CYBER SECURITY
MINOR ROJECT

UNDER ESTEEMED GUIDENESS OF

Ms. YANDAMURI UMADEVI

Department of Cyber Security

SUBMITTED BY

KOTA SANDEEP

(kotasandeep2003@gmail.com**)**

ABSTRACT

Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is cybercrimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

The high level of insecurity on the internet is becoming worrisome so much so that transaction on the web has become a thing of doubt. Cybercrime is becoming ever more serious and prevalent. Findings from 2002 Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. In this paper, we provide an overview of Cybercrime and present an international perspective on fighting Cybercrime.

This work seeks to define the concept of cyber-crime, explain tools being used by the criminals to perpetrate their evil handiworks, identify reasons for cyber-crime, how it can be eradicated, look at those involved and the reasons for their involvement, we would look at how best to detect a criminal mail and in conclusion, proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

TABLE OF CONTENTS

1.FOOT PRINTING

Introduction to Foot Printing

- Foot Printing will allow the attacker to gather the information related to internal and external security architecture, attacker collects publicly available sensitive information.
- Collection of information also helps the attacker to identify the vulnerabilities in a system and which will in exploits to gain access.
- Getting more information about target reduces the focus area & bring attacker closer to the target to perform easier to attack.

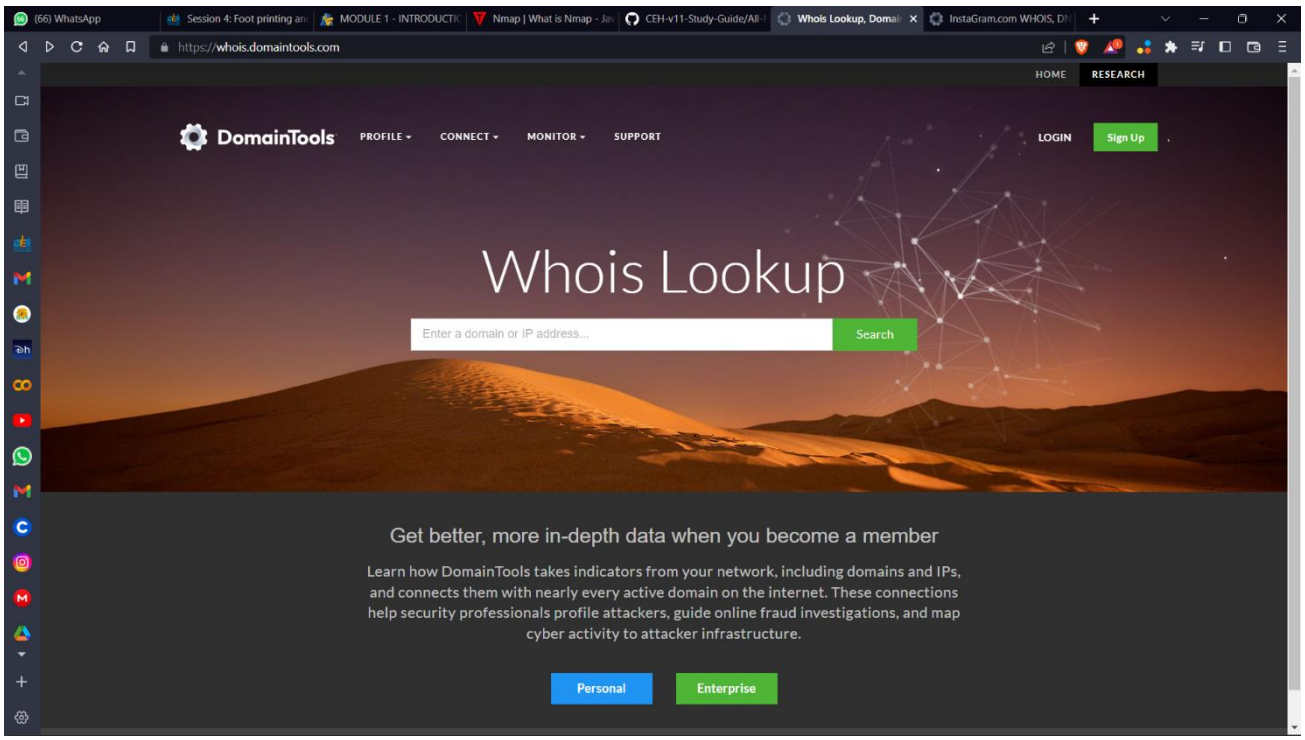
AIM :-

Finding domain registration details with Whois tool for 5 sites of your choice.

/// **By Whois Website**

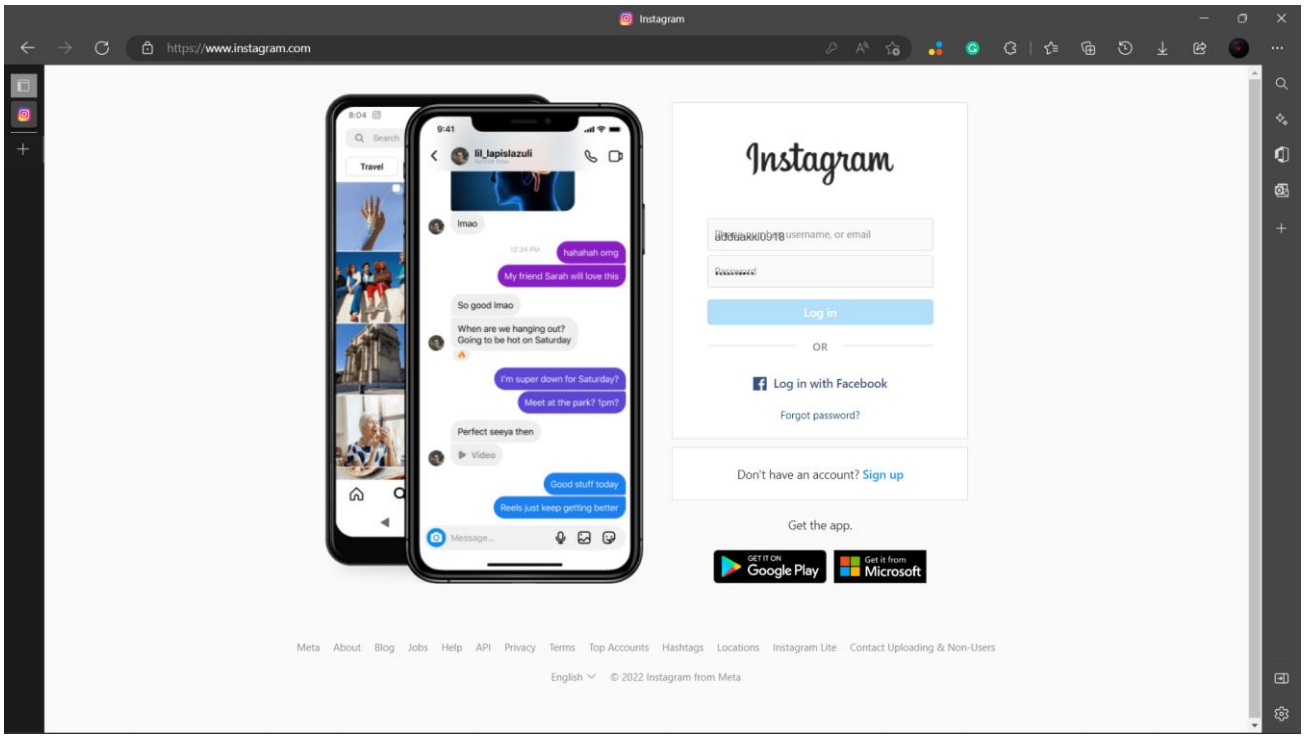
REFERENCE WEBSITE LINK

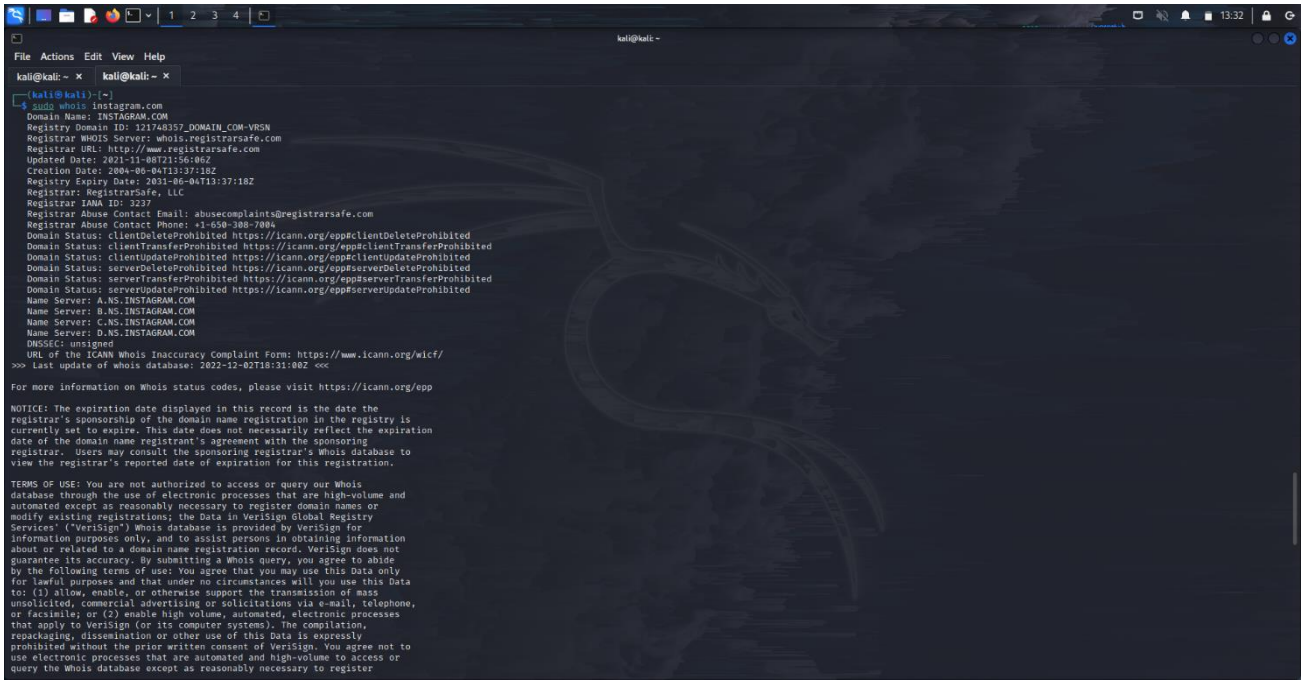
$ https://whois.domaintools.com/



1.1 Domain registration details of Instagram website

Web Site Name : https://www.instagram.com/





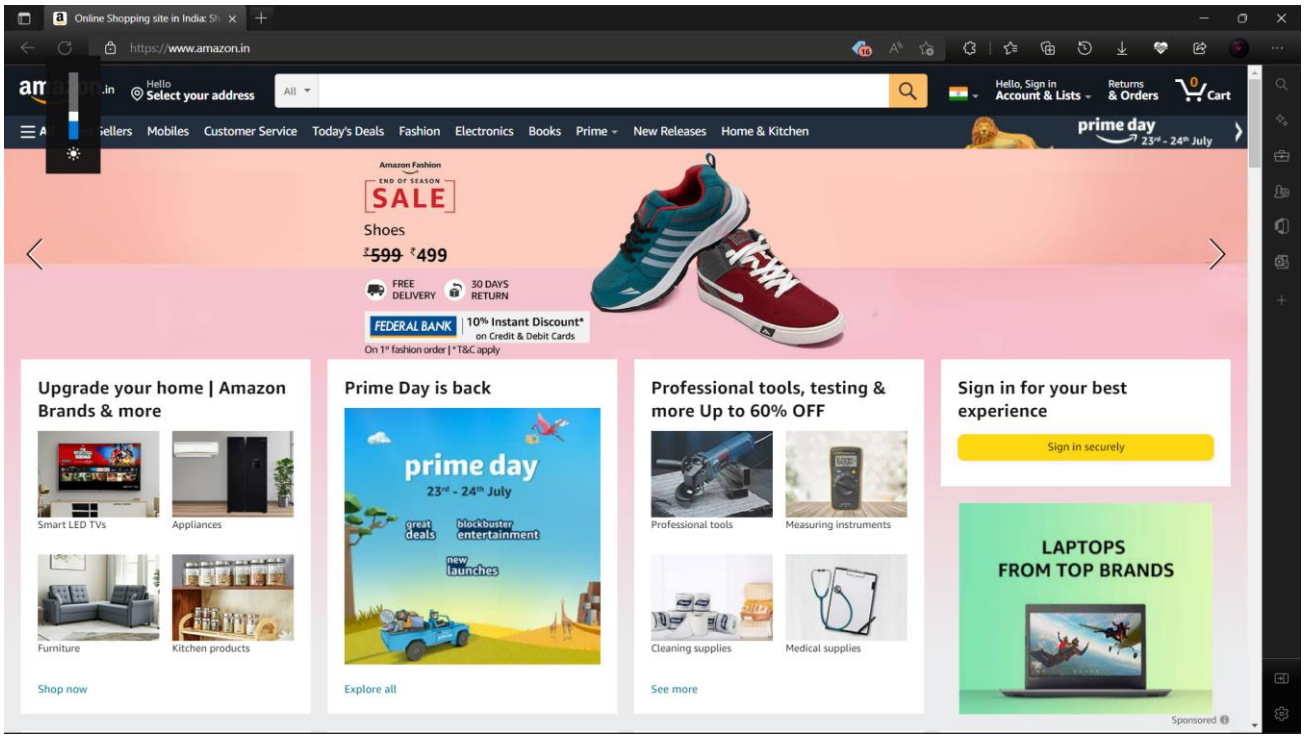
- Registry Domain ID: 121748357_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.registrarsafe.com
- Registrar URL: https://www.registrarsafe.com
- Updated Date: 2021-11-08T21:56:06Z
- Creation Date: 2004-06-04T13:37:18Z
- Registrar Registration Expiration Date: 2031-06-04T13:37:18Z

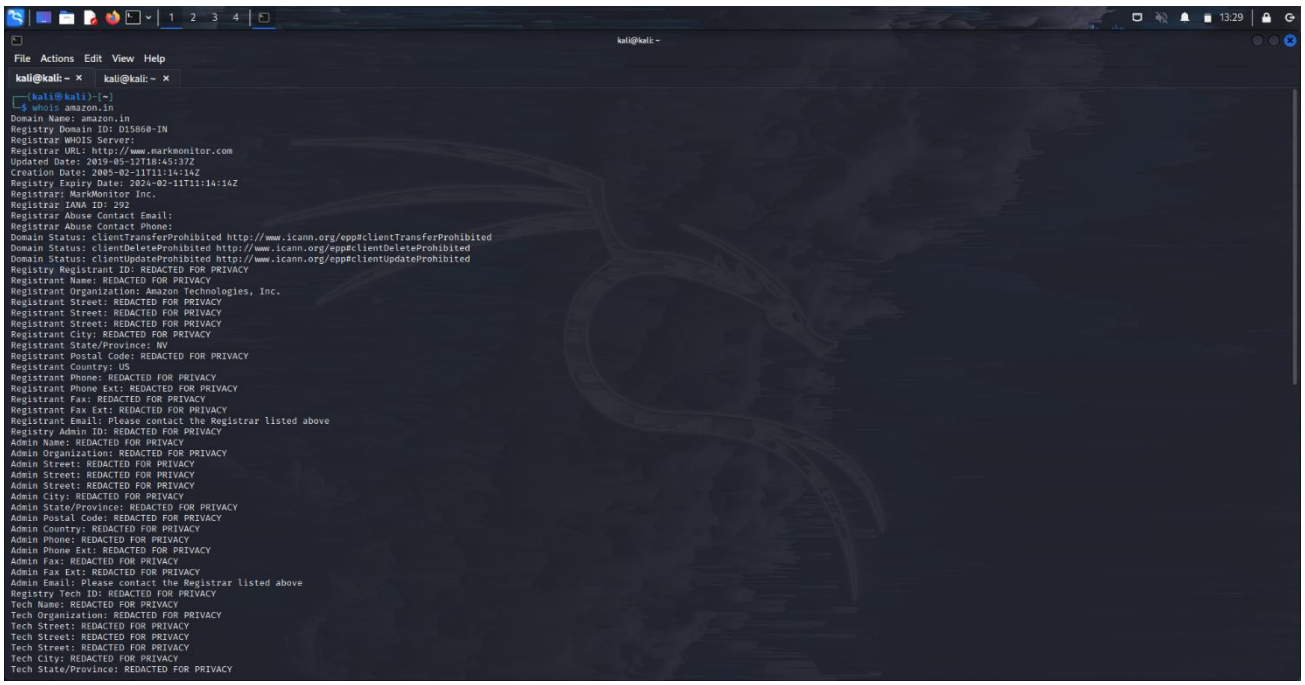
- Registrar: RegistrarSafe, LLC
- Registrar IANA ID: 3237
- Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
- Registrar Abuse Contact Phone: +1.6503087004
- Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
- Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
- Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited
- Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
- Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
- Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
- Registry Registrant ID:
- Registrant Name: Domain Admin
- Registrant Organization: Instagram LLC
- Registrant Street: 1601 Willow Rd
- Registrant City: Menlo Park
- Registrant State/Province: CA
- Registrant Postal Code: 94025
- Registrant Country: US
- Registrant Phone: +1.6505434800
- Registrant Phone Ext:
- Registrant Fax:
- Registrant Fax Ext:
- Registrant Email: domain@fb.com
- Registry Admin ID:
- Admin Name: Domain Admin
- Admin Organization: Instagram LLC
- Admin Street: 1601 Willow Rd
- Admin City: Menlo Park
- Admin State/Province: CA
- Admin Postal Code: 94025
- Admin Country: US
- Admin Phone: +1.6505434800
- Admin Phone Ext:
- Admin Fax:
- Admin Fax Ext:
- Admin Email: domain@fb.com
- Registry Tech ID:
- Tech Name: Domain Admin
- Tech Organization: Instagram LLC
- Tech Street: 1601 Willow Rd
- Tech City: Menlo Park
- Tech State/Province: CA
- Tech Postal Code: 94025
- Tech Country: US
- Tech Phone: +1.6505434800
- Tech Phone Ext:

- Tech Fax:
- Tech Fax Ext:
- Tech Email: domain@fb.com
- Name Server: A.NS.INSTAGRAM.COM
- Name Server: D.NS.INSTAGRAM.COM
- Name Server: B.NS.INSTAGRAM.COM
- Name Server: C.NS.INSTAGRAM.COM
- DNSSEC: unsigned

1.2 Domain registration details of Amazon website

Web Site Name : www.amazon.in

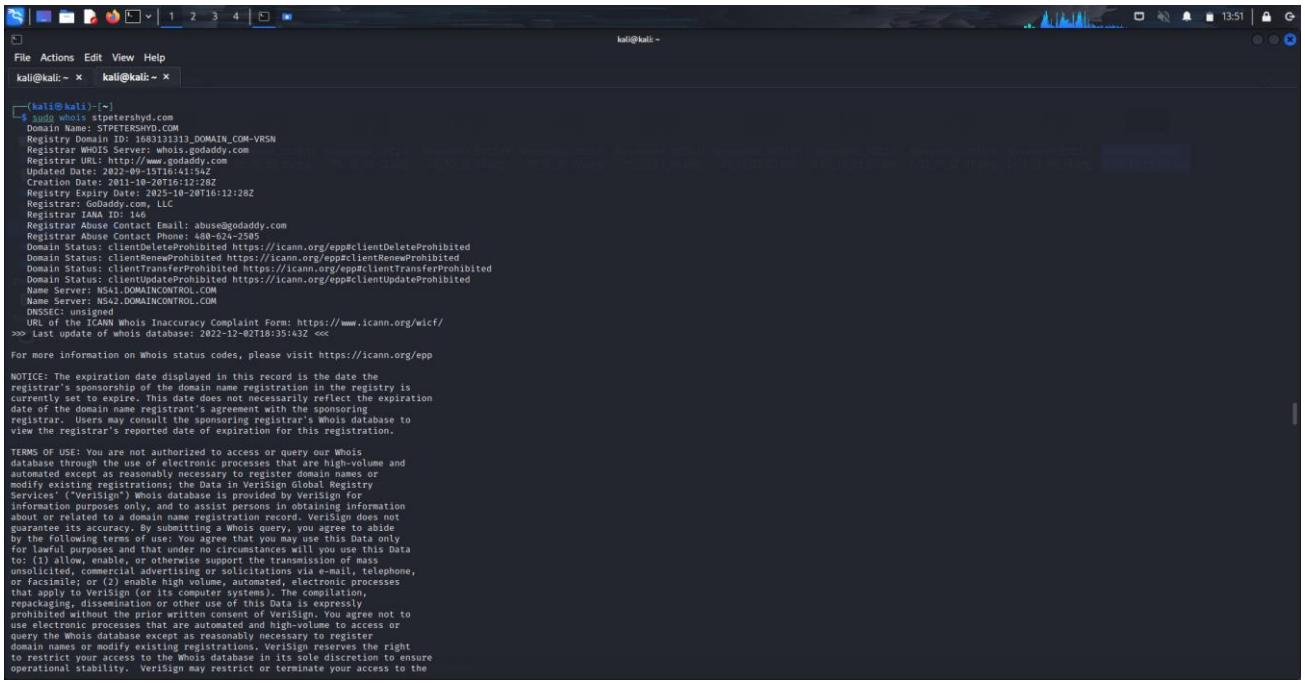




- Registry Domain ID: D15860-IN
- Registrar URL: http://www.markmonitor.com
- Updated Date: 2019-05-12T18:45:37Z
- Creation Date: 2005-02-11T11:14:14Z
- Registry Expiry Date: 2024-02-11T11:14:14Z
- Registrar: MarkMonitor Inc.
- Registrar IANA ID: 292
- Registrar Abuse Contact Email:
- Registrar Abuse Contact Phone:
- Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
- Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
- Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibitedRegistrant Organization: Amazon Technologies, Inc.
- Tech Email: Please contact the Registrar listed above
- Name Server: ns2.p31.dynect.net
- Name Server: ns1.p31.dynect.net
- Name Server: pdns1.ultradns.net
- Name Server: pdns6.ultradns.co.uk
- Name Server: pdns2.ultradns.net
- Name Server: pdns4.ultradns.org
- Name Server: pdns5.ultradns.info
- Name Server: pdns3.ultradns.org

1.3 Domain registration details of St. Peter's Engineering college website

Web Site Name : https://www.stpetershyd.com/

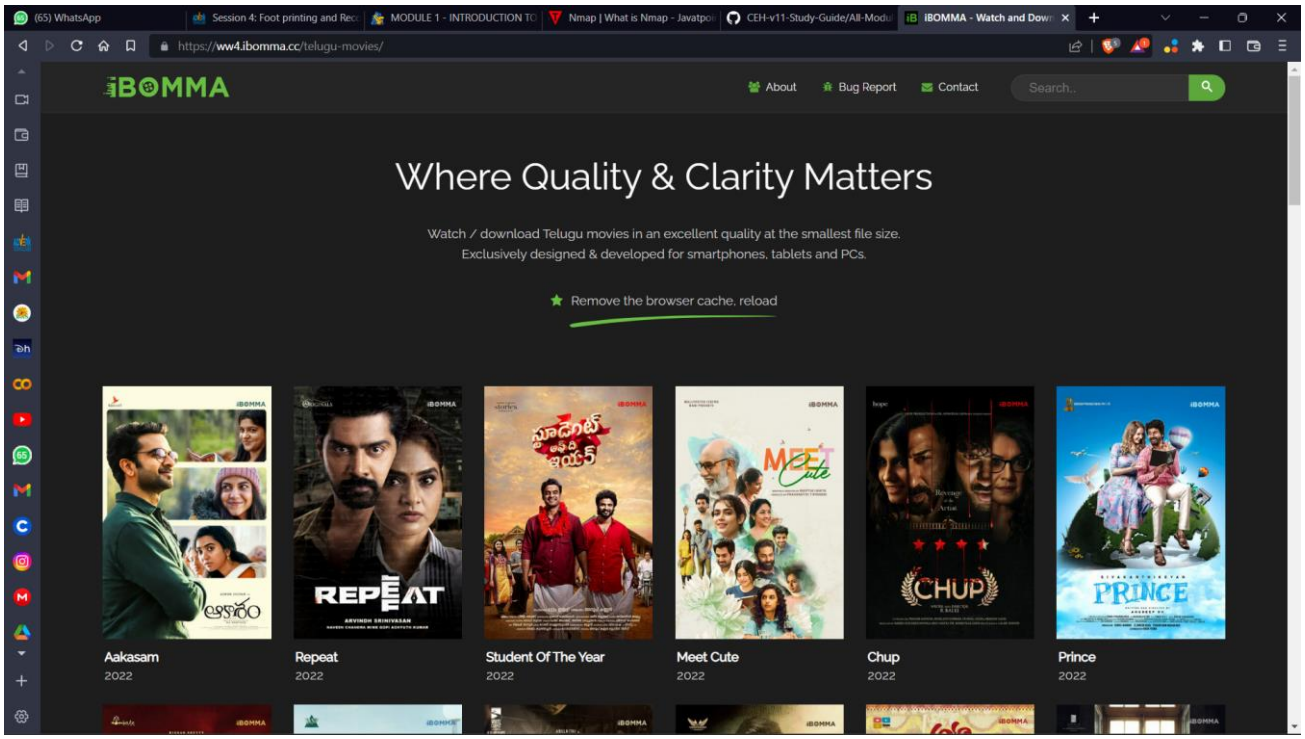


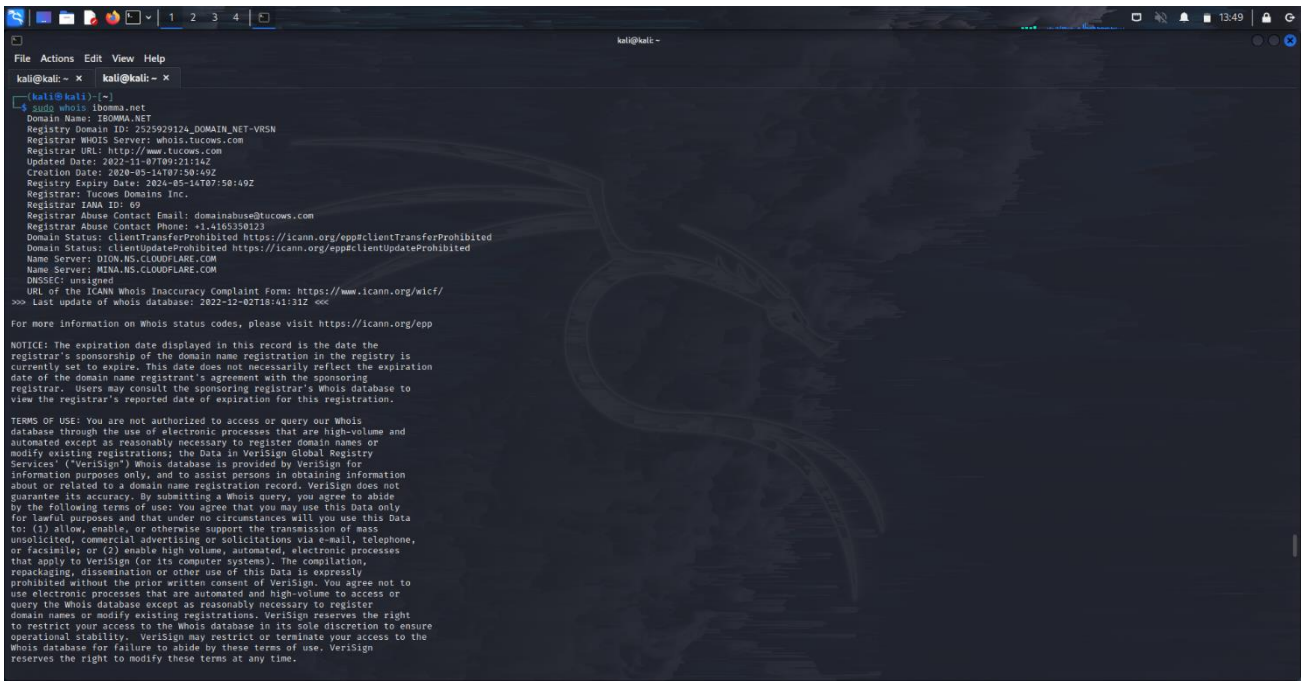
- Registry Domain ID: 1683131313_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.godaddy.com
- Registrar URL: https://www.godaddy.com
- Updated Date: 2020-10-26T01:54:40Z
- Creation Date: 2011-10-20T11:12:28Z
- Registrar Registration Expiration Date: 2025-10-20T11:12:28Z
- Registrar: GoDaddy.com, LLC
- Registrar IANA ID: 146
- Registrar Abuse Contact Email: abuse@godaddy.com
- Registrar Abuse Contact Phone: +1.4806242505
- Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
- Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
- Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
- Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
- Registry Registrant ID: Not Available From Registry
- Registrant Name: Registration Private
- Registrant Organization: Domains By Proxy, LLC
- Registrant Street: DomainsByProxy.com
- Registrant Street: 2155 E Warner Rd
- Registrant City: Tempe
- Registrant State/Province: Arizona
- Registrant Postal Code: 85284
- Registrant Country: US
- Registrant Phone: +1.4806242599
- Registrant Phone Ext:
- Registrant Fax: +1.4806242598
- Registrant Fax Ext:
- Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=STPETERSHYD.COM
- Registry Admin ID: Not Available From Registry
- Admin Name: Registration Private
- Admin Organization: Domains By Proxy, LLC
- Admin Street: DomainsByProxy.com
- Admin Street: 2155 E Warner Rd
- Admin City: Tempe
- Admin State/Province: Arizona
- Admin Postal Code: 85284
- Admin Country: US
- Admin Phone: +1.4806242599
- Admin Phone Ext:
- Admin Fax: +1.4806242598
- Admin Fax Ext:
- Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=STPETERSHYD.COM
- Registry Tech ID: Not Available From Registry
- Tech Name: Registration Private

- Tech Organization: Domains By Proxy, LLC
- Tech Street: DomainsByProxy.com
- Tech Street: 2155 E Warner Rd
- Tech City: Tempe
- Tech State/Province: Arizona
- Tech Postal Code: 85284
- Tech Country: US
- Tech Phone: +1.4806242599
- Tech Phone Ext:
- Tech Fax: +1.4806242598
- Tech Fax Ext:
- Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=STPETERSHYD.COM
- Name Server: NS41.DOMAINCONTROL.COM
- Name Server: NS42.DOMAINCONTROL.COM
- DNSSEC: unsigned

1.4 Domain registration details of IBOMMA website

Web Site Name : https://ww4.ibomma.cc/



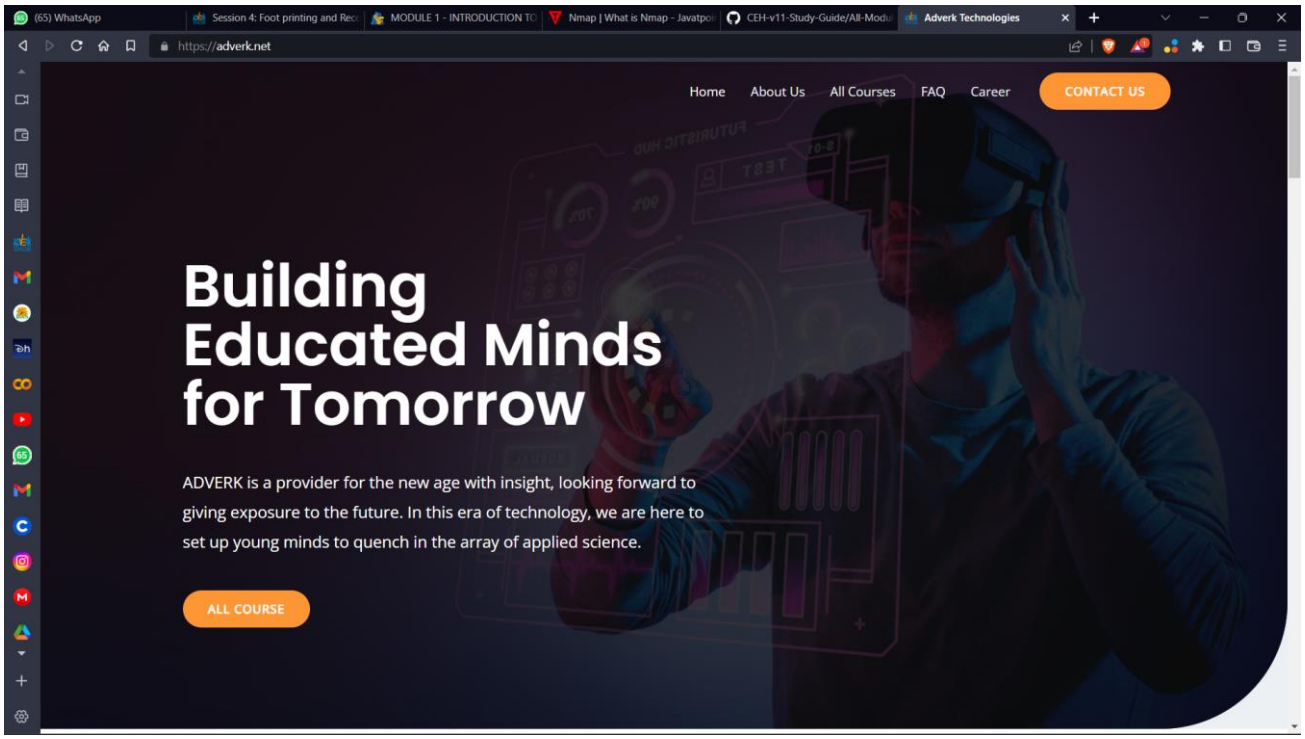


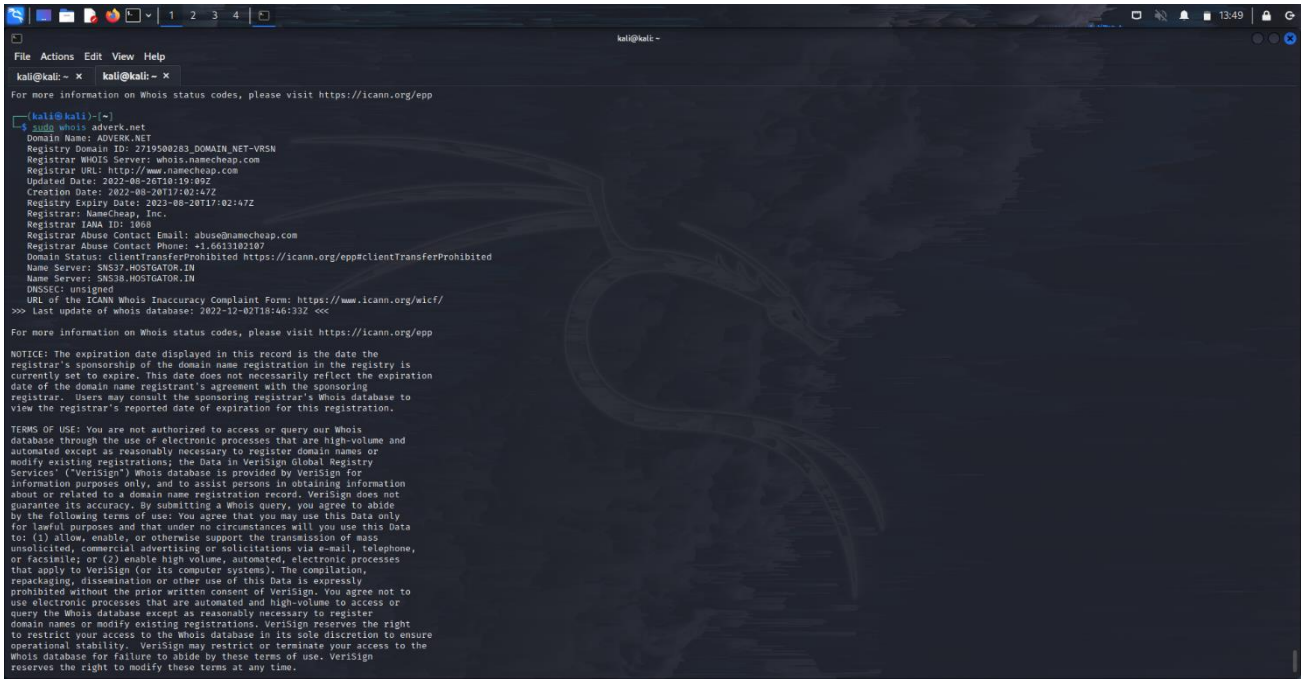
- Registry Domain ID: 2525929124_DOMAIN_NET-VRSN
- Registrar WHOIS Server: whois.tucows.com
- Registrar URL: http://tucowsdomains.com
- Updated Date: 2022-11-07T09:21:14
- Creation Date: 2020-05-14T07:50:49
- Registrar Registration Expiration Date: 2024-05-14T07:50:49
- Registrar: TUCOWS, INC.
- Registrar IANA ID: 69
- Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
- Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
- Registry Registrant ID:
- Registrant Name: REDACTED FOR PRIVACY
- Registrant Organization: REDACTED FOR PRIVACY
- Registrant Street: REDACTED FOR PRIVACY
- Registrant City: REDACTED FOR PRIVACY
- Registrant State/Province: Charlestown
- Registrant Postal Code: REDACTED FOR PRIVACY
- Registrant Country: KN
- Registrant Phone: REDACTED FOR PRIVACY
- Registrant Phone Ext:
- Registrant Fax: REDACTED FOR PRIVACY
- Registrant Fax Ext:
- Registrant Email: https://tieredaccess.com/contact/463a4c22-af3f-4c82-956a-8091bdfda4be
- Registry Admin ID:
- Admin Name: REDACTED FOR PRIVACY
- Admin Organization: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin City: REDACTED FOR PRIVACY
- Admin State/Province: REDACTED FOR PRIVACY
- Admin Postal Code: REDACTED FOR PRIVACY
- Admin Country: REDACTED FOR PRIVACY
- Admin Phone: REDACTED FOR PRIVACY
- Admin Phone Ext:
- Admin Fax: REDACTED FOR PRIVACY
- Admin Fax Ext:
- Admin Email: REDACTED FOR PRIVACY
- Registry Tech ID:
- Tech Name: REDACTED FOR PRIVACY
- Tech Organization: REDACTED FOR PRIVACY
- Tech Street: REDACTED FOR PRIVACY
- Tech City: REDACTED FOR PRIVACY
- Tech State/Province: REDACTED FOR PRIVACY
- Tech Postal Code: REDACTED FOR PRIVACY
- Tech Country: REDACTED FOR PRIVACY
- Tech Phone: REDACTED FOR PRIVACY
- Tech Phone Ext:
- Tech Fax: REDACTED FOR PRIVACY

- Tech Fax Ext:
- Tech Email: REDACTED FOR PRIVACY
- Name Server: dion.ns.cloudflare.com
- Name Server: mina.ns.cloudflare.com
- DNSSEC: unsigned
- Registrar Abuse Contact Email: domainabuse@tucows.com
- Registrar Abuse Contact Phone: +1.4165350123

1.5 Domain registration details of Adverk Technologies website

Web Site Name : https://adverk.net/



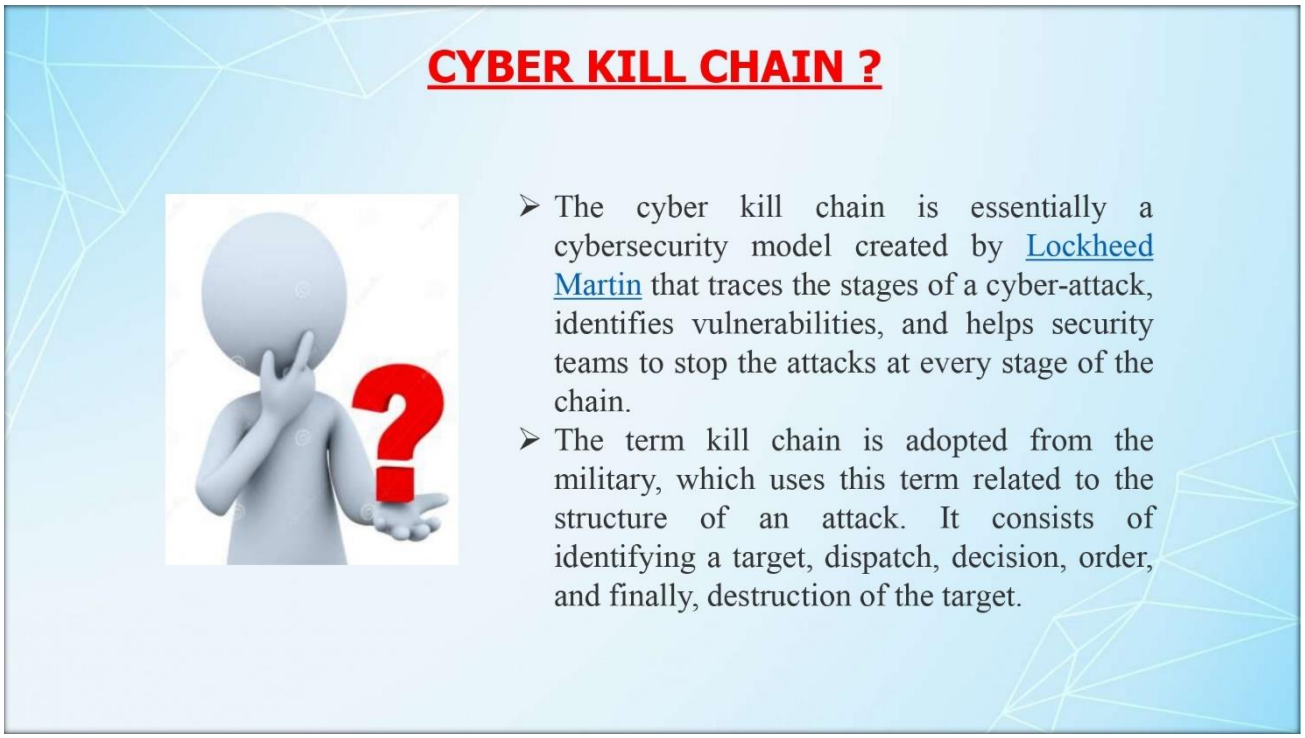


- Registry Domain ID: 2719500283_DOMAIN_NET-VRSN
- Registrar WHOIS Server: whois.namecheap.com
- Registrar URL: http://www.namecheap.com
- Updated Date: 0001-01-01T00:00:00.00Z
- Creation Date: 2022-08-20T17:02:47.00Z
- Registrar Registration Expiration Date: 2023-08-20T17:02:47.00Z
- Registrar: NAMECHEAP INC
- Registrar IANA ID: 1068
- Registrar Abuse Contact Email: abuse@namecheap.com
- Registrar Abuse Contact Phone: +1.9854014545
- Reseller: NAMECHEAP INC
- Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
- Registry Registrant ID:
- Registrant Name: Redacted for Privacy
- Registrant Organization: Privacy service provided by Withheld for Privacy ehf
- Registrant Street: Kalkofnsvegur 2
- Registrant City: Reykjavik
- Registrant State/Province: Capital Region
- Registrant Postal Code: 101
- Registrant Country: IS
- Registrant Phone: +354.4212434
- Registrant Phone Ext:
- Registrant Fax:
- Registrant Fax Ext:
- Registrant Email: ebbfc363a54248659e9546976b3748a3.protect@withheldforprivacy.com
- Registry Admin ID:
- Admin Name: Redacted for Privacy
- Admin Organization: Privacy service provided by Withheld for Privacy ehf
- Admin Street: Kalkofnsvegur 2
- Admin City: Reykjavik
- Admin State/Province: Capital Region
- Admin Postal Code: 101
- Admin Country: IS
- Admin Phone: +354.4212434
- Admin Phone Ext:
- Admin Fax:
- Admin Fax Ext:
- Admin Email: ebbfc363a54248659e9546976b3748a3.protect@withheldforprivacy.com
- Registry Tech ID:
- Tech Name: Redacted for Privacy
- Tech Organization: Privacy service provided by Withheld for Privacy ehf
- Tech Street: Kalkofnsvegur 2
- Tech City: Reykjavik
- Tech State/Province: Capital Region
- Tech Postal Code: 101
- Tech Country: IS
- Tech Phone: +354.4212434

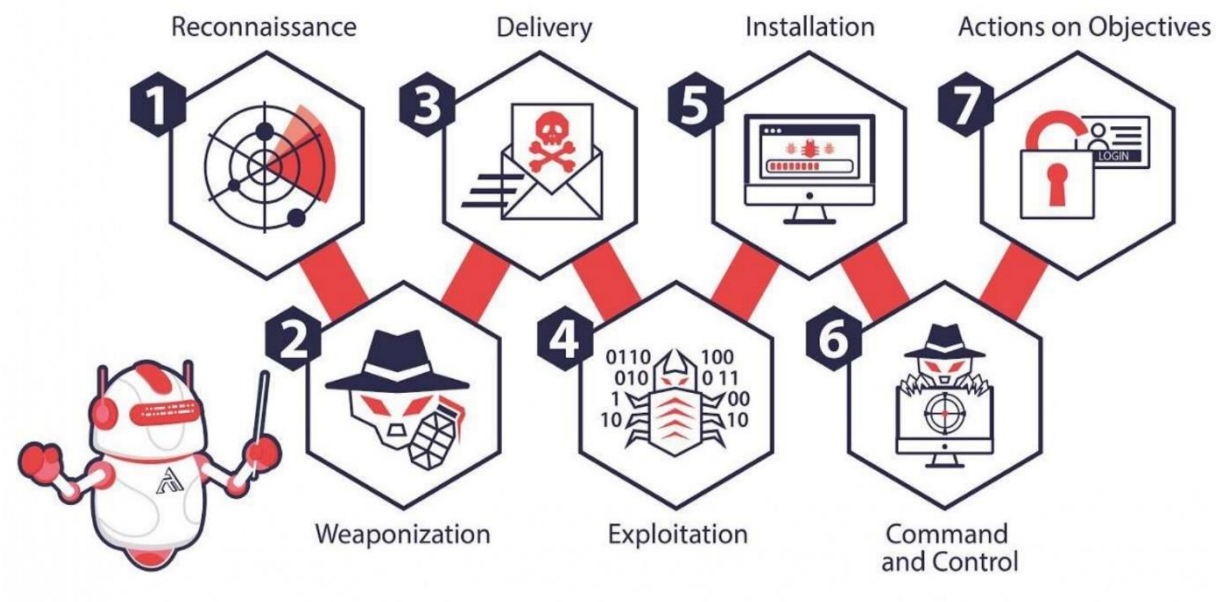
- Tech Phone Ext:
- Tech Fax:
- Tech Fax Ext:
- Tech Email: ebbfc363a54248659e9546976b3748a3.protect@withheldforprivacy.com
- Name Server: sns37.hostgator.in
- Name Server: sns38.hostgator.in
- DNSSEC: unsigned

2. PPT on Cyber Kill Chain

Aim : Use GHDB (Google Dorks) to find 10 admin login pages.



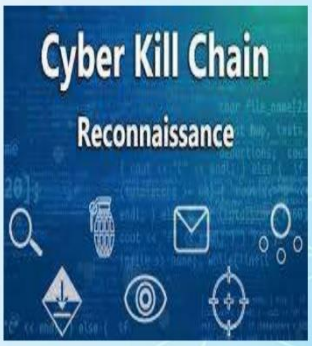
How does the Cyber Kill Chain Work?



The cyber kill chain consists of 7 distinct steps:

1.Reconnaissance

- ✓ The attacker collects data about the target and the tactics for the attack. This includes harvesting email addresses and gathering other information.
- ✓ Automated scanners are used by intruders to find points of vulnerability in the system. This includes scanning firewalls, intrusion prevention systems, etc to get a point of entry for the attack.

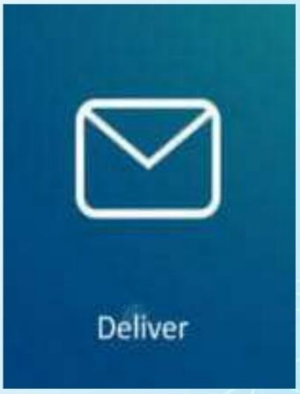


2.Weaponization

Attackers develop malware by leveraging security vulnerabilities. Attackers engineer malware based on their needs and the intention of the attack. This process also involves attackers trying to reduce the chances of getting detected by the security solutions that the organization has in place.

3.Delivery

The attacker delivers the weaponized malware via a phishing email or some other medium. The most common delivery vectors for weaponized payloads include websites, removable disks, and emails. This is the most important stage where the attack can be stopped by the security teams.



4.Exploitation

- The malicious code is delivered into the organization's system. The perimeter is breached here. And the attackers get the opportunity to exploit the organization's systems by installing tools, running scripts, and modifying security certificates.
- Most often, an application or the operating system's vulnerabilities are targeted. Examples of exploitation attacks can be scripting, dynamic data exchange, and local job scheduling.

5.Installation

A backdoor or remote access trojan is installed by the malware that provides access to the intruder. This is also another important stage where the attack can be stopped using systems such as HIPS (Host-based Intrusion Prevention System).

6.Command and Control

The attacker gains control over the organization's systems and network. Attackers gain access to privileged accounts and attempt brute force attacks, search for credentials, and change permissions to take over the control.

7.Actions on Objective

The attacker finally extracts the data from the system. The objective involves gathering, encrypting, and extracting confidential information from the organization's environment.

Based on these stages, the following layers of control implementation are provided:

1. Detect – Determine the attempts to penetrate an organization.
2. Deny – Stopping the attacks when they are happening.
3. Disrupt – Intervene is the data communication done by the attacker and stops it then.
4. Degrade – This is to limit the effectiveness of a cybersecurity attack to minimize its ill effects.
5. Deceive – Mislead the attacker by providing them with misinformation or misdirecting them.
6. Contain – Contain and limit the scope of the attack so that it is restricted to only some part of the organization.

The following security controls can be used to control the attraction at various stages of the kill chain, according to Orion Cassetto of Exabeam:

Reconnaissance

Detect: Web Analytics; Threat Intelligence; Network Intrusion Detection System
Deny: Information Sharing Policy; Firewall Access Control Lists

Weaponization

Detect: Threat Intelligence; Network Intrusion Detection System
Deny: Network Intrusion Prevention System

Delivery

Detect: Endpoint Malware Protection
Deny: Change Management; Application Whitelisting; Proxy Filter; Host-Based Intrusion Prevention System
Disrupt: Inline Anti-Virus
Degrade: Queuing
Contain: Router Access Control Lists; App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System

Exploitation

Detect: Endpoint Malware Protection; Host-Based Intrusion Detection System
Deny: Secure Password; Patch Management
Disrupt: Data Execution Prevention
Contain: App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System

Installation

Detect: Security Information and Event Management (SIEM); Host-Based Intrusion Detection System
Deny: Privilege Separation; Strong Passwords; Two-Factor Authentication
Disrupt: Router Access Control Lists
Contain: App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System

Command & Control

Detect: Network Intrusion Detection System; Host-Based Intrusion Detection System
Deny: Firewall Access Control Lists; Network Segmentation
Disrupt: Host-Based Intrusion Prevention System
Degrade: Tarpit
Deceive: Domain Name System Redirect
Contain: Trust Zones; Domain Name System Sinkholes

Actions on Objectives

Detect: Endpoint Malware Protection
Deny: Data-at-Rest Encryption
Disrupt: Endpoint Malware Protection
Degrade: Quality of Service
Deceive: Honeypot
Contain: Incident Response

Exfiltration

Detect: Data Loss Prevention; Security Information and Event Management (SIEM)
Deny: Egress Filtering
Disrupt: Data Loss Prevention
Contain: Firewall Access Control Lists"

How can Cyber Kill Chain Protect Against Attacks?

1.Simulate Cybersecurity Attacks

- Real cybersecurity attacks can be simulated across all vectors to find vulnerabilities and threats. This includes simulating cyber-attacks through email gateways, web gateways, web application firewall, and similar more.

2.Evaluate the Controls to Identify Security Gaps

- This involves evaluating simulations and identifying the areas of risk. Simulation platforms give you a detailed risk score and report around every vector.

3.Remediate and Fix the Cybersecurity Gaps

- The next step is to fix the security gaps that were identified in the previous step. This may include steps like installing patches and changing configurations to reduce the number of threats and vulnerabilities in the organization's system.

CONCLUSION

Network test assignment is the most important way of ethical hacking for putting and storing information asset in secure way. The best three advantages of ethical hacking are ,improving the overall protective postures, providing security against the intellectual property thieves and fulfilling legislative mandates. The majority of Information Technology organizations are conducting their ethical hacking on wireless and wireline networks, operating systems and applications in frequent way or annual search .There is no single unique set of methodology for move on with ethical hacking. The reference terms are used for different phases in the hacking anatomy might vary, but includes are similar. Hacking is not for everyone but for an objective mind set. A lot of free time, dedication is needed to keep up with hacking process and they never use the knowledge to the purposes of offence. The lack of the experienced staff is mostly cited as significant challenge in conducting ethical hacking internally and improving the capabilities of ethical hacking.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe