د ایتیکل هکینګ زده کړه!

لیکوال : رحمان علی

2024

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

لومړی : د ایتیکل هیکینګ بنسټیز مفاهیمو زده کړه؟

ایتیکل هیکینګ (اخلاقي هیکینګ) د سیسټمونو 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 هیکینګ د بنسټیزو مفاهیمو لپاره یو ساده لارښود دی:

۱.ایتیکل هیکینګ څه شی دی؟

ایتیکل هیکرز (چې "وایټ هټ" هیکرز بلل کېږي) د اجازې سره د شرکتونو یا سازمانونو سیسټمونه او شبکې ازمویي. هدف یې دا دی چې زیانمن ټکي پیدا کړي مخکې له دې چې خرابکار هیکرز ورته لاسرسی وموميِ.

۲.د ایتیکل هیکر اصلي مسؤولیتونه

- 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 سیسټمونو لپاره د قوي امنیتي پالیسۍ جوړول.

۳. د ایتیکل هیکینګ اساسي مراحل

1. **د اجازې ترلاسه کول**: له مالک یا اداري څخه رسمي اجازه ترلاسه کړئ.
2. **د معلوماتو راټولول**: د ټارګیټ 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 هیکینګ 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 ازموینې لپاره.
- **Kali Linux**: د هیکینګ لپاره ځانګړې عملیاتي سیستم.

۵ .د زده کړې وړاندیزونه

- Onlineکورسونه:
  - CEH (Certified Ethical Hacker)کورسونه.
  - TryHackMe
  - Hack The Box
- کتابونه:
  - "Hacking: The Art of Exploitation"
  - "The Web Application Hacker’s Handbook"

۶ .قانوني چوکاټ

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

دوهیم: د وسایلو او تخنیکونو په اړه معلومات؟

د ایتیکل هیکینګ وسایل او تخنیکونه

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

۱.د معلوماتو راټولولو وسایل

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

- **Nmap:** د شبکې سکین کولو او فعاله وسیلو موندلو لپاره.
- **Recon-ng:** د اتوماتیک استخباراتي معلوماتو راټولولو لپاره.
- **theHarvester:** د ایمیل آدرسونو، ډومینونو، او نورو عامه معلوماتو د راټولولو لپاره.
- **Shodan:** د انټرنیټ سره وصل وسیلو (IoT) د پلټنې لپاره.

تخنیکونه:

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

۲.د زیانمنو ټکو پیدا کولو وسایل

دا وسایل د زیانمنو ټکو کشف کولو او امنیتي ستونزو موندلو کې مرسته کوي.

- **Nessus:** د زیانمنو ټکو سکینر.
- **OpenVAS:** وړیا او خلاص‌سرچینه سکینر.
- **Nikto:** د ویب سرور د زیانمنو ټکو معلومولو لپاره.
- **Burp Suite:** د ویب اپلیکیشن امنیت لپاره.

- **OWASP ZAP:** د ویب اپلیکیشن سکین کولو لپاره یو بل مشهور وسیله.

تخنیکونه:

- د ویب اپلیکیشن سکین کول.
- د شبکې سکین کول د TCP/IP پروتوکولونو له لارې.

۳. د زیانمنو ټکو کارولو (Exploitation) وسایل

دا مرحله د زیانمنو ټکو د ارزونې لپاره ده.

- **Metasploit:** د امنیتي بریدونو لپاره تر ټولو مشهور وسیله.
- **BeEF:** د براوزر د زیانمنو ټکو معلومولو لپاره.
- **SQLmap:** د SQL انجیکشن د ازموینې لپاره.
- **Social-Engineer Toolkit (SET):** د ټولنیز انجینرۍ حملو لپاره.

تخنیکونه:

- د SQL انجیکشن حملې.
- د سسټم د شاتنۍ دروازې جوړول.(Backdoors)
- د ټولنیز انجینرۍ له لارې اعتبار ترلاسه کول.

۴. د شبکې تحلیل وسایل

دا وسایل د شبکې ټرافیک تحلیل لپاره دي.

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

تخنیکونه:

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

۵ .د پاسورډ کرک کولو وسایل

د زیانمنو پاسورډونو معلوملو لپاره.

- **John the Ripper:** د پاسورډ کرک کولو لپاره.
- **Hashcat:** د پاسورډ هش کولو لپاره.
- **Hydra:** د لاګ ان د کرک کولو لپاره.

تخنیکونه:

- Brute Force.
- Dictionaryحملې.
- د هش ارزونه.

۶ .عملي هیکینګ لپاره عملیاتي سیستمونه

ځانګړي عملیاتي سیستمونه چې د ایتیکل هیکینګ لپاره ډیزاین شوي دي:

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

د عملي زده‌کړې لپاره پلیټفارمونه

- TryHackMe: د هیکینګ زده‌کړې لپاره اسانه پلیټفارم.
- Hack The Box: د امنیتي ازموینې مجازی چاپیریال.
- CTF (Capture The Flag): د امنیتي ستونزو د حل کولو مسابقې.

• 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 ښه‌والی دی. دا برخې تاسو ته د قانوني او اخلاقي چوکاټونو په اړه عمومي پوهه درکوي:

۱. ایتیکل هیکینګ او قانوني اجازې

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

- **رسمي اجازه**: مخکې له دې چې د هر شرکت یا سازمان سیسټم 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 سیسټمونو 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

ایتیکل هیکینګ د لاندې قوانینو له مخې قانوني کېږي:

- Computer Fraud and Abuse Act (CFAA): په امریکا کې دا قانون د غیرقانوني لاسرسي مخنیوي 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 قانوني محدودیتونو څخه سرغړونه

که ایتیکل هیکرز لاندې کړنې ترسره کړي، نو دا قانوني سرغړونه ګڼل کېږي:

- د اجازې پرته هیکینګ.
- د ترلاسه شویو معلوماتو افشا کول.
- د سیسټم یا شبکې د فعالیت ګډوډول.
- د امنیتي زیانونو له منځه وړلو کې ناکامي.

۵. د ایتیکل هیکر لپاره مسلکي سندونه

د قانوني او اخلاقي پوهې لپاره، لاندې سندونه اخیستل ګټور دي:

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

- Offensive Security Certified Professional (OSCP): د هیکینګ پرمختللي تخنیکونه پوښي.
- CompTIA Security+: د سایبري امنیت بنسټیز سند.

۶. د ایتیکل هیکر د مسوولیتونو اهمیت

- د سیسټم مالک سره شفاف اړیکه ساتل.
- د زیانمنو ټکو په اړه واضح، عملي او ګټورې حلارې وړاندې کول.
- د هر ډول غیر قانوني یا غیر اخلاقي کړنې څخه ډډه کول.

مهم یادونه:

ایتیکل هیکینګ باید تل د قوانینو په چوکاټ کې ترسره شي. د قانوني اجازې پرته هیکینګ، که نیت مو ښه هم وي، غیر قانوني ګڼل کېږي او د جزا وړ دی.

څلورم: د سیسټمونو او شبکو امنیتي ازموینې زده کړه

د ایتیکل هیکینګ د زده کړې لپاره کورسونه او سرچینې

که غواړئ د ایتیکل هیکینګ په برخه کې مهارت ترلاسه کړئ، لاندې کورسونه، ویب‌سایټونه، 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 هیکینګ زده کړې لپاره جوړ شوي دي:

1. Certified Ethical Hacker (CEH):
   - د EC-Councilلخوا وړاندې کېږي.
   - د ایتیکل هیکینګ بنسټیز او پرمختللي مفاهیم پوښي.
   - د CEHکورس وګورئ
2. Offensive Security Certified Professional (OSCP):
   - د هیکینګ پرمختللي تخنیکونه او عملیاتي تمرینونه شامل دي.
   - د OSCPکورس معلومات
3. TryHackMeکورسونه:
   - د نوي‌کارو لپاره ساده او تفریحي تمرینونه.
   - وړیا او د پیسو ورکولو دوړه امکانات لري.
   - TryHackMeته لاړ شئ
4. Udemy Ethical Hackingکورسونه:
   - د ارزانه قیمت سره کورسونه.
   - د لومړنیو مهارتونو څخه تر پرمختللي وسایلو پورې شامل دي.
   - د Udemyکورسونه وګورئ

۲. تمرین لپاره پلیټفارمونه

د عملي هیکینګ لپاره تمریني چاپیریالونه:

1. Hack The Box (HTB):
   - د شبکې او سیسټمونو امنیت د ازموینې لپاره.
   - د تمرین خونو او مسابقو سره.
   - Hack The Boxته لاړ شئ
2. TryHackMe:
   - د ایتیکل هیکینګ د زده‌کړې لپاره ساده او ښوونیز محیط.
   - د مختلفو موضوعاتو تمرینونه لکه: شبکې، ویب امنیت، او نور.
3. OverTheWire:
   - د لینکس او شبکې امنیت تمرینونو لپاره.
   - OverTheWireته لاړ شئ
4. VulnHub:
   - د مجازی ماشینونو لپاره وړیا تمرینونه.
   - د زیانمنو سیسټمونو ازموینه.

۳. کتابونه

ځینې غوره کتابونه چې تاسو ته پراخ معلومات درکوي:

1. "Hacking: The Art of Exploitation" د Jon Ericksonلخوا:
   - د زیانمنو ټکو تخنیکي تحلیل.

2. "The Web Application Hacker's Handbook" د Dafydd Stuttard لخوا:
   - د ویب اپلیکیشن امنیت زده کړې لپاره غوره کتاب.
3. "Metasploit: The Penetration Tester's Guide" د David Kennedy لخوا:
   - د Metasploit وسیلې کارول زده کړئ.
4. "Linux Basics for Hackers" د OccupyTheWeb لخوا:
   - د لینکس بنسټیزې زده کړې د هیکینګ لپاره.

۴. مهم عملیاتي سیستمونه او وسایل

د هیکینګ لپاره ځانګړي عملیاتي سیستمونه:

- **Kali Linux:** د ایتیکل هیکینګ لپاره بشپړ عملیاتي سیستم.
- **Parrot OS:** د محرمیت او امنیت ازموینې لپاره.
- **BlackArch:** د پرمختللي هیکرز لپاره.

مشهور 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 ازموینې لپاره.

۵. ویب‌سایټونه او ټولنې

خپلې پوښتنې شریک کړئ او د مسلکي خلکو مشورې واخلئ:

- **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 سیالۍ:

- **CTFtime:** د نړیوالو CTF سیالیو مهال‌وېش.
- **Google CTF:** د امنیتي زیانونو حل کولو نړیواله سیالي.

The End