Fall 2023

Offensive Security Techniques Using Kali Linux

Kurtis Brent Kenady
Boise State University

Offensive Security Techniques Using Kali Linux

Kurtis B. Kenady

Boise State University

Author Note

Kurtis B. Kenady, Department Interdisciplinary Professional Studies (IPS) and Department of Cyber Operations and Resilience (CORe) Boise State University. Capstone mentor: Margaret Sass. kurtiskenady@u.boisestate.edu

Abstract

For my capstone project, I built a cybersecurity website that provides practical resources and hacking tools for any cybersecurity student or enthusiast. This website details the exact environments and steps needed to perform strategies including man-in-the-middle, SSH brute-forcing, wireless network password cracking, and other attacks. It includes complete instructions for getting started in offensive security and includes other valuable cybersecurity information, such as secure coding practices and Security+ certification insights. It shows complete instructions for start-to-finish of downloading the necessary operating system for performing attacks, Kali Linux.

Keywords: Offensive Security, Cybersecurity, Kali Linux, Hacking

Section 1: Offensive Security with Kali Linux

Project Inspiration

While my main motivation was learning more, my secondary motivation was providing concise and easy-to-use resources that provide practical instructions for offensive security. The internet is filled with a myriad of bogus sources and filler information. This creates difficulty for the aspiring cybersecurity professional to access useful information. This project freely delivers easy-to-understand and concise information for offensive security techniques, tools, CompTIA Security+ indispensable knowledge, and steps for common attacks.

Summary of Project Development

I started with the template for the website. I added data analytics to gauge interest, created the core content of my website and explained the main attacks, while continually improving the delivery of the information. I improvised the usability of the website, and lastly, uploaded useful extra cybersecurity content I learned in my Cyber Operations Engineering program.

Section 2: Elements coming together

Innovative Approach

I originally set out to teach cyber enthusiasts about technology. I had a lot of ideas for what I would do, including creating a specific program using AI. I thought I could do this with a medium such as a website, social media posts, or something similar. Ultimately, I concluded the best thing to do would be to create a website covering offensive security/cybersecurity, a topic I have the most resources in and would be the most straightforward to implement. I integrated a number of approaches and found that simply incorporating AI and offensive security worked the

best. I covered how Chat-GPT can be used to produce safe coding practices, input validation and parameterized queries, which merged AI knowledge with my education.

I used AI and my program resources to create the website and combine the possibilities of Kali Linux operating system hacks that can be complemented by having safe coding practices on the website. Coding is heavily integrated with hacking, and this makes it a valuable section on my security website. It emphasizes the need for knowledge of coding, not just on the security side, but on the offensive side as well. I integrated this perspective with my offensive security content in the most concise, clear, and effective way.

Emotional Intelligence

I suppose this project helped me be patient with myself and others, as I was able to incorporate feedback and struggled with my own difficulties. To figure out what I wanted to do, I tried to listen to what I was feeling in my soul about this project, and base it off of that, things that were relatable and useful. I considered current topics and things that would better connect with my readers so that they could more easily understand the content in addition to being interested in it. My goal was to make it easily comprehensible and intriguing.

Consideration of the Audience

My website targets an audience of cyber enthusiasts, who are essentially students of the cyber world, always learning. I do this through my writing and understanding of how students think and process information, in addition to their comprehension and decisions. I ensure to keep things like this in mind and their sense of comfort in navigating the website. While some of my approaches are in more of a neutral tone of voice, this is an intentional strategy, which better suits my audience and is preferred by motivated students. As a technician and engineer, I understand that concise clear communication is desired communication.

Value to Others

My website is extremely valuable to others because I appeal to them through the most envied and well-known skill in cybersecurity: hacking, presented in an understandable way. I explain the ethical hacker's toolkit of Kali Linux and the myriad of possible attacks, in addition to providing a means to gauge their interest in the career. This specific information allows the common person to perform most any attack in as little as 30 minutes. I simply lay specific attack instructions and concise environment descriptions for the reader's use (Hammond, Byte, Academy, Haralson, Gibson). I practice empathy by stepping into what the reader was thinking, saying, and experiencing, and practiced better communication skills.

Creative Thinking

I would say that applying what I learned in my Integrative Thinking course helped especially in the brainstorming sections. In addition, rethinking drafted content from the IPS Creative Thinking course and producing engaging and effective ways to produce information catalyzed my thought processes. I especially used reflection. Chat-GPT increased modernity of content.

Unique Approaches

I would say that my concise and easy-to-follow approach and ability to complete any attack in 30 minutes is unique. None of these factors are common. I also prioritized coming alongside users in all varying degrees of education. I include a highly valuable study approach for the Security+ certification: a difficult certification in cybersecurity, saving the reader fourteen-hundred dollars. For the specifics of this website project, I describe how to use these common tools: Burp Suite, Ettercap, SSLStrip, and Wireshark, used primarily in penetration testing and unethical hacking. It shows a fault tree analysis of SQLI, exposing the viewer to an actionable fault tree that is commonly used in vulnerability management risk assessment. ChatGPT provided secure coding examples and gave the reader the realization of Chat-GPT usefulness and functionalities.

Innovative Solution

My website demonstrates innovation because it is a straightforward, practical, and quick to implement resource for cyber enthusiasts for a variety of purposes, including gauging interest in offensive security and penetration testing. It consists of critical certification and secrets to using Kali Linux offensive security tools and defensive tools, like Wireshark packet analyzer, a references list for researchers, steps for a variety of modern attack types. In addition, is a copy/paste command-line hacking solution with downloadable tool links (Byte).

Innovative Approach to the Problem/Project

My choice of approach, offensive security, was more novel than other ideas I had produced. It included the most important things I learned, which included extremely practical knowledge and hacking skills with beginning-to-end instructions from invaluable sources. Another approach I considered was showing the steps to produce a program with ChatGPT, but this is super common. I was also considering doing other projects like explaining things I learned from my internship as an IT Technician, but this would not have been specific enough and not as effective in providing useful information. On the other hand, offensive security and cybersecurity opens a lot of doors for possibilities and fuels my interest.

Section 3: Results

I would say that the feedback I got from people regarding it was good. I got mostly verbal comments and critiques. I would say that most of the feedback has been regarding the layout of the website. People really liked the content.

Benefits to Stakeholders

The benefit is current and practical education. This knowledge can be used for cybersecurity enthusiasts. Education never goes away, even if some specific information becomes obsolete. The Security+ certificate is an industry-recognized certificate and gets candidates jobs (Gibson). This website will most likely be up for years for anyone to use. It will provide a baseline for common types of attacks on small to medium size businesses.

Actual Impact

They really liked the content and practical examples. They liked the tools and ease of getting started with hacking that the website offered. They also appreciated learning about a few types of attacks, including MiTMs with Ettercap, brute forcing, and proxy attacks (Hammond). These attacks are all executed with tools on Kali Linux (but the general idea can be applied elsewhere) and learning about it gave them a good idea of where to start in this field.

Section 4: Conclusion

Results

I anticipated getting less than what I got. I expected to get under one hundred viewers until I submitted it. I believed it would help educate Cybersecurity enthusiasts and broaden their knowledge and horizons for career exploration. It gave them additional ideas for what kind of tools and skills they might want to learn in cybersecurity.

Surprises

I had thirty-one people view the website with six unique visits. With the “special” website views (visits that exhibit a type of page interaction) I know that the special views uniquely benefited

and provided knowledge they could use elsewhere. I believed that most would just be the average person and look a page or two without reading too much in, and that it would be more deeply impactful for a select few, but helpful for everyone.

Things I Would Have Changed

I would also have made the topic a bit broader, including this and other useful cybersecurity knowledge. I believe I also would have considered doing something more closely related to the healthcare field or some of the things learned in my internship. I would say I would go farther back and include some of my older control grids, with mapped security controls for relevant risks.

References

Academy, V. (2020, October 17). *Learn Wireshark in 10 minutes - Wireshark Tutorial for Beginners*. YouTube. https://www.youtube.com/watch?v=lb1Dw0elw0Q

Byte, N. (2020, August 10). *How Hackers Could Brute-Force SSH Credentials to Gain Access to Servers*. YouTube. https://www.youtube.com/watch?v=FKVsz_2IWJs

Gibson, D. (2017). *CompTIA Security+ Get Certified Get Ahead*. Ycda, LLC.

Hammond, J. (2020, January 24). *Burpsuite Basics (FREE Community Edition)*. YouTube. https://www.youtube.com/watch?v=G3hpAeoZ4ek

Haralson, C. (2014, February 24). *How To: Use SSLstrip On Kali Linux*. YouTube. https://www.youtube.com/watch?v=OtO92bL6pYE

Appendix

Offensive security website

Website Photos

Offensive Security Techniques Using Kali Linux

Instructions for MiTM & Aircrack NG Tools

Attack Steps

acks do not work it is probably because you do not have the necessary attack conditions. Please see the "Quick Reference"

Attack Steps

Please note, if the following attacks do not work it is probably because you do not have the necessary attack conditions. Please see the "Quick Reference" page for these details.

See links below to videos with complete instructions!

•**Aircrack** NG Suite and Crunch
•**BetterCap**
•**SSLStrip**
•**Ettercap**
•Chatgpt

1.**SSLStrip:**

- 1.Use a Man-in-the-Middle (MiTM) attack by stripping the SSL encryption from HTTPS traffic and forwarding the modified HTTP request packets to the router and destination.
- 2.Begin reconnaissance using nmap to identify potential targets and their vulnerabilities.
- 3.Enable router forwarding for IPv4 tables to redirect traffic through the attacker's system.
- 4.Perform ARP spoofing on the router within the network using command line tools.
- 5.View logs to identify and potentially extract credentials from intercepted data using the ssl log.

! Sslstrip instructions: Command-line Commands in Order !

nterface> wlan clear. **3**. Echo 1 > /proc/sys/net/ipv4/ip_forward **4**. Iptables -t nat -A PREROUTING -p tcp –destination-port 80 -J
5. Route -n then record gateway ip address **6**. Nmap -sS -O <gateway IP>/24 **7**. Arpspoof -i <interface> -t <target IP> -r

Serious Career Seekers:

- **DM hiring managers/HR and get endorsement from someone in the field. Or direct message people.**

For jobs, get an endorsement and put it on LinkedIn, and DM/email HR/hiring managers with nice personal messages in addition to applying. This has greatly increased my chances of getting an interview. I have a job because of asking a YouTuber I watch in my field for help and after he put me on his LinkedIn page I got two leads from which I got job offers from both. Do pen test camps.

- Get the CEH cert, CompTIA Pentest+, or the Kali Linux offsec certificate. Take the time to learn it.

If you're wanting to do more defensive security stuff, learn **Splunk** big data organizer tool really well.

- **Netdevgroup** labs are gold for defensive and offensive security.

If want to be CISO, ask small business for work and overplay it on resume (know your skills). Learn to apply NIST controls. Convince executives of the need for improvement with metrics for eg. 20% increase successful phishing attacks. Learn the **CIS controls** and be aware of the NIST SP 83, 800-160, and 53. Know **cyber-insurance** stuff. Use Elephant Drive and VeraCrypt encryption.
Or learn Cloud Azure virtualization infrastructure to be cloud engineer.

Cybersecurity Enthusiasts/Career Seekers:

- For practical stuff on YouTube, watch **NullByte, David bombal, Network Chuck**, and John Hammond, and then turn around and do it. Use CoPilot AI or Chat-GPT to refine attacks with "I am a penetration tester" as justification.
- Watch Infosec for a plethora of content, if you search it. OWASP for decent cybersecurity content.

The following are the necessary attack conditions to be present before performing any attacks listed on this page. References (YouTube) are linked at the bottom.

Ettercap (or download Bettercap here):

1. **Wireless Network Environment:**
   - 1.wireless networks using WPA/WPA2 encryption.
   - 2.Accessible Wi-Fi signals within the attacker's proximity.
2. **Network Configuration:**vulnerable wireless networks with weak security settings.
   - 1.outdated security protocols or weak encryption.
3. **Access and Permissions:**
   - 1.Access to the target network
   - 2.Sufficient permissions to execute Ettercap commands and manipulate network traffic.
4. **Physical Proximity.**
5. **Target Selection and reconnaissance:**
   - 1.Identification of target network's BSSID, devices, and IP addresses.

BetterStrip:

1. **Network Configuration:**

ems with vulnerable web browsers.

d browsers with potential security flaws.

Cybersecurity Framework

AIANCA is an acronym for the **6 pillars of information security**
Accountability | Integrity | Availability | Non-repudiation | Confidentiality | Authenticity

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Update data management plan, polish password and access controls	*Inadequate Awareness and training*, role-specific training system, Data Protection, remediation process, Inadequate Configuration Management (R-CM-1)	*Inadequate security monitoring* (R-MP-1)	*Inadequate Incident Response* (R-IR-1) &3	Improvements data and software recovery remediation plan.
Inadequate inventories of access controls, accounts,	Inadequate email and browser infrastructure	security event detection , including active and passive means.	Communications in responding to security events in line with the level of emergency and type of response plan	*Create, maintain, and plan Backups*

NIST CSF Categories	Current	NIST Control Improvments
IDENTIFY	Basic risk assessment framework	Improve Governance, policies, inventorying
PROTECT	*Automatic monitoring system/auditing*	*Awareness Data Protection, Supply chain & vulnerability management./IR,* email/browser & infrastructure protections
DETECT	Network-wide monitoring system	Network Monitoring, Security Event Detection, *auditing software*
RESPOND	1 designated IR responder	IR: Communications & remediation process, diversified risk management, and improved recovery process (SP 800-61 ITU-T x.1056a)

Cybersecurity Framework

AIANCA is an acronym for the **6 pillars of information security**
Accountability | Integrity | Availability | Non-repudiation | Confidentiality | Authenticity

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Update data management plan, polish password and access controls	*Inadequate Awareness and training*, role-specific training system, Data Protection, remediation process, Inadequate Configuration Management (R-CM-1)	*Inadequate security monitoring* (R-MP-1)	*Inadequate Incident Response* (R-IR-1) &3	Improvements data and software recovery remediation plan.
Inadequate inventories of access controls, accounts,	Inadequate email and browser infrastructure	security event detection , including active and passive means.	Communications in responding to security events in line with the level of emergency and type of response plan	*Create, maintain, and plan Backups*

NIST CSF Categories	Current	N Ir
IDENTIFY	Basic risk assessment framework	Ir p
PROTECT	*Automatic monitoring system/auditing*	A P c m e in p
DETECT	Network-wide monitoring system	N S D s
RESPOND	1 designated IR responder	IR: Communications & remediation process, diversified risk management, and improved recovery process (SP 800-61 ITU-T x.1056a)