**1.3 Given a scenario, analyze potential indicators associated with application attacks.**

- [Privilege escalation](https://tryhackme.com/module/privilege-escalation) (or at [attack&defense pentester academy](https://attackdefense.pentesteracademy.com/listing?labtype=windows-priv-esc&subtype=windows-priv-esc-basic))

- [Cross-site Scripting (XSS)](https://portswigger.net/web-security/cross-site-scripting) (Reflected, Stored/Persistent, DOM-based)

- Injections

- [Structured Query Language (SQL)](https://portswigger.net/web-security/sql-injection) (Blind content-based, Blind timing-based)

- [Dynamic-link Library (DLL)](https://tryhackme.com/room/abusingwindowsinternals)

- [Lightweight Directory Access Protocol (LDAP)](https://www.youtube.com/watch?v=S2mQBXcW3P0&ab_channel=JohnHammond) + (extra info at [brightsec](https://brightsec.com/blog/ldap-injection/))

- [Extensible Markup Language (XML)](https://portswigger.net/web-security/xxe)

- *Not on the exam objectives but it is included on the Study Guide:* [Command Injection](https://portswigger.net/web-security/os-command-injection).

- Pointer/object dereference

- [Directory traversal](https://portswigger.net/web-security/file-path-traversal)

- [Buffer overflows](https://tryhackme.com/room/bof1)

- [Race conditions](https://portswigger.net/web-security/file-upload/lab-file-upload-web-shell-upload-via-race-condition)

- Time of check/time of use

- [Error handling](https://portswigger.net/web-security/information-disclosure)

- Improper input handling

- [Replay Attack](https://www.comparitech.com/blog/information-security/what-is-a-replay-attack/)

- Session Replays

- Integer overflow

- Request Forgeries

- [Server-side (SSRF)](https://portswigger.net/web-security/ssrf)

- [Cross-site (CSRF/XSRF)](https://portswigger.net/web-security/csrf)

- [Application Programming Interface (API) attacks](https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-data-leakage-in-redirect)

- Resource Exhaustion

- [Memory Leak](https://attackdefense.pentesteracademy.com/challengedetails?cid=508)

- Secure Sockets Layer (SSL) Stripping

- Driver manipulation

- Shimming

- Refactoring

- [Pass the Hash](https://tryhackme.com/room/attackingkerberos)

**Ferramentas que você deve conhecer:**

* [Nmap](https://nmap.org/book/man.html) e outra opção é o Nmap-[RTFM](https://blog.zsec.uk/nmap-rtfm/)
* [Metasploit](https://www.offensive-security.com/metasploit-unleashed/introduction/)
* Burp suite (vários dos labs acima utilizam o Burp)
* Nessus
* Nikto
* Netcat e Ncat
* Wireshark
* TCPdump
* Hydra
* John The Ripper
* Medusa

**Info adicionais:**

* [Diferenças entre XSS vs CSRF](https://portswigger.net/web-security/csrf/xss-vs-csrf)
* [OWASP Juice Shop:](https://owasp.org/www-project-juice-shop/)abrange vulnerabilidades de todo o OWASP Top Ten junto com muitas outras falhas de segurança encontradas em aplicativos do mundo real.
* [CertMaster Labs Videos](https://www.youtube.com/playlist?list=PLZ4vdb01vqpsEr1Yb36Icf3BZRP9mxbwG)

—---------------------------------------------------------------------------------------------------------------------

**Above & Beyond**

[**Offensive Security PEN-103**](https://portal.offensive-security.com/courses/pen-103/books-and-videos/modal/modules/introduction)**:** o curso é gratuito, basta criar um cadastro e clicar em “continue” mesmo não selecionando nenhuma opção de subscrição, além disso, este curso pode servir como um roteiro, referência técnica e guia de estudo para aqueles que buscam a certificação Kali Linux Certified Professional.

Os jogos de guerra oferecidos pela comunidade **[OverTheWire](https://overthewire.org/wargames/)** podem ajudá-lo a aprender e praticar conceitos de segurança na forma de jogos. Comece por:

* **Bandit**: ótimo para se familiarizar com Linux e Bash: [resolução/walk-through.](https://www.abatchy.com/tag/OverTheWire%20-%20Bandit/)
* **Natas**: focado em aplicações web: [resolução/walk-through](https://www.abatchy.com/tag/OverTheWire%20-%20Natas/).

**Observação:** veja as resoluções/walk-through como último recurso, e somente depois de: *“tentar, tentar de novo, tentar mais uma vez, e tentar novamente mas dessa vez mais ainda, e se não conseguiu ou está preso* ***TRY HARDER****”* esse mindset vai ajudá-lo no seu aprendizado e desenvolvimento profissional.

Python for Pentesters, Attacking and Defending Active Directory, Windows Process Injection for Red-Blue Teams, Pentesting with Metasploit, Wi-Fi Security and Pentesting, Exploiting Simple Buffer Overflows on Win32, Windows System Programming: Fundamentals, Web Application Pentesting, Network Pentesting - <https://www.pentesteracademy.com/topics>

* [Running a Buffer Overflow Attack by Computerphile](https://www.youtube.com/watch?v=1S0aBV-Waeo&ab_channel=Computerphile) + [Buffer overflow exploitation Megaprimer for Linux](http://www.securitytube.net/groups?operation=view&groupId=4)
* [Redirecionamento de portas/tunneling](https://chamibuddhika.wordpress.com/2012/03/21/ssh-tunnelling-explained/) e meu artigo no linkedin [“Descomplicando o SSH Tunneling”](https://www.linkedin.com/pulse/descomplicando-o-ssh-tunneling-fl%C3%A1vio-costa/?originalSubdomain=pt); outra opção é este [artigo prático](https://www.abatchy.com/2017/01/port-forwarding-practical-hands-on-guide).
* [Pentesting Tools Cheat Sheet](https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/) ; [Pentest Cheat Sheet by Kitsun3Sec](https://github.com/Kitsun3Sec/Pentest-Cheat-Sheets)

### **Passive Recon:**

Leia as seguintes ferramentas/técnicas, experimente o máximo possível.

* [Google dorks](http://whatis.techtarget.com/definition/Google-dork-query)
* [Whois](https://whois.icann.org/en/about-whois)
* [Netcraft](https://searchdns.netcraft.com/)
* [Recon-ng](https://bitbucket.org/LaNMaSteR53/recon-ng): [Usage guide](https://bitbucket.org/LaNMaSteR53/recon-ng/wiki/Usage%20Guide).

### **Active Recon:**

* Entenda o que é **DNS**, como funciona, como realizar pesquisas diretas e reversas, o que são transferências de zona e como realizá-las. Ótima fonte [aqui](http://resources.infosecinstitute.com/dns-hacking/" \l "gref).
* Enumeração de serviços: [SMTP](https://pentestlab.blog/2012/11/20/smtp-user-enumeration/), [SNMP](http://carnal0wnage.attackresearch.com/2007/07/over-in-lso-chat-we-were-talking-about.html), SMB, entre outros. Não apenas enumere-os, entenda para que servem e como funcionam.

**Sistemas Operacionais**

* Linux Journey
* [Basic Linux Privilege Escalation](https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/)
* [Encyclopedia of Windows Privilege Escalation by Brett Moore](https://www.youtube.com/watch?v=kMG8IsCohHA&ab_channel=RuxconMc%27Gavin)
  + [List of commands](http://pwnwiki.io/#!privesc/windows/index.md)

**Programação**

* [Bash for Beginners](http://www.tldp.org/LDP/Bash-Beginners-Guide/html/): melhor referência sobre bash IMO. [Outra opção](https://guide.bash.academy/)
* [Explainshell](http://www.explainshell.com/): NÃO substitui as páginas do manual, mas divide os comandos facilmente para os novatos.
* [Learn Python the Hard Way](https://learnpythonthehardway.org/)

**What’s next? OFFENSIVE SECURITY - OSCP**Para quem quer algum dia seguir esse caminho de red team

Se você é um iniciante completo como eu, recomendo ler o livro *[Penetration Testing – A Hands on Introduction to Hacking](https://www.amazon.com.br/Penetration-Testing-Hands-Introduction-Hacking/dp/1593275641)* ([review do livro](https://kentosec.com/2018/09/09/penetration-testing-a-hands-on-introduction-to-hacking-book-review/)) e assistir aos vídeos do [IppSec de máquinas HackTheBox mais fáceis](https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA). Se você não estiver muito preocupado com o tempo para conquistar a OSCP, e se houver recursos financeiros, obter a certificação [eJPTv2](https://ine.com/learning/certifications/internal/elearnsecurity-junior-penetration-tester-v2) também pode valer muito a pena no caminho para a OSCP. Depois disso, basta dar uma chance ao PwK (link mais abaixo).

[Kioptrix 1-4 no Vulnhub](https://www.vulnhub.com/entry/kioptrix-level-1-1,22/): a série Kioptrix é bem conhecida na comunidade por ser amigável para iniciantes. Existem também inúmeras orientações disponíveis que você pode usar para acompanhar, [esta por exemplo](https://kentosec.com/2018/09/16/kioptrix-1-4-my-first-vulnerable-machines/).

Outras recomendações:

* [OSCP Preparation Notes](https://oscpnotes.infosecsanyam.in/My_OSCP_Preparation_Notes.html) ou [The Ultimate OSCP Preparation Guide, 2021](https://johnjhacking.com/blog/the-oscp-preperation-guide-2020/)
* [OSCP-Like Machines - VM LIST](https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=0) - Depoimento de alguém que começou do zero e conseguiu a certificação OSCP: *“I can confirm that HackTheBox is absolutely a proper platform to get more than well prepared to get into OSCP and I’d like to thanks to TJNull for elaborating that useful OSCP-like machines list since it was very helpful for me.”* Ismael Rodriguez.
* [Lista de Top 10 VMs no Hack The Box recomendada pelo Ismael](https://ismaelr.medium.com/my-top-10-oscp-like-hackthebox-machines-list-6d298edf8921)
* [Hack The Box Write Ups by Ranakhalil](https://ranakhalil101.medium.com/) *“If you have the time, I would strongly recommend completing TJ\_Null’s list of Hack The Box OSCP-like VMs and watching IppSec’s videos of how to solve them. You won’t know how accurate that list is until you start working on the boxes in the OSCP lab. That’s all I’m going to say.”*
* [Virtual Hacking Labs (VHL)](https://www.virtualhackinglabs.com/): se por acaso você fizer a prova e não passar, recomendo esse recurso como uma alternativa extra de estudos.
* **Exploits:** [Exploit-DB](https://www.exploit-db.com/); [Packetstorm](https://packetstormsecurity.com/files/tags/exploit/)

**Tools/Ferramentas extras:**

[**AutoRecon by Tib3rius**](https://github.com/Tib3rius/AutoRecon) **–** An incredible tool that makes enumeration so much easier, this tools is basically an essential for anyone attempting the OSCP exam.

[**Dirsearch by maurosoria**](https://github.com/maurosoria/dirsearch) **–** My go to directory enumeration tool, I personally find this tool to be much faster and more versatile than GoBuster or Dirb.

[**pspy by DominicBreuker**](https://github.com/DominicBreuker/pspy)– A linux process monitoring tool, pspy is great for viewing running processes to spot cron jobs or other potentially exploitable services. Has come in handy on multiple occasions.

[**linux-smart-enumeration by Diego Treitos**](https://github.com/diego-treitos/linux-smart-enumeration) **–** One of the best Linux privilege escalation tools out there, this was always my first port of call when faced with a low privileged Linux shell.

[**J.A.W.S by 411Hall**](https://github.com/411Hall/JAWS) **–** I found this script provides the most amount of information required for Windows privilege escalation, and is very worthwhile to run when working with a low privileged Windows session.