لارو چارو څخه کار اخیستل دي، څو د هغوی امنیت قوي شي. دلته د ایتیکل هیکینگ د بنسټیزو مفاهیمو لپاره یو ساده لارښود دی:

۱. ایتیکل هیکینگ څه شی دی؟

ایتیکل هیکرز (چې "وايت هېټ" هیکرز بلل کېږي) د اجازې سره د شرکتونو یا سازمانونو سیستمونه او شبکې ازمويني. هدف یې دا دی چې زیانمن ټکي پیدا کړي مخکې له دې چې خرابکار هیکرز ورته لاسرسی ومومي.

۲. د ایتیکل هیکر اصلي مسؤلیتونه

- د زیانمنو ټکو (Weaknesses) موندل او راپور ورکول.
- د امنیتي بریدونو مخنیوي لپاره حللارې وړاندې کول.

- د امنیتي وسایلو لکه فایروال، انټي وایرس او نور آزموینه.
- د شبکې او سیستمونو لپاره د قوي امنیتي پالیسی جوړول.

۳. د ایتیکل هیکینگ اساسي مراحل

1. د اجازې ترلاسه کول: له مالک یا ادارې څخه رسمي اجازه ترلاسه کړئ.
2. د معلوماتو راټولول: د ټارگیت په اړه ټول اړین معلومات راټول کړئ (Reconnaissance).
3. د زیانمنو ټکو پیدا کول: د سکین کولو او نورو تخنیکونو څخه استفاده کول.
4. د زیانمنو ټکو ارزونه: هر زیانمن ټکی تحلیل کړئ او معلومه کړئ چې څومره خطرناک دی.
5. راپور ورکول: د موندل شویو ستونزو په اړه راپور چمتو کړئ او د حل لارې وړاندې کړئ.

۴. د ایتیکل هیکینگ لپاره مهم وسایل

- Nmap: د شبکې سکین کولو لپاره.
- Metasploit: د زیانمنو ټکو کارولو لپاره.
- Wireshark: د شبکې ټرافیک تحلیل لپاره.
- Burp Suite: د ویب اپلیکیشن امنیت آزمویڼې لپاره.
- Kali Linux: د هیکینگ لپاره ځانگړې عملیاتي سیستم.

۵. د زده کړې وړاندیزونه

- Online کورسونه:

- CEH (Certified Ethical Hacker) کورسونه.

- [TryHackMe](#)

- [Hack The Box](#)

- کتابونه:

- "Hacking: The Art of Exploitation"

- "The Web Application Hacker's Handbook"

۶. قانوني چوکاټ

ایټیکل هایکنگ باید تل د قانوني اجازې لاندې ترسره شي. د قانون خلاف هایکنگ د جزا وړ دی، حتی که نیت مو ښه وي.

دوهیم: د وسایلو او تخنیکونو په اړه معلومات؟

د ایټیکل هایکنگ وسایل او تخنیکونه

که تاسو غواړئ د ایټیکل هایکنگ په برخه کې پرمختللي پوهه ترلاسه کړئ، د وسایلو او تخنیکونو په اړه پوهه لرل ضروري ده. لاندې د ایټیکل هایکنگ لپاره مهم وسایل او د هغوی تخنیکونه ذکر شوي دي:

۱. د معلوماتو راتولولو وسایل

دا مرحله د ټارگيټ په اړه معلومات ترلاسه کولو لپاره ده.

- Nmap د شبکې سکين کولو او فعاله وسيلو موندلو لپاره.
- Recon-ng د اتوماتيک استخباراتي معلوماتو راتولولو لپاره.
- theHarvester د ايميل آدرسونو، ډومېنونو، او نورو عامه معلوماتو د راتولولو لپاره.
- Shodan د انټرنېټ سره وصل وسيلو (IoT) د پلټنې لپاره.

تخنيکونه:

- د DNS سکين کول.
- د شبکې نقشه جوړول.
- د خدمتونو او بندرونو (Ports) موندل.

۲. د زيانمنو ټکو پيدا کولو وسایل

دا وسایل د زيانمنو ټکو کشف کولو او امنيتي ستونزو موندلو کې مرسته کوي.

- Nessus د زيانمنو ټکو سکينر.
- OpenVAS وړيا او خلاص سرچينه سکينر.
- Nikto د ويب سرور د زيانمنو ټکو معلومولو لپاره.
- Burp Suite د ويب اپليکيشن امنيت لپاره.

- OWASP ZAP د ويب اپليکيشن سکين کولو لپاره يو بل مشهور وسيله.

تخنيکونه:

- د ويب اپليکيشن سکين کول.
- د شبکې سکين کول د TCP/IP پروتوکولونو له لارې.

۳. د زيانمنو ټکو کارولو (Exploitation) وسایل

دا مرحله د زيانمنو ټکو د ارزونې لپاره ده.

- Metasploit د امنيتي بریدونو لپاره تر ټولو مشهور وسيله.
- BeEF د براوزر د زيانمنو ټکو معلومولو لپاره.
- SQLmap د SQL انجیکشن د ازموينې لپاره.
- Social-Engineer Toolkit (SET) د ټولنيز انجینرۍ حملو لپاره.

تخنيکونه:

- د SQL انجیکشن حملې.
- د سستم د شاتنې دروازې جوړول. (Backdoors)
- د ټولنيز انجینرۍ له لارې اعتبار ترلاسه کول.

۴. د شبکې تحليل وسایل

دا وسایل د شبکې ټرافيک تحليل لپاره دي.

- Wireshark د شبکې ټرافیک او پروتوکولونو تحلیل لپاره.
- Tcpdump د لینکس لپاره د ټرافیک شننه.
- Ettercap د مین ان دی میډل (MITM) حملو لپاره.

تخنیکونه:

- د ټرافیک نیول. (Packet Capturing)
- د ډیټا انکرپشن تحلیل.
- د MITM حملې.

۵. د پاسورډ کرک کولو وسایل

د زیانمنو پاسورډونو معلومولو لپاره.

- John the Ripper د پاسورډ کرک کولو لپاره.
- Hashcat د پاسورډ هاش کولو لپاره.
- Hydra د لاگ ان د کرک کولو لپاره.

تخنیکونه:

- Brute Force.
- Dictionary حملې.
- د هاش ارزونه.

۶. عملي هیکنګ لپاره عملیاتي سیستمونه

ځانگړي عملياتي سیستمونه چې د ایتیکل هیکینګ لپاره ډیزاین شوي دي:

- Kali Linux د هیکینګ لپاره تر ټولو مشهور عملياتي سیستم.
- Parrot Security OS د امنیتي ازموینې لپاره.
- BlackArch د پرمختللي هیکینګ لپاره.

د عملي زده کړې لپاره پلیټ فارمونه

- TryHackMe د هیکینګ زده کړې لپاره اسانه پلیټ فارم.
- Hack The Box د امنیتي ازموینې مجازې چاپیریال.
- CTF (Capture The Flag) د امنیتي ستونزو د حل کولو مسابقي.

• دریم: د قانوني چوکاټونو او اخلاقي محدودیتونو پوهه؟

د ایتیکل هیکینګ لپاره قانوني چوکاټونه او اخلاقي محدودیتونه

ایتیکل هیکینګ د قانوني اجازې په چوکاټ کې ترسره کېږي، او هدف یې د سیستمونو او شبکو د امنیت ښه والی دی. دا برخې تاسو ته د قانوني او اخلاقي چوکاټونو په اړه عمومي پوهه درکوي:

۱. ایتیکل هیکنگ او قانونی اجازې

ایتیکل هیکرز باید د فعالیتونو لپاره لاندې گامونه په پام کې ونیسي:

- **رسمي اجازه:** مخکې له دې چې د هر شرکت یا سازمان سیستم ته لاسرسی وکړئ، د هغوی رسمي اجازه ترلاسه کړئ.
- **قانوني سندونه:** د (NDA (Non-Disclosure Agreement) لاسلیک، ترڅو د محرمانه معلوماتو د افشا کولو مخنیوی وشي.
- **د فعالیت محدودول:** یوازې هغه برخې ازمویئ چې په قرارداد یا اجازې کې مشخصې شوې وي.

۲. اخلاقي اصول

ایتیکل هیکرز د لاندې اخلاقي اصولو پابند دي:

- **صادق اوسئ:** د خپلې ازموینې هر اړخ په شفاف ډول ترسره کړئ.
- **د معلوماتو ساتنه:** د ترلاسه شویو معلوماتو د محرمانیت درناوی وکړئ.
- **هیڅ زیان مه رسوئ:** د خپلو فعالیتونو په ترڅ کې د سیستمونو یا ډیټابیس زیانمنولو څخه ډډه وکړئ.
- **راپور ورکول:** د زیانمنو ټکو په اړه مفصل او مسلکي راپور وړاندې کړئ.

۳. د نړیوالو قانوني چوکاټونو پیژندنه

ایټیکل هیکنگ د لاندې قوانینو له مخې قانونی کېږي:

- **Computer Fraud and Abuse Act (CFAA):** په امریکا کې دا قانون د غیرقانونی لاسرسی مخنیوی لپاره دی.
- **General Data Protection Regulation (GDPR):** په اروپا کې د شخصي معلوماتو د ساتنې لپاره.
- **Cybersecurity Information Sharing Act (CISA):** په امریکا کې د سایبري امنیت د معلوماتو شریکولو قانون.

۴. د قانونی محدودیتونو څخه سرغړونه

که ایټیکل هیکرز لاندې کړنې ترسره کړي، نو دا قانونی سرغړونه گڼل کېږي:

- د اجازې پرته هیکنگ.
- د ترلاسه شویو معلوماتو افشا کول.
- د سیستم یا شبکې د فعالیت گډوډول.
- د امنیتي زیانونو له منځه وړلو کې ناکامی.

۵. د ایټیکل هیکر لپاره مسلکي سندونه

د قانونی او اخلاقي پوهې لپاره، لاندې سندونه اخیستل گټور دي:

- **Certified Ethical Hacker (CEH):** د ایټیکل هیکر لپاره نړیوال معیار دی.

- Offensive Security Certified Professional (OSCP) د هيکينگ پرمختللي تخنيکونه پوښي.
- CompTIA Security+ د سايبيري امنيت بنسټيز سند.

٦. د ايتيکل هيکر د مسووليتونو اهميت

- د سيستم مالک سره شفاف اړيکه ساتل.
- د زيانمنو ټکو په اړه واضح، عملي او گټورې حلارې وړاندې کول.
- د هر ډول غير قانوني يا غير اخلاقي کړنې څخه ډډه کول.

مهم يادونه:

ايتيکل هيکينگ بايد تل د قوانينو په چوکاټ کې ترسره شي. د قانوني اجازې پرته هيکينگ، که نيت مو ښه هم وي، غير قانوني گڼل کېږي او د جزا وړ دی.

څلورم: د سيستمونو او شبکو امنيتي ازمويښې زده کړه

د ايتيکل هيکينگ د زده کړې لپاره کورسونه او سرچينې

که غواړئ د ایتیکل هایکینگ په برخه کې مهارت ترلاسه کړئ، لاندې کورسونه، ویب سایټونه، او منابع ستاسو لپاره مناسبې دي. دا سرچینې تاسو ته له بنسټیزو څخه تر پرمختللو تخنیکونو زده کړه درکوي.

۱. آنلاین کورسونه

مشهور آنلاین کورسونه چې د ایتیکل هایکینگ زده کړې لپاره جوړ شوي دي:

1. Certified Ethical Hacker (CEH):

- د EC-Council لخوا وړاندې کېږي.
- د ایتیکل هایکینگ بنسټیز او پرمختللي مفاهیم پوښي.
- د CEH کورس وگورئ

2. Offensive Security Certified Professional (OSCP):

- د هایکینگ پرمختللي تخنیکونه او عملیاتي تمرینونه شامل دي.
- د OSCP کورس معلومات

3. TryHackMe کورسونه:

- د نوي کارو لپاره ساده او تفریحي تمرینونه.
- وړیا او د پیسو ورکولو دواړه امکانات لري.
- [TryHackMe ته لار شئ](#)

4. Udemy Ethical Hacking کورسونه:

- د ارزانه قیمت سره کورسونه.
- د لومړنیو مهارتونو څخه تر پرمختللي وسایلو پورې شامل دي.
- د Udemy کورسونه وگورئ

۲. تمرین لپاره پلیتفارمونه

د عملي هیکنگ لپاره تمرینی چاپیریالونه:

1. Hack The Box (HTB):

- د شبکې او سیستمونو امنیت د ازموینې لپاره.
- د تمرین خونو او مسابقو سره.
- [Hack The Box ته لار شئ](#)

2. TryHackMe:

- د ایتیکل هیکنگ د زده کړې لپاره ساده او ښوونیز محیط.
- د مختلفو موضوعاتو تمرینونه لکه: شبکې، ویب امنیت، او نور.

3. OverTheWire:

- د لینکس او شبکې امنیت تمرینونو لپاره.
- [OverTheWire ته لار شئ](#)

4. VulnHub:

- د مجازی ماشینونو لپاره وړیا تمرینونه.
- د زیانمنو سیستمونو ازموینه.

۳. کتابونه

ځینې غوره کتابونه چې تاسو ته پراخ معلومات درکوي:

1. "Hacking: The Art of Exploitation" د Jon Erickson لخوا:

- د زیانمنو ټکو تخنیکي تحلیل.

2. "The Web Application Hacker's Handbook" د Dafydd Stuttard

لخوا:

- د ويب اپليکيشن امنيت زده کړې لپاره غوره کتاب.

3. "Metasploit: The Penetration Tester's Guide" د David Kennedy

لخوا:

- د Metasploit وسيلې کارول زده کړې.

4. "Linux Basics for Hackers" د OccupyTheWeb لخوا:

- د لينکس بنسټيزې زده کړې د هيکينگ لپاره.

۴. مهم عملياتي سيستمونه او وسايل

د هيکينگ لپاره ځانگړي عملياتي سيستمونه:

- Kali Linux: د ايتيکل هيکينگ لپاره بشپړ عملياتي سيستم.
- Parrot OS: د محرمت او امنيت ازموينې لپاره.
- BlackArch: د پرمختللي هيکرز لپاره.

مشهور وسايل:

- Nmap: د شبکې سکين کولو لپاره.
- Metasploit: د زيانمنو ټکو کارولو لپاره.
- Wireshark: د شبکې ټرافيک تحليل لپاره.
- Burp Suite: د ويب اپليکيشن امنيت ازموينې لپاره.

۵. ويب سايټونه او ټولنې

خپلې پوښتنې شریک کړئ او د مسلکي خلکو مشورې واخلي:

- Reddit (r/EthicalHacking) د ایتیکل هیکینګ لپاره پراخه ټولنه.
- Stack Overflow د تخنیکي ستونزو حل لپاره.
- Cybersecurity Forums د امنیت په اړه بحث او نظر شریکونه.

۶. مسابقې (CTF - Capture The Flag)

د هیکینګ مهارتونو لپاره سیالي:

- CTFtime: د نړیوالو CTF سیالیو مهال وېش.
- Google CTF: د امنیتي زیانونو حل کولو نړیواله سیالي.

The End

**Get more e-books from www.ketabton.com
Ketabton.com: The Digital Library**