International Journal of Multidisciplinary Trends

E-ISSN: 2709-9369
P-ISSN: 2709-9350
www.multisubjectjournal.com
IJMT 2023; 5(11): 34-39
Received: 19-09-2023
Accepted: 26-10-2023

Shubham
Research Scholar, Om Sterling Global University, Hisar, Haryana, India

Dr. Rajinder Singh Sodhi
Professor (CSE), Om Sterling Global University, Hisar, Haryana, India

Dr. Preet Kaur
Assistant Professor, JC Bose University of Science & Technology, YMCA, Faridabad, Haryana, India

Corresponding Author:
Shubham
Research Scholar, Om Sterling Global University, Hisar, Haryana, India

Safeguarding mobile ecosystems: A comprehensive examination of cyber-attacks and mobile security

Shubham, Dr. Rajinder Singh Sodhi and Dr. Preet Kaur

Abstract
Mobile devices have become ubiquitous in today's digital landscape, serving as indispensable tools for communication, productivity, and entertainment. However, alongside their widespread adoption, mobile platforms have become prime targets for cyber-attacks, posing significant risks to individuals, businesses, and society at large. This paper provides a comprehensive examination of cyber-attacks targeting mobile ecosystems, exploring the tactics employed by malicious actors and the vulnerabilities inherent in mobile devices and applications.

The proliferation of mobile malware, phishing scams, and network intrusions underscores the urgent need for robust mobile security measures. This research delves into the various attack vectors utilized by cybercriminals to compromise mobile devices and exploit sensitive data. Furthermore, it investigates the evolving threat landscape, encompassing emerging trends such as mobile banking fraud, ransomware targeting mobile platforms, and supply chain attacks on mobile app stores.

Ultimately, this research contributes to the ongoing discourse on mobile security by providing insights into the evolving nature of cyber threats targeting mobile platforms and offering actionable recommendations for mitigating these risks. By fostering a proactive approach to mobile security, stakeholders can foster a safer and more secure mobile computing environment for all users.

Keywords: Cyber, security, ecosystem, productivity, cybercriminals

Introduction
Cyber-attacks targeting mobile devices have become increasingly prevalent and diverse, posing substantial risks to individuals, organizations, and even nations. These attacks encompass a wide range of tactics, from malware infections and phishing scams to network intrusions and data breaches. As the capabilities of mobile technology continue to advance, so too do the methods employed by malicious actors to compromise these devices. One of the primary motivations driving cyber-attacks on mobile platforms is the vast amount of sensitive data stored on these devices. From personal photos and messages to financial information and corporate emails, mobile devices often contain a treasure trove of valuable data ripe for exploitation. Consequently, cybercriminals relentlessly seek to exploit vulnerabilities in mobile operating systems, applications, and communication channels to gain unauthorized access to this wealth of information.

This research paper aims to provide a comprehensive examination of cyber-attacks targeting mobile devices, elucidating the various tactics employed by cybercriminals and exploring the vulnerabilities inherent in mobile ecosystems. Additionally, the paper will delve into the latest advancements in mobile security technologies and best practices to safeguard against these threats. By understanding the evolving landscape of mobile security risks and implementing robust defense mechanisms, individuals and organizations can mitigate the potential consequences of cyber-attacks and foster a safer mobile computing environment.

Literature Review
Orong *et al*. (2018) [7] have conducted a study which clustered the indexed crime data of the province of Misamis Occidental, Philippines and that provided prediction of future crimes in the next five years. Their study utilised the k-means clustering algorithm and AutoRegressive Integrated Moving Average (ARIMA) model to cluster and forecast the indexed crime data respectively.

Khraisat *et al*. (2019) [8] proposed SIDS or Knowledge-based Detection or Misuse Detection rely upon pattern matching approaches for determining a known attack. It made use of matching methods for determining any prior intrusion. That is, on the match of an intrusion signature with a previous existing intrusion signature existing in the signature database, an alarm signal is raised. In SIDS, there was inspection of host's logs for determining sequences of actions/commands that have been detected as malware.

Ayesha Arshad *et al.* (2021) [9] Phishing is the number one threat in the world of internet. Phishing attacks are from decades and with each passing year it is becoming a major problem for internet users as attackers are coming with unique and creative ideas to breach the security. In this paper, different types of phishing and anti-phishing techniques are presented. For this purpose, the Systematic Literature Review (SLR) approach is followed to critically define the proposed research questions. At first 80 articles were extracted from different repositories. These articles were then filtered out using Tollgate Approach to find out different types of phishing and anti-phishing techniques. Research study evaluated that spear phishing, Email Spoofing, Email Manipulation and phone phishing are the most commonly used phishing techniques. On the other hand, according to the SLR, machine learning approaches have the highest accuracy of preventing and detecting phishing attacks among all other anti-phishing approaches.

Alok Mishra *et al*. (2022) [10] Cyber threats have risen as a result of the growing usage of the Internet. Organizations must have effective cybersecurity policies in place to respond to escalating cyber threats. Individual users and corporations are not the only ones who are affected by cyber-attacks; national security is also a serious concern. Different nations' cybersecurity rules make it simpler for cybercriminals to carry out damaging actions while making it tougher for governments to track them down. Hence, a comprehensive cybersecurity policy is needed to enable governments to take a proactive approach to all types of cyber threats. This study investigates cybersecurity regulations and attributes used in seven nations in an attempt to fill this research gap. This paper identified fourteen common cybersecurity attributes such as telecommunication, network, Cloud computing, online banking, E-commerce, identity theft, privacy, and smart grid. Some nations seemed to focus, based on the study of key available policies, on certain cybersecurity attributes more than others. For example, the USA has scored the highest in terms of online banking policy, but Canada has scored the highest in terms of E-commerce and spam policies. Identifying the common policies across several nations may assist academics and policymakers in developing cybersecurity policies. A survey of other nations' cybersecurity policies might be included in the future research.

XML External Entity Attacks

There are online services that can read and process XML files. There are hazards associated with the programme known as an XML parser, which is responsible for processing the documents.

Vulnerability: It is possible for the XML parser to accept references from external entities if it is not properly set. An attacker may trick these third parties into thinking they are referring to files stored on the server processing the XML file. While gaining access to sensitive information is usually the intended outcome, a Denial-of-Service attack is another possible outcome.

Attack

A malicious XML file may be easily sent using a text editor. All we need is a basic understanding of how the XML parser works so that we can get the sensitive data. This XML document requests the contents of the "passwd" file from the UNIX server, as seen in the following example.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
  <foo>&xxe;</foo>
```

Fig 1: Example of an XML External Entity attack (Top 10-2017 A4-XML External Entities (XXE), 2018)

When a user requests a resource, the server will search for it and then provide the file's content, which may include account information. Keep in mind that you may also access the files stored on the server's network.

Ethical Hacking In Smartphones

It is important to emphasize that the pentester or hacker must have a good knowledge about technology to be able to carry out an ethical hacking, for which they must define a methodology that allows to take an order in the execution of the test and optimize the time in the execution phase.

Figure 2 shows the cycles of ethical hacking, in this methodology the different phases and tests are observed in an environment mounted with mobile devices.

Fig 2: Phases of an Ethical Hacking

Footprint Review

Footprint review is the process where the hacker develops a map that can be networks, systems or company. From here it will begin to collect all the information of the victim determining the objective as a system and the application that wants to attack.

The hacker arrives at the assembly of the map from non-intrusive methods, making use of social engineering from the website and telephone directories of the company, through this technique allows to discover initial information and build a map of the range of the network.

Information retrieval

This stage begins with a search through the Google search engine in order to investigate the name and if it is a company through the DNS, know the IP address of the server and collect the information.

Some examples of the filter of this search are.

- Search ads or press job offers in the systems department, because here you can find clues about the infrastructure they have or databases they use. For example, if you are looking for a webmaster who manages Apache, you would already know which web server they use.
- With the Who is command you can obtain information on the name of the company that owns the domain, address and telephones of the administrator, as well as knowing the assigned IP ranges since many companies do not pay for the information privacy service.
- In social networks such as Facebook, LinkedIn and Twitter, it handles important information for hackers and best of all that is free and can be used in a social engineering attack.
- Information retrieval (dumpuster diving), is a very useful method that allows to find keys in the pos-it that users throw away, where the recycling paper contains information relevant to the company.
- You can find many tools to perform a deep recognition, but the most important is to make a footprinting with a command line and a browser.

Fig 3: Simple Footprinting

In the following example, the search is performed on an Nmap Scanner page, a site managed by Fyodor where recognition and scanning tests can only be performed.

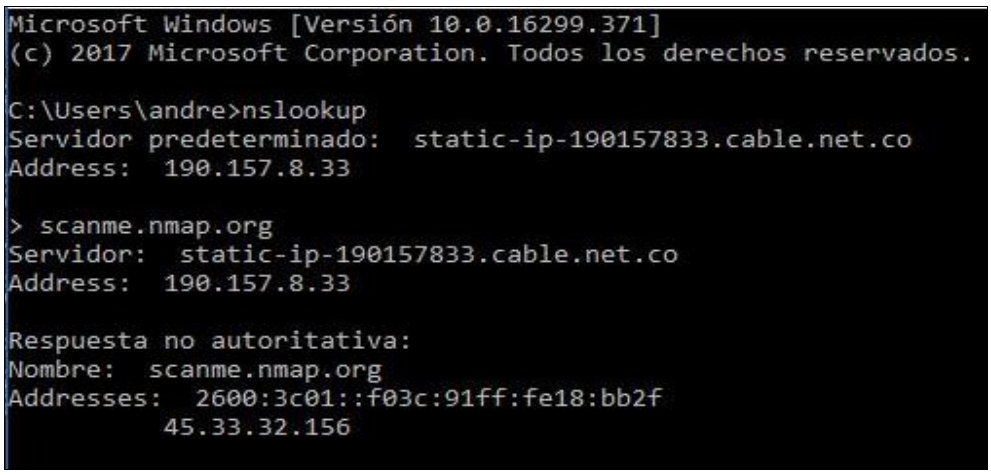

Fig 4: DNS resolution with NSLOOKUP in Windows

As Seen in figure 4, the search yields almost eleven thousand results but the one that is needed is located first, to optimize the search you can use the google bookmarks (+, -, "", and many more). Knowing the main site of the victim, a DNS query is performed to identify the IP address. Pinging the victim's site verifies that he is active and knows his IP address.

Ping scanme.nmap.org

Haciendo ping a scanme.nmap.org [45.33.32.156] con 32 bytes de datos.

Estadísticas de ping para 45.33.32.156.

Then the NSLOOKUP command is used, which allows to know if the DNS server is resolving the names in a correct way.

In the query made in Figure 5, it can be analyzed that the site has two IPV 6 and IPV 4 addresses, where the IPV 4 address is of class A since the first octet is 74 bits, so the range of the Host to analyze would be very large and would take a long time.

Set type = [NS | MX | ALL].

Permite establecer el tipo de consulta, NS servicio de Nombres, MX servicio de correo (mail exchanger) y ALL para mostrar todo [22].

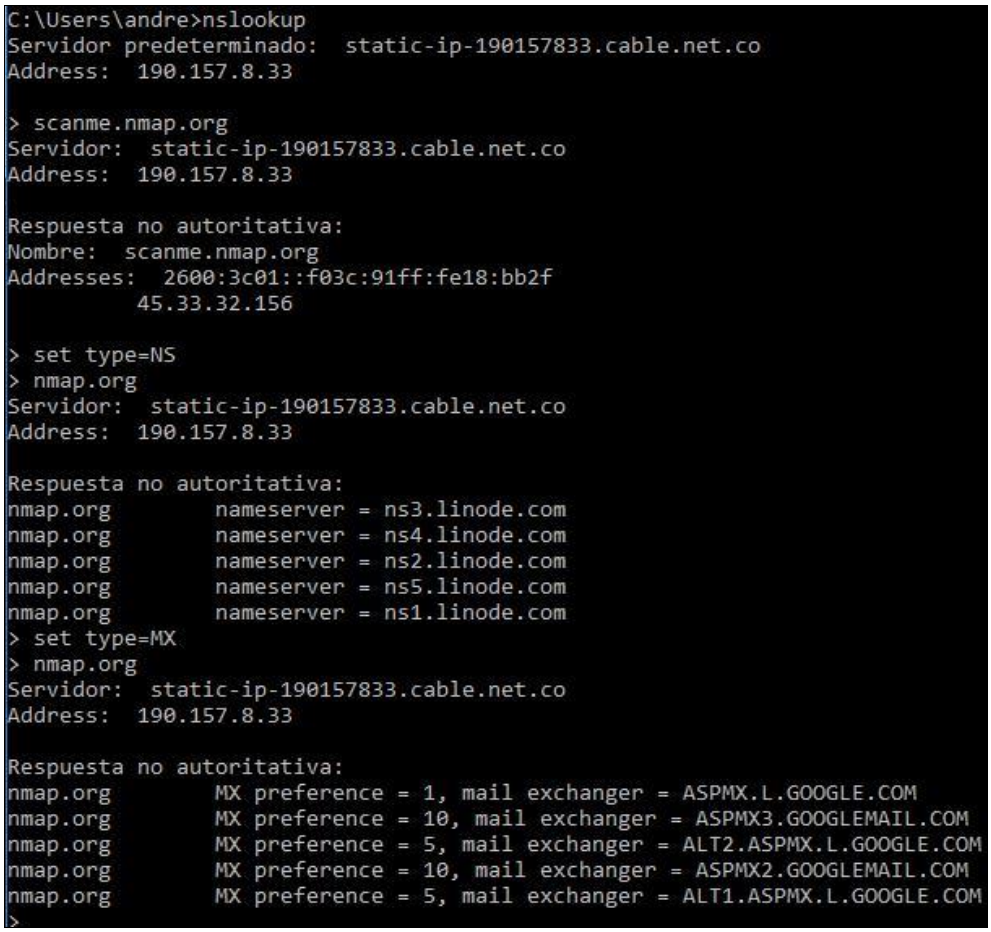

Fig 5: Nslookup: Set type=NS and Set type=MX

```
> set type=ALL
> nmap.org
Servidor:  static-ip-190157833.cable.net.co
Address:  190.157.8.33

Respuesta no autoritativa:
nmap.org        AAAA IPv6 address = 2600:3c01::f03c:91ff:fe98:ff4e
nmap.org        text =

        "v=spf1 a mx ptr ip4:45.33.49.119 ip4:173.255.243.189 ip4:192.81.131.254 ip6:26
00:3c01::f03c:91ff:fe98:ff4e ip6:2600:3c01::f03c:91ff:fe70:d085 include:_spf.google.com
 ~all"
nmap.org        internet address = 45.33.49.119
nmap.org
        primary name server = ns1.linode.com
        responsible mail addr = hostmaster.insecure.org
        serial  = 2016070584
        refresh = 14400 (4 hours)
        retry   = 14400 (4 hours)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
nmap.org        nameserver = ns5.linode.com
nmap.org        nameserver = ns3.linode.com
nmap.org        nameserver = ns2.linode.com
nmap.org        nameserver = ns1.linode.com
nmap.org        nameserver = ns4.linode.com
nmap.org        MX preference = 10, mail exchanger = ASPMX3.GOOGLEMAIL.com
nmap.org        MX preference = 10, mail exchanger = ASPMX2.GOOGLEMAIL.com
nmap.org        MX preference = 5, mail exchanger = ALT1.ASPMX.L.GOOGLE.com
nmap.org        MX preference = 5, mail exchanger = ALT2.ASPMX.L.GOOGLE.com
nmap.org        MX preference = 1, mail exchanger = ASPMX.L.GOOGLE.com
>
```

Fig 6: Nslookup set type = All

In Figure 6, the information in the NS query can be analyzed with respect to the name servers for the domain in which the target is hosted and in the MX query information is observed about who the mail servers are for that domain. The option ALL obtains combined information from the two previous consultations where you can see important information such as: nmap.org is hosted in an external hosting provided by Linode and the mail service is with the server mail.titan.net which is in a network segment other than the scanme.nmap.org server. Also, the Who is tool can help corroborate and expand contact information.

Information related to 'xx.xxx.xxx.x - xx.xxx.xxx.xxx'
netname: H0STING
descr: Main Hosting Servers
remarks: Abuse contact: *****Qmain-hosting.com

Fig 7: Scanner Inalámbrico Network Analyzer

With this query you can see the names of contacts, phones and emails, a positive point for the hacker giving him the possibility of social engineering, so it is worrisome that this information is disclosed in a public database.

Table 1: Report vulnerabilities found in the mobile

No.	Importance	Vulnerability
1.	High	Nessus Scan Information
2.	Low	Multiple Ethernet Driver Frame appending Information Discloksure (Etherleask)
3.	Low	ICMP Timestamp Request Remote Date Disclosure.
4.	Low	TCP/IP Timestamps Supported
5.	Low	OS Identification
6.	Low	Common Platform Enumeration (CPE)
7.	Low	Traceroute Information
8.	Low	Port SSH (222/TCP) - Service Detection
9.	Low	SSH Server Type and Version Information

Conclusion

In our interconnected digital age, mobile devices have become indispensable tools, serving as gateways to a vast array of services, information, and communication platforms. However, alongside the convenience they offer, mobile devices also present significant security challenges. With the proliferation of smartphones, tablets, and other portable gadgets, cybercriminals have found new avenues to exploit vulnerabilities and launch sophisticated attacks. One of the primary motivations driving cyber-attacks on mobile platforms is the vast amount of sensitive data stored on these devices. From personal photos and messages to financial information and corporate emails, mobile devices often contain a treasure trove of valuable data ripe for exploitation. Consequently, cybercriminals relentlessly seek to exploit vulnerabilities in mobile operating systems, applications, and communication channels to gain unauthorized access to this wealth of information. Furthermore, given the evolving nature of cyber threats, continuous monitoring, and timely updates are imperative to stay ahead of emerging vulnerabilities and attack vectors. Mobile security frameworks should prioritize proactive threat detection, rapid incident response, and ongoing risk assessment to mitigate the impact of cyber-attacks.

References

1. Bharati A, Sarvanaguru RA. Crime Prediction and Analysis Using Machine Learning. International Research Journal of Engineering and Technology. 2018;5(9):1037-1042.
2. Mandal I, Sairam N. New machine-learning algorithms for prediction of Parkinson's disease. International Journal of Systems Science. 2014;45(3):647-666.
3. Chatterjee C, Sarma N, Oki E. Routing and spectrum allocation in elastic optical networks: A tutorial. IEEE Communications Surveys & Tutorials. 2015;17:1776-1800.
4. Osisanwo FY. Supervised Learning Algorithms: Classification and Comparisons. International Journal of Computer Trends and Technology. 2017;48(3):128-132.
5. Weng WH. Machine Learning for Clinical Predictive Analytics. Machine Learning. MIT CSAIL; c2019.
6. Saleh MA, Khan IR. Crime Data Analysis in Python using K Means clustering. International Journal of Research in Applied Science and Engineering Technology. 2019;7(4):151-155.
7. Orong MY, Sison AM, Hernandez AA. Mitigating vulnerabilities through forecasting and crime trend analysis. In: 2018 5th IEEE International Conference on Business and Industrial Research (ICBIR); c2018. p. 57-62.
8. Khraisat A, Gondal I, Vamplew P. An anomaly intrusion detection system using C5 decision tree classifier. In: Trends and applications in knowledge discovery and data mining. Springer; c2019. p. 149-155.
9. Arshad A, Ur Rehman A, Javaid S, Ali T, Sheikh J, Azeem M, *et al*. A Systematic Literature Review on Phishing and Anti-Phishing Techniques; c2021.
10. Mishra A, Alzoubi YI, Anwar MJ, Gill AQ. Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security. 2022;120:102820. DOI: 10.1016/j.cose.2022.102820