The Hacker's Meetup : 2k20

CFP : Call For Paper

Here I'm submitting Cyber Security Topics which will be good to covered in next the Hacker's meetup:2k20, I'm submitting 5 topics, you can select any topics and I'll give session in Meetup.

 # Topics:

1) Carding : Art of Banking Frauds
2) Digital Forensics Tools and Techniques
3) API Penetration Testing and Vulnerability Assessment
4) Cloud Pentesting, Forensics and Hardening
5) Incident Response Tools and Techniques

 # Explanation :

1) Carding : Art of Banking Frauds

What Is Carding?

Carding is a form of credit card fraud in which a stolen credit card is used to charge prepaid cards. Carding typically involves the holder of the stolen card purchasing store-branded gift cards, which can then be sold to others or used to purchase other goods that can be sold for cash. Credit card thieves who are involved in this type of fraud are called “carders.”

 # Discussion:

- What is Carding?
- How to Get Debit/Credit Card details?
- How to Bypass shopping website's Security?
- How to Bypass Banking Security?
- Deep learning about Cards Components and Security.
- How to secure yourself from Carding Attacks?
- How Hackers Secure themself during Carding Attacks?

 # Tools :

1. VPN
2. ProxyChains
3. VPS (Virtual Private Server)
4. DarkWeb

 # Note :

Duration : 1 Hour / 2 Hour

1. If there is chance so i can also perform Carding Demo.
2. I'll definitely try to secure some Important things so students can't misuse this knowledge.
3. There will be a good thing if you bring Indian defence officers so they can bring some security in Indian Banking Sector.

 # Reference :

- https://www.investopedia.com/terms/c/carding.asp
- https://en.m.wikipedia.org/wiki/Carding_(fraud)

2) Digital Forensics Tool and Techniques :

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

 # Discussion:

1. What is Digital Forensics?
2. Chain of Custody for Digital Forensics?
3. Which tool are important to perform Digital Forensics?
4. Which Techniques are important to perform Digital Forensics?
5. Future Scope of Digital Forensics in Cyber Crime Investigation?

 # Tools :

1. Autopsy, Encase, FTK, UFED
2. Volatility Framework
3. Imager Tool

 # Note :

Duration : 1 Hour / 2 Hour

1. If there is chance so i can also perform demo of Digital Forensics Tools .
2. I'll definitely try to secure some Important things so students can't misuse this knowledge.
3. There will be a good thing if you bring Indian Cyber Cell Team.

 # Reference :

1. https://en.wikipedia.org/wiki/Digital_forensics
2. https://www.techopedia.com/definition/27805/digital-forensics
3. https://www.computersciencedegreehub.com/faq/what-is-digital-forensics/

3) API Penetration Testing and Vulnerability Assessment :

API Penetration Testing is one of the favourite attack surfaces, where the attacker can use to gain further access to the application or server. During the blog reading, I've described the OWASP 2017 Test Cases which is applicable for a general application pen test. I'm going to cover the basics of the API penetration testing.

 # Discussion:

1. What is API pen testing?
2. Structure of API request and response?
3. Methodology, Tools and Test Case to perform Pen testing?
4. Brief about API Penetration Testing

 # Reference:

1. https://blog.securelayer7.net/api-penetration-testing-with-owasp-2017-test-cases/
2. https://medium.com/@asfiyashaikh10/web-services-api-pentesting-part-1-464313481720

 # Tools:

1. BurpSuite
2. FuzzAPI
3. Web VAPT Tools

4. OWASP ZAP Proxy

 # Note :

Duration : 1 Hour

1. Demo Will be Performed.
2. I'll definitely try to secure some Important things so students can't misuse this knowledge.
3. There will be a good thing if you bring Cyber Security Researcher and Analyst.

4) Cloud Pentesting, Forensics and Hardening:

The growth of cloud has led to some interesting angles on pen testing. Cloud-based applications need to be pen tested, as do their on-premises counterparts. However, pen testing applications that run in public clouds come with some complexities you must deal with, including legal and technical obstacles. To help address the challenges, here are five steps on how to approach cloud-based pen testing.

 # Discussion:

1. What is Cloud? How to use, types, environment?
2. Cloud Pentesting Checklist?
3. Tool and Techniques?
4. Cloud Forensics Tool and Techniques?
5. Cloud Security Hardening Techniques?

 # Tools:

1. Load Balancers
2. Firewalls
3. Rlog / Syslog
4. PFsense IDS

 # Note :

Duration : 1 Hour

1. Demo Will be not Performed because of lack of computer system but still i'll try my best to share knowledge.
2. I'll definitely try to secure some Important things so students can't misuse this knowledge.
3. There will be a good thing if you bring Cyber Security Researcher and Analyst.

 # Reference:

1. https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-cloud-need-know/
2. https://techbeacon.com/enterprise-it/pen-testing-cloud-based-apps-step-step-guide

5) Incident Response Tools and Techniques:

The threat of cyber attacks and other security incidents looms over all organisations. There are simply too many things that can go wrong – whether it's a cyber attack, a technical malfunction or another delay – to assume that operations will always be functional. But that doesn't mean you need to accept that delays are inevitable. You should be constantly assessing what might go wrong and how you would deal with it, because the way you respond to an incident may well be the difference between a minor disruption and a major disaster.

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

 # Discussion:

1. What is Incident Response?
2. Chain of Custody for incident response?
3. Tools and Techniques for incident response?
4. How to Behave During Attack?
5. Splunk Tool Demo?
6. Red teaming and Blue Teaming Assessment

 # Tools:

1. Splunk
2. Firewalls

3. IBM Qradar
4. SIEM Tools

 # Note :

Duration : 1 Hour / 2 Hour

1. Demo Will be Performed with Tools and techniques.
2. There will be a good thing if you bring Cyber Security Researcher and Analyst.

 # Reference:

1. https://searchsecurity.techtarget.com/definition/incident-response
2. https://www.cisecurity.org/controls/incident-response-and-management/

❖ **About Me:**

Dharmin A. Suthar
M.sc in Digital Forensics and Information Security
CEISH, CEH, CEI, CCSE.
Cyber Security Analyst and Researcher

Mobile: +91 8401853906
Email : suthardharmin@gmail.com
Social Media: https://in.linkedin.com/in/dharmin-suthar-94a983155