

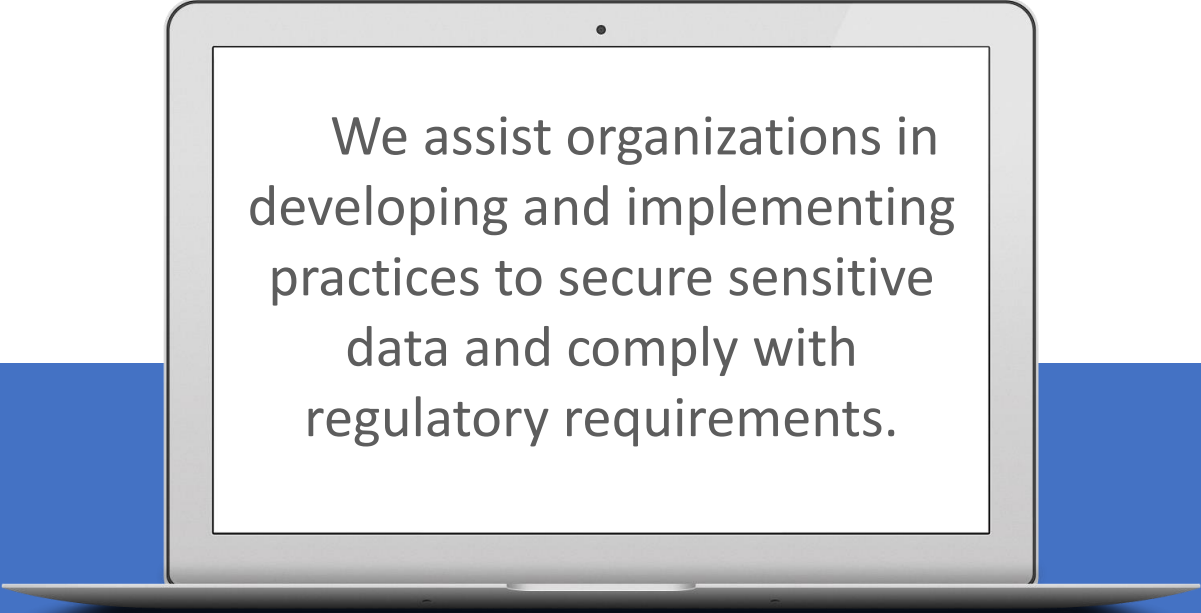
Vulnerability Assessment and Penetration Testing (VAPT) to Secure Data



databrackets
info@databrackets.com
866-276-8309



WHO WE ARE ...



We assist organizations in developing and implementing practices to secure sensitive data and comply with regulatory requirements.



DIY TOOLKIT

DIY assessment, training, customized policies & procedures and much more ...



CONSULTING

Professional services to help you with your Compliance needs



MANAGED SERVICES

Managed compliance and security services to focus on your key business outcome.

DISCLAIMER

Consult your attorney

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.



ALL WEBINARS ARE RECORDED AND AVAILABLE AS AN “ON DEMAND” SUBSCRIPTION



Srimi Kolathur

CISSP, CISA, CISM, MBA

Director, databrackets

Srimi's Background

- Security and Compliance
- Cisco IT Infrastructure
- HIPAA, PCI, Sarbanes-Oxley and ISO 27k Series
- A member of Rotary Club of Morrisville
- Interests: Running, healthy living and giving back

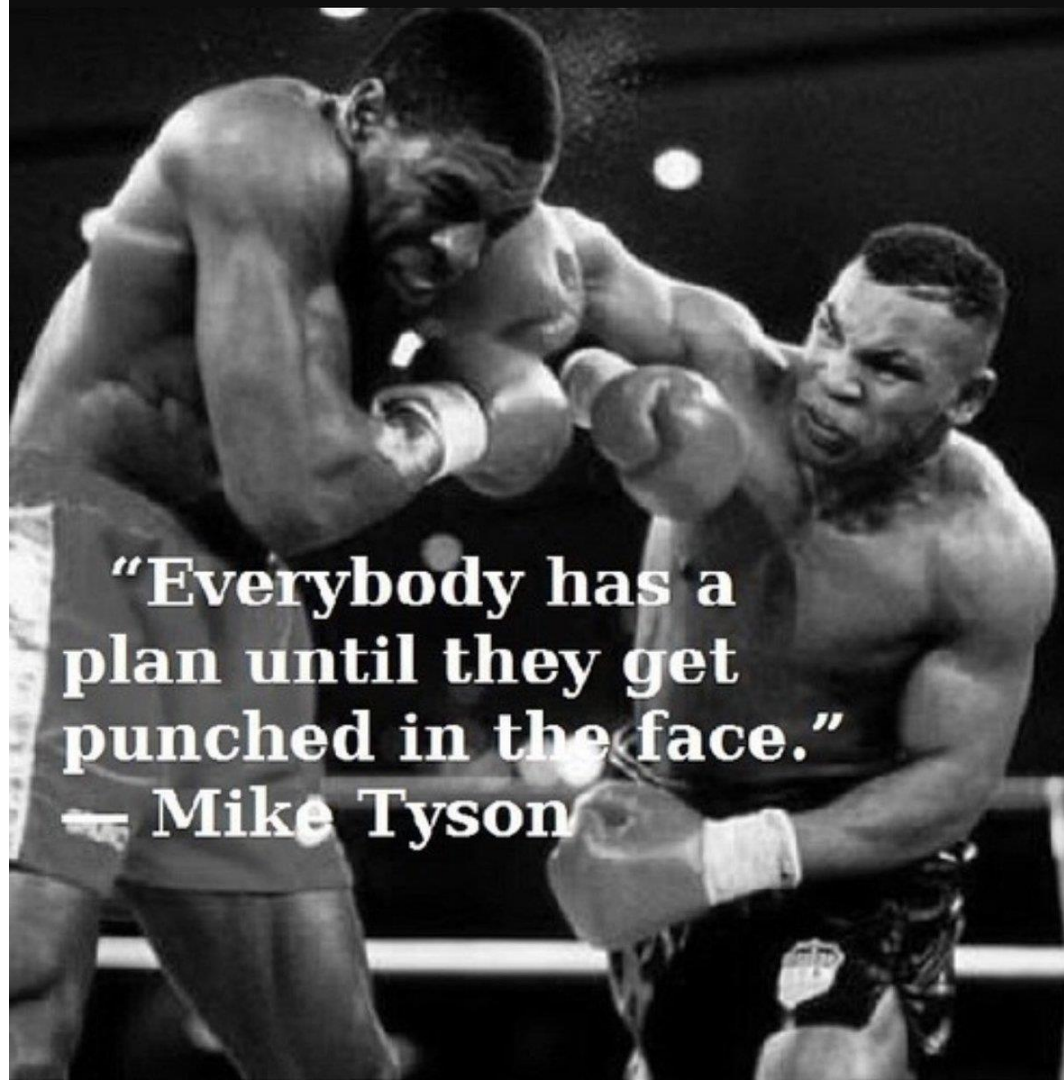
AGENDA

- 1 BACKGROUND
- 2 VAPT WORKFLOW
- 3 GOAL & OBJECTIVE
- 4 SCOPE
- 5 INFORMATION GATHERING
- 6 VULNERABILITY DETECTION
- 7 INFORMATION ANALYSIS & PLANNING
- 8 ATTACKS & PENETRATION
- 9 PRIVILEGE ESCALATION
- 10 RESULT ANALYSIS
- 11 REPORTING & CLEAN-UP
- 12 SUMMARY
- 13 NEXT STEPS
- 14 Q&A



WHY VAPT

- Required to protect your critical information assets
- Many of B2B customers might demand it
- Compliance requirement (NY Cybersecurity, GDPR, ISO 27k, etc.)
- Insurance claims/due-diligence



**“Everybody has a
plan until they get
punched in the face.”
— Mike Tyson**

WHO DOES IT APPLY TO ...

Anyone having sensitive data:

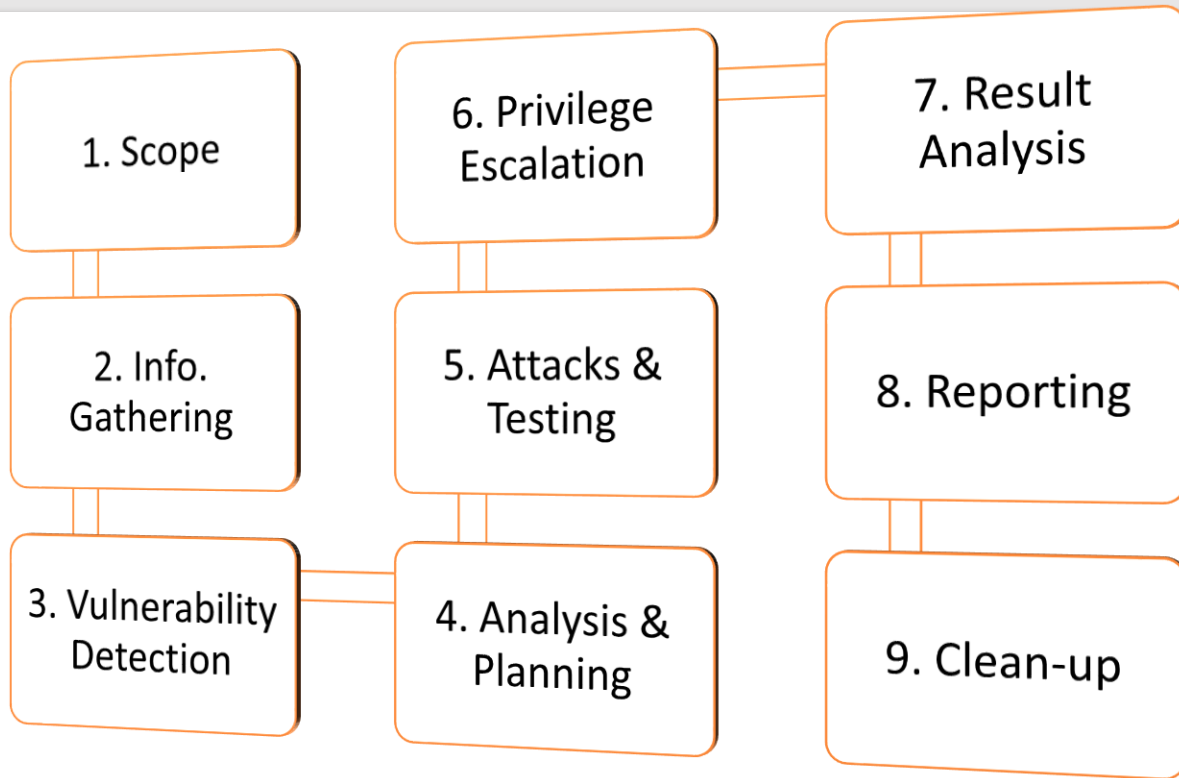
Customer data

Employee data

Financial data

Health data

VAPT WORKFLOW



Workflow steps might vary based on the scope, objectives and architecture

1. GOAL & OBJECTIVES

Two distinct objectives

- Vulnerability assessment tools **discover** which vulnerabilities are present
- Penetration test attempt to **utilize** the vulnerabilities in a system to **determine** if any unauthorized access or other malicious activity is possible and identify the threats

Sample Goal Statement:

- One of the major goals of the project is to educate developers in the field of application software security

Is the Goal Statement stated as a SMART goal?

2. SCOPE

The scope for each test depends on the company, industry, compliance standards, etc.

- Any and all devices with an IP address can be considered for a VAPT activity
- Penetration testing should focus on your organization's **external** parameters (IP Addresses, Offices, People, etc.)
- Vulnerability assessment should focus on your **internal** infrastructure (servers, databases, switches, routers, desktops, firewalls, laptops, etc.)
- Anything out of bounds for the project

SCOPE ...Cont'd.

Types of Penetration Testing :

- Network
- Application Security
- Physical
- Social Engineering

3. INFORMATION GATHERING

- Black Box/White box/Gray Box

Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities

Need to include all of information assets to identify the risks during this discovery phase

4. VULNERABILITY DETECTION

The most important step :

Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities

Mostly automated vulnerability scanning tools are used for identifying the vulnerabilities

5. ATTACKS & PENETRATION

1. Discover/Map
2. Reconnaissance
3. Discovery
4. Public Domain Sources
5. Port Scanning
6. Identification of Services
7. Short Listing of Crucial IPs
8. Identification of Operating System
9. Identification of Vulnerabilities
10. Exploitation of Vulnerabilities
11. Privilege Escalation
12. Other Attacks

- Nessus
- Meta Sploit
- Burp Suite
- And many other tools...

Depending on the complexity of the system additional steps might be required

6. RESULT ANALYSIS

- False positive
- Prioritized issues
- Follow-up testing

The key is to eliminate all unwanted noises so that organization can focus on key infrastructure/risks on a timely manner.

7. REPORTING

Report format:

- Introduction
 - Objectives of the assignment
 - Scope of the assignment
 - Standards followed
 - Duration of the assignment
- Management Summary
 - High-level findings
 - High-level recommendations
 - Graphical summary
- Technical Report
 - This report will contain the vulnerabilities discovered with CVE ratings and the mitigation recommendations
- Conclusion

High level summary reports are frequently shared with all stakeholders to share the risks/exposure

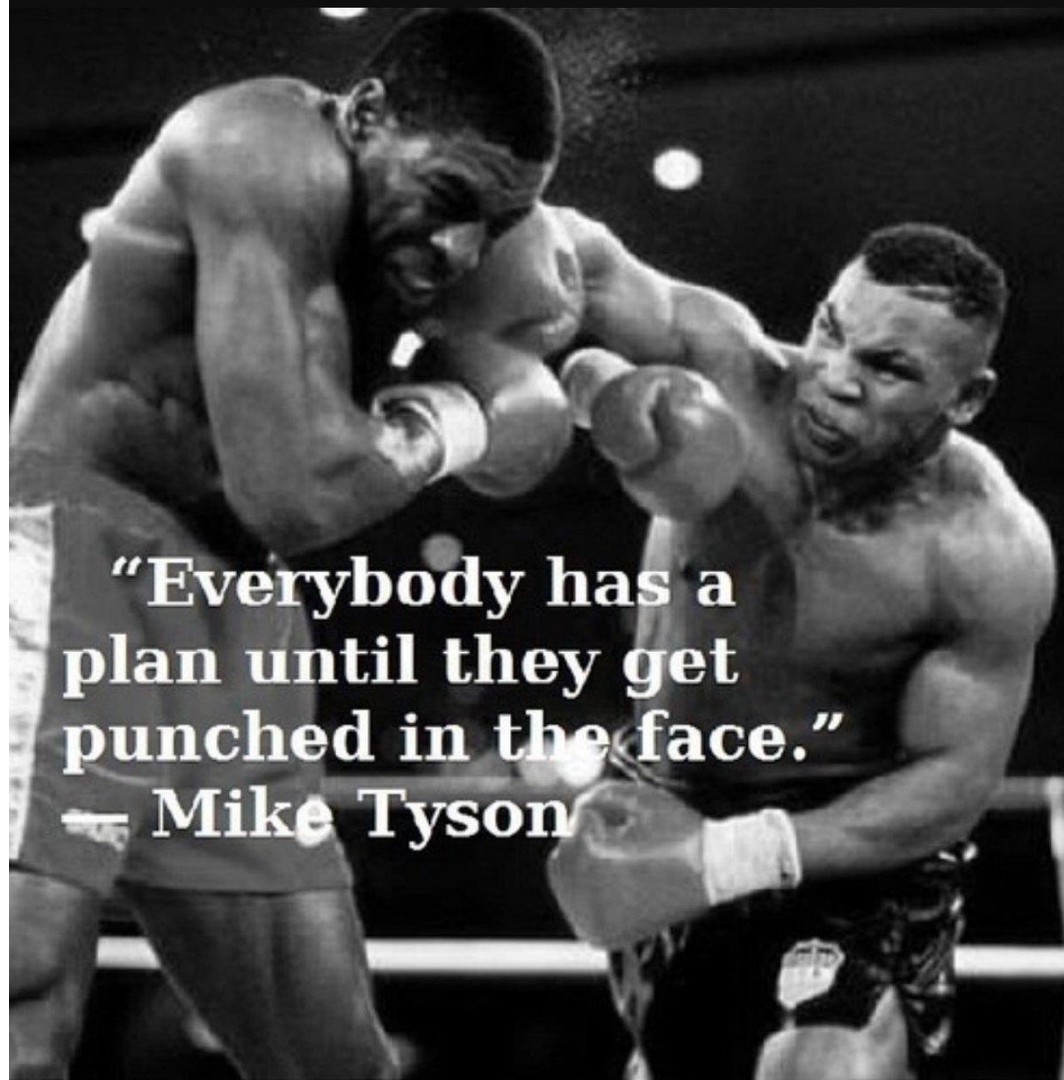
8. CLEAN-UP

- Removing any executables, scripts and temporary files from compromised systems
- Reconfiguring settings back to the original parameters prior to the pentest
- Eliminating any rootkits installed in the environment
- Removing any user accounts created to connect to the compromised system

NEXT STEPS

Contact databrackets for free no-obligation evaluation on your penetration testing and vulnerability assessment needs

866-276 8309 or info@databrackets.com



**“Everybody has a
plan until they get
punched in the face.”
— Mike Tyson**

UPCOMING EVENTS

❑ Business Continuity and Disaster Recovery – 11/7

Register now >> databrackets.com/webinars

FIND US



CALL US
866-276 8309



SERVICE
info@databrackets.com



LOCATION
150, Cornerstone Dr.
Cary, NC



SOCIALIZE
Facebook
Twitter

Twitter: [@databrackets](https://twitter.com/databrackets)

Facebook: [databrackets](https://facebook.com/databrackets)

Questions

Please don't hesitate to ask

Thank You

for your attention!

To purchase reprints of this document, please
email info@databrackets.com.

Thank you for joining us today

23 October, 2019