Making your network ready for Cyber Forensics Analysis

XtremePython Conference – April 16, 2024

Nishant Krishna
Researcher - Cognitive Computing, Cybersecurity, Cyber Forensics
Executive Director – Visiminds Technologies
Co-Founder and CTO – TechMachinery Labs™

in https://in.linkedin.com/in/nishantkrishna

https://twitter.com/nishantkrishna

✉ nishant.krishna@gmail.com

Disclaimer: Few of the images used in these slides may be the copyright of their respective owners. These images are used only for academics and non-commercial presentations.

About Nishant Krishna

Researcher - Cognitive Computing, Cybersecurity, Cyber Forensics

23+ years of experience working on Architecture, Cybersecurity, API Development, Anti-Counterfeiting Technologies, Cloud and Virtualization, Internet of Things (IoT), Machine Learning.

6 patents granted and 9 patents filed / pending.

Guest Professor / Adjunct Professor in Computing at Ramaiah Institute of Technology (RIT), REVA University, Bangalore.

Author of book "Python for Cybersecurity Cookbook"

Contributor to IEEE standards (P1931.1, P1451-99, P2994) working on defining standards for IoT, Cybersecurity, and Smart Cities.

My areas of interest and research include Cognitive Computing, Cybersecurity, and Cyber Forensics.

I have a Master of Science (MS) in Software Engineering from BITS, Pilani, along with many technical certifications.

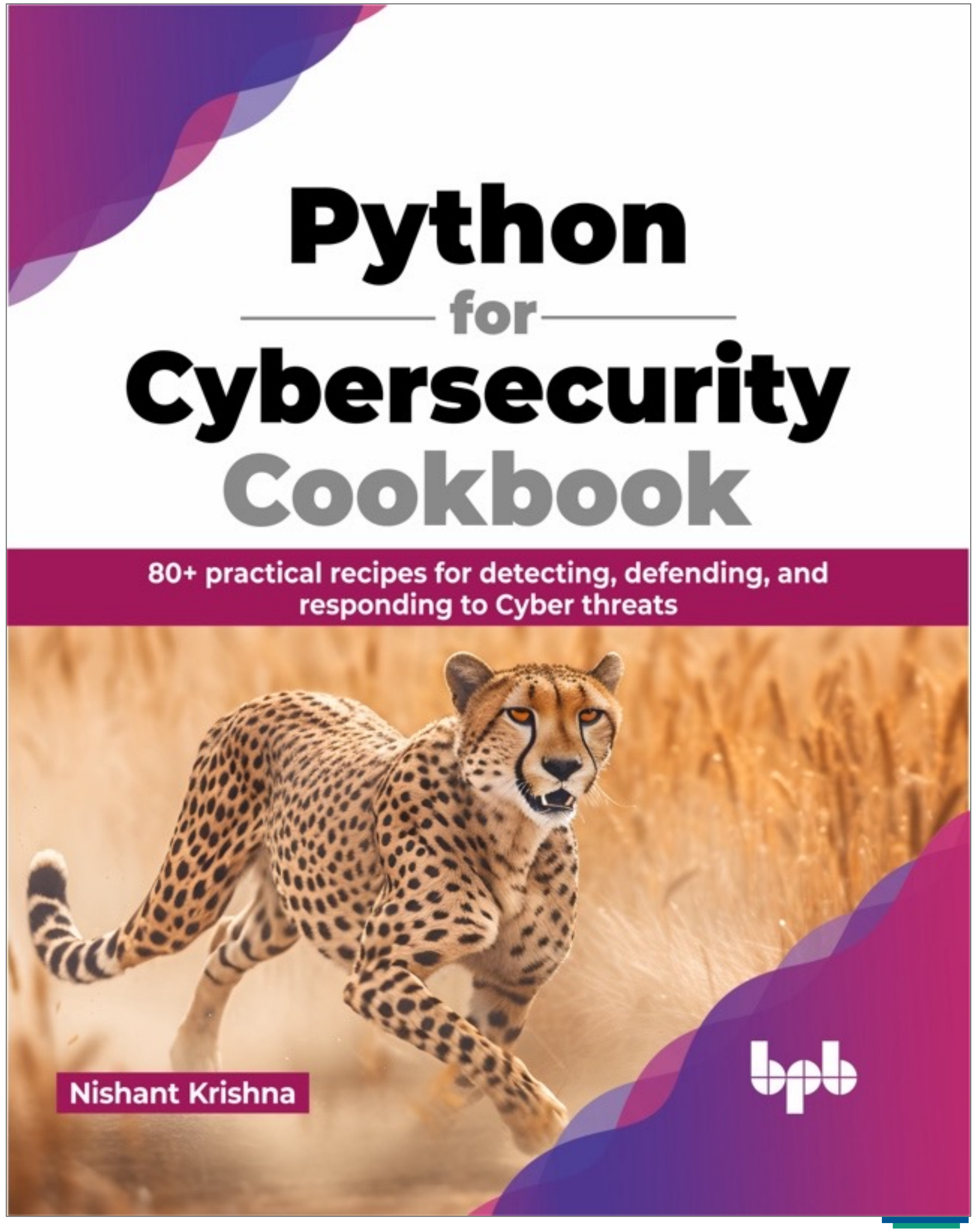
Python for Cybersecurity Cookbook

80+ practical recipes for detecting, defending, and responding to Cyber Threats

Python for Cybersecurity Cookbook has 80+ practical recipes for detecting, defending from, and responding to Cyber threats. If one wants to work in cybersecurity or hone your skills, this book is for them. That includes professionals, researchers, educators, students, and those considering a career in the field.

This book is a comprehensive guide to solving simple to moderate complexity problems in cybersecurity using Python. It starts with fundamental issues in reconnaissance and then moves on to the depths of topics such as forensic analysis, malware, phishing analysis, and working with wireless devices. Furthermore, it also covers defensive and offensive security topics, such as system hardening, discovery and implementation, defensive security techniques, offensive security techniques, and penetration testing.

All the source code for this book is available under MIT License on my GitHub.


Python
for
Cybersecurity
Cookbook
80+ practical recipes for detecting, defending, and responding to Cyber threats
Nishant Krishna
bpb

About Visiminds Technologies

VISIMINDS
TECHNOLOGIES

Visiminds Technologies is focused on vCISO and vCTO consulting and training in Cybersecurity, Cyber Forensics, Cloud Security, Compliance, Hyperscaling, Distributed Architecture, HA & DR, and BCP.

Summary of Cyber Forensics

1 Similarity with Forensics

- Malicious actors commit various cybercrimes, from snooping into the network and accessing the data to destroying the data or even committing cyber espionage.
- When cybercrime is committed, like any other crime, one has to collect evidence and analyze it to prosecute the cybercriminals.

2 Main goal of Cyber Forensics

The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence, and present the findings for prosecution.

3 Main functions of Cyber Forensics

1. Collection from the cybercrime scene
2. Preservation of the collected data
3. Analysis by Cyber Forensics experts
4. Documentation and Presentation

4 What constitutes Digital Evidence?

- Everything that is stored digitally, e.g., laptops, desktops, smartphones, flash drives, digital cameras, secondary storage
- System information and status, network information, running processes, logged-in users, logs, etc.
- Sources which are critical in the analysis, e.g., cache, history, printer and firewall logs
- Other sources, e.g., malware footpring,

Making your network ready for Cyber Forensics

Log everything important, using access logs, security logs, event logs, audit logs, etc.

Enable audit logs to catch any file changes

All the important security equipment should produce logs, e.g., firewalls, IDSs, and IPSs

Backup device configurations on periodic basis

Create network baselines on regular basis against which the changes can be compared

Use Security information and event management (SIEM) solutions

Periodically archive logs and other potential evidence to a centralized system

Keep the network audit trail ready

What about adding security control to perform a vulnerability scan and live packet capture on various interfaces whenever a critical file has changed?

Demo - Making your network ready for Cyber Forensics

1 Check if audit is enabled

- Audit logs in Linux can be used to track any changes in the system – trail of what happened
- For example, audit logs can be used to log every attempt to modify system files like sshd_config, passwd, change in system date and time, etc.
- Linux's auditctl utility is used to create audit trail

2 Checking if syslog is enabled

- Syslog infrastructure can send the logs on a system to a remote and centralized server, which can the n be used to find intrusions, anomalies, etc.
- Enabling syslog is important for making your system and network ready for Cyber Forensics

3 Analyze if Crontab has changed

- You can use Crontab to add crons jobs that are scheduled to do certain things like collect periodic logs, reset intentional/unintentional changes, etc.
- Having a way to audit if the content of the crontab file has changed is important
- This can be done using auditctl , too, but this method can be applied to many other files even if they are not under audit

4 Has someone installed new RPMs

- Checking if new RPMs are installed and are different from the baseline is a way to tell you that there may be intentional changes in the system
- A diff from the last list of RPMs with the new list can be used

Code for this demo will be available at https://github.com/Open-Source-Cybersecurity/xtremepython.

Thank You