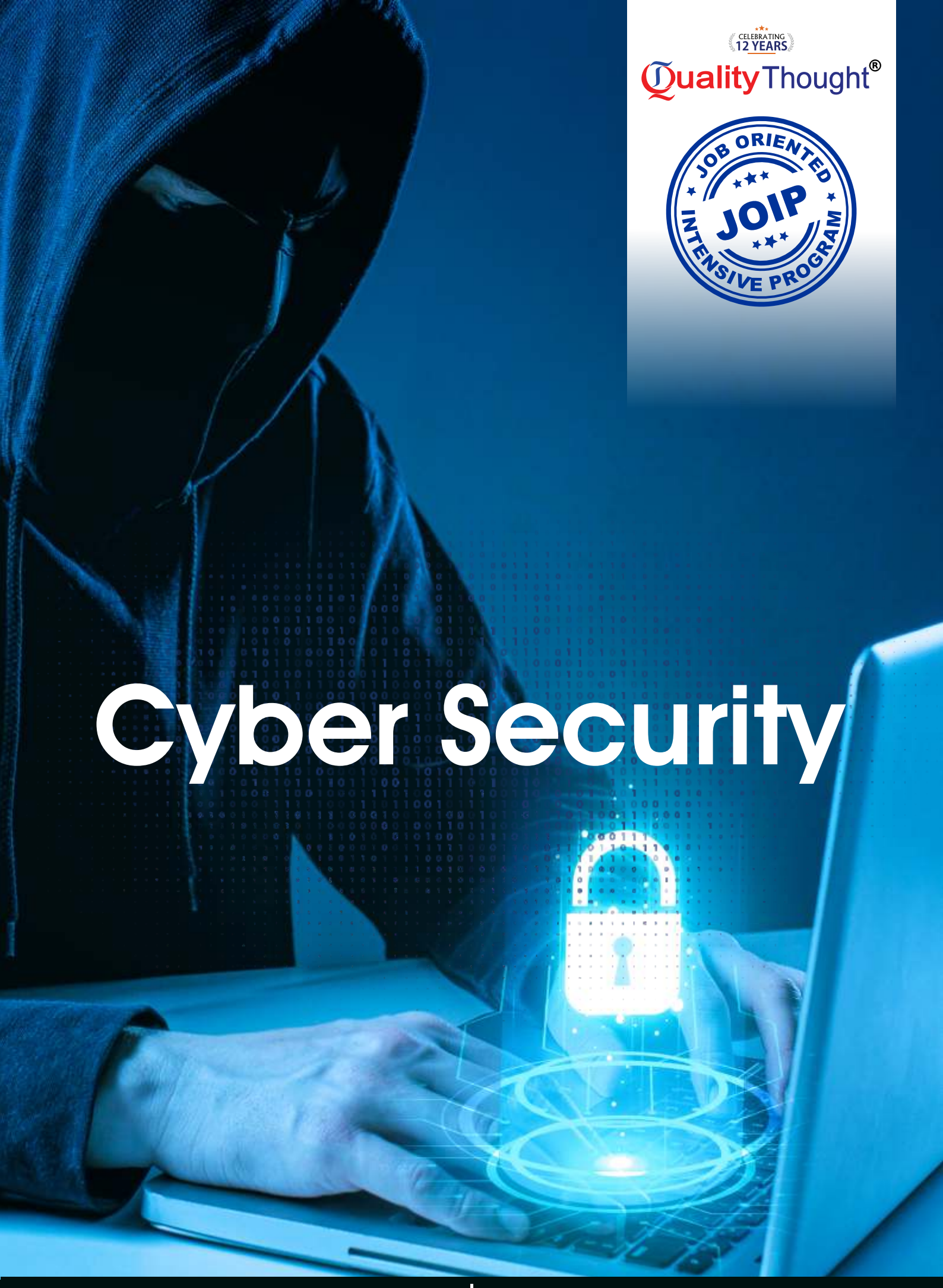
CELEBRATING
12 YEARS
QualityThought®
JOB ORIENTED
JOIP
INTENSIVE PROGRAM
Cyber Security

CELEBRATING 12 YEARS

Quality Thought®

# Cyber Security

## Networking Basics

- Introduction to Networks
- Types of Networks
- Types of Topologies
- IP address, Ports
- Protocols and Protocol types
- OSI layers and protocols
- Networking Devices and Advanced Networking Devices
- Wireless technologies
- Virtualization and network storage
- Security policies
- Physical Security Devices
- Authentication and Access Control
- Common Networking Attacks
- Network Troubleshooting
- Network Hardware tools and Software tools

## Introduction To Ethical Hacking

- **Information security overview**
- **Elements of information security**
- **Motives, goals and objects of information security attacks**
- **Classification of attacks**
- Passive attacks
- Active attacks
- Close-in-attacks
- Insider attacks
- Distribution attacks

## Information warfare

- Command and control warfare
- Intelligence-based warfare
- Electronic warfare
- Psychological warfare
- Hacker warfare
- Economic warfare
- Cyber warfare
- Defensive information warfare
- Offensive information warfare

## Cyber kill chain concepts (*)

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and control
- Actions on objects

## Tactics, techniques and procedures (TTPs) Adversary behavioural identification

- Internal reconnaissance
- Use of PowerShell
- Unspecified proxy activities
- Use of command-line interface
- Http user agent
- Command and control server
- Use of DNS Tunnelling
- Use of web shell
- Data staging

## Indicators of compromise Categories of indicators of compromise

- Email indicators
- Network indicators
- Host-based indicators
- Behavioural indicators

## Hacking concepts

- Hacker classes
- Phases of hacking

## Ethical hacking concepts

- What and why ethical hacking
- Scope and limitations of an ethical hacker
- Skills of an ethical hacker

## Types of threat intelligence

- Strategic threat intelligence
- Tactical threat intelligence
- Operational threat intelligence
- Technical threat intelligence

## Threat modelling

- Identify security objectives
- Application overview
- Identify roles
- Identify key usage scenarios
- Identify technologies
- Identify application security mechanisms

## Decompose the application

- Identify trust boundaries
- Identify data flows
- Identify entry points
- Identify exit points
- Identify threats
- Identify vulnerabilities

## Incident management Incident handling and response

- Preparation
- Incident recording and assignment
- Incident triage
- Notification
- Containment
- Evidence gathering and forensic analysis
- Eradication
- Recovery
- Post-incident activities

## Role of AI and ML in cyber security

- Supervised learning
- Unsupervised learning

## How do AI and ML prevent cyber-attacks?

- Password protection and authentication
- Phishing detection and prevention
- Threat detection
- Vulnerability management
- Behavioural analytics
- Network security
- AI-based antivirus
- Fraud detection
- Botnet detection
- AI to combat AI threats

## Information security laws and standards

- Payment card industry Data security standard (PCI DSS) ISO/IEC 27001:2013
- Health Insurance Probability and Accountability Act (HIPAA)
- Electronic transactions and code set standards
- Privacy rule
- Security rule
- Employer identifier standard
- National provider identifier standard (NPI)
- Enforcement rule
- **Sarbanes Oxley Act (SOX)**
- **The digital millennium copyright Act (DMCA)**
- **The Federal Information security Management Act (FISMA)**
- **Cyber laws in different countries**

# Footprinting And Reconnaissance

## Foot-printing concepts

**What is footprinting and types?**

- Active footprinting
- Passive footprinting

**Information obtained in foot printing**

- Organization footprinting
- Network footprinting
- System footprinting

**Objectives of footprinting**

- Know security posture
- Reduce focus area
- Identify vulnerabilities
- Draw network map

## Footprinting threats

- Social engineering
- System and network attacks
- Information leakage
- Privacy loss
- Corporate espionage
- Business loss

## Footprinting methodology

- Footprinting through search engines
- Footprinting using advanced search operators (GHDB)
- VoIP and VPN footprinting through GHDB
- Gathering information using google advanced search.
- Gathering information from video search engines
- Gathering information from Meta search engines
- Gathering information from ftp search engines
- Gathering information from IOT search engines
- Footprinting through web services
- Finding company's TLD's and sub-domains
- Finding geographical locations of the target
- Footprinting through social networking sites
- Website footprinting
- Gathering information from financial services
- Footprinting through job sites
- Deep web and Dark web footprinting
- VoIP and VPN footprinting through shodan
- Competitive intelligence gathering
- Information gathering using groups forums and blogs
- Footprinting using website mirrors
- Footprinting using web spiders
- Footprinting using wayback archive
- Email footprinting
- Whois footprinting
- DNS footprinting
- Network footprinting
- Footprinting through social engineering

CELEBRATING 12 YEARS

Quality Thought®

# Cyber Security

## Scanning Networks

### Overview of network scanning

### Types of scanning

- Port scanning
- Network scanning
- Vulnerability scanning

**Objectives of network scanning**

**Tcp communication flags**

**TCP/IP communication**

### Host discovery

- Arp ping scan
- Udp ping scan
- Icmp ping scan
- Icmp echo ping sweep
- Icmp timestamp ping
- Icmp address mask ping
- Tcp ping scan
- Ip protocol scan

### Port and service discovery

- Open tcp scanning methods
- Stealth tcp scanning methods
- Third party and spoofed tcp scanning methods

### Os discovery (banner grabbing/ os fingerprinting)

- Active banner grabbing
- Passive banner grabbing

### Scanning beyond IDS and Firewall

**Ids/firewall evasion techniques**

- Packet fragmentation
- Source routing
- Source port manipulation
- Ip address decoy
- Ip address spoofing
- Creating custom spoofing
- Randomizing host order
- Sending bad checksum
- Proxy servers
- Anonymizes

## Enumeration

### Enumeration concepts

**Techniques for enumeration**

- Extract usernames using email ids
- Extract information using default passwords
- Brute force active directory
- Extract information using DNS zone transfer
- Extract user groups from windows
- Extract usernames using SNMP

### Service and ports enumerate

- NetBIOS enumeration
- Snmp enumeration
- LDAP enumeration
- NTP and NFS enumeration
- SMTP and DNS enumeration
- MySQL enumeration
- FTP enumeration
- Telnet enumeration
- Http/https enumeration
- Ssl/tls enumeration
- Smb enumeration

**Enumeration countermeasures**

## Vulnerability Analysis

### Vulnerability assessment concepts

- Vulnerability research

### Vulnerability classification and assessment types

**Vulnerability management life-cycle**

·Identify assets and create a baseline
·Vulnerability scan
·Risk assessment
·Remediation
·Verification
·Monitor

**Vulnerability classifications**

·Misconfiguration
·Default installations
·Buffer overflows
·Unpatched servers
·Design flaws
·Operating system flaws
·Application flaws
·Open services
·Default passwords

**Types of vulnerability assessment**
- Active assessment
- Passive assessment
- External assessment
- Internal assessment
- Host based assessment
- Network based assessment
- Application assessment
- Database assessment
- Wireless network assessment
- Distributed assessment
- Credentialed assessment
- Non-credentialed assessment
- Manual assessment
- Automated assessment

## Vulnerability assessment solutions and tools

### Comparing approaches of vulnerability assessment
- Product-based assessment
- Service based-assessment
- Tree-based assessment
- Inference-based assessment

### Characteristics of a good vulnerability assessment solutions

### Working os vulnerability scanning solutions

### Types of vulnerability assessment tools
- Host-based vulnerability assessment tools
- Depth assessment tools
- Application-layer vulnerability assessment tools
- Scope assessment tools
- Active and passive tools
- Location and data examination tools

**Vulnerability assessment reports**

## System Hacking

### System hacking concepts
- Footprinting module
- Scanning module
- Enumeration module
- Vulnerability analysis module

### Gaining access

**Cracking passwords**
- Security accounts manager (SAM)
- Database NTLM authentication
- Kerberos authentication

**Password cracking**

**Types of password cracking**

**Non-electronic attacks**
- Social engineering
- Shoulder surfing
- Dumpster diving

**Active online attacks**
- Dictionary attack
- Brute-force attack
- Rule-based attack
- Password guessing
- Default passwords
- Trojan/spyware/keylogger
- Hash injection/pass-the-hash (path) attack
- LLMNR/NBT-NS poisoning
- Internal monologue attack
- Cracking Kerberos password
- Pass the ticket attack
- Combinatory attack
- Fingerprint attack
- Prince attack
- Toggle-case attack
- Markov-chain attack

**Passive online attacks**
- Wire sniffing
- Man-in-the-middle and replay attacks

**Offline attacks**
- Rainbow table attack
- Distributed network attack

### Password recovery tools
- Elcomsoft distributed password recovery
- Password recovery toolkit
- Passware kit forensic
- Hash cat
- Windows password recovery tool
- Pcunlocker

**How to defend against password cracking**

**How to defend against LLMNR/NBT-NS poisoning**

## Buffer overflow

- Types of buffer overflow
- Stack-based buffer overflow
- Heap-based buffer overflow

**Windows buffer overflow exploitation**
**Escalating privileges**
**Types of privilege escalation**

- Horizontal privilege escalation
- Vertical privilege escalation

**Privilege escalation using DLL Hijacking**
**Privilege escalation by exploiting vulnerabilities**
**Privilege escalation using Dylib hijacking**
**Privilege escalation using spectre and meltdown vulnerabilities**
**Privilege escalation using named pipe impersonation**
**Privilege escalation by exploiting is configured services**
**Pivoting and relaying to hack external machines**
**Defend against privilege escalation**

## Maintaining access

- Executing applications
- Backdoors
- Crackers
- keylogger
- Spyware

## Remote code execution techniques

- Exploitation for client execution
- Web-browser-based exploitation
- Office-application-based exploitation
- Third-party applications-based exploitation

## Remote code execution techniques

- Exploitation for client execution
- Web-browser-based exploitation
- Office-application-based exploitation
- Third-party applications-based exploitation

**Scheduled task**
**Service execution**
**Windows management instrumentation (WMI)**
**Windows remote management (WimRM)**

## Keylogger

**Types of keyloggers**
**Hardware keylogger**

- Pc/BIOS embedded
- Keylogger keyboard
- External keylogger
- Ps/2 and usb keylogger
- Acoustic/CAM keylogger
- Bluetooth keylogger
- Wi-Fi keylogger software keylogger
- Application keylogger
- Kernel keylogger
- Hypervisor-based keylogger
- Form grabbing based keylogger
- JavaScript based keylogger
- Memory injection based keylogger

## Spyware

**Types of spyware**

- Desktop spyware
- Email spyware
- Internet spyware
- Child-monitoring spyware
- Screen-capturing spyware
- Usb spyware
- Audio spyware
- Video spyware
- Print spyware
- Telephone/cell phone spyware
- Gps spyware

## Anti-keyloggers
## Anti-spywares
## Rootkits

- Types of rootkits
- Hypervisor-level rootkit
- Hardware/firmware rootkit
- Kernel-level rootkit
- Boot-loader-level rootkit
- Application-level/user-mode rootkit
- Library-level rootkits

**How to defend from rootkits**
**Anti-rootkits**

## Steganography

**Technical steganography**

- Invisible ink
- Microdots

**Computer based methods**

- Substitution techniques
- Transform domain techniques
- Spread spectrum techniques
- Statistical techniques
- Distortion techniques
- Cover generation techniques

**Linguistic steganography**

**Semagrams**

- Visual semagrams
- Text semagrams

Open codes

Jargon codes

Covered ciphers

- Null ciphers
- Grille ciphers

## Types of steganography

- Image steganography
- Document steganography
- Folder steganography
- Video steganography
- Audio steganography
- Whitespace steganography
- Web steganography
- Spam/email steganography
- DVD-Rom steganography
- Natural steganography
- Hidden os steganography
- C++ source-code steganography

## Steganalysis

**Steganalysis methods/attacks on steganography**

- Stego-only attack
- Known-stego attack
- Known-message attack
- Known-cover attack
- Chosen-message attack
- Chosen-stego attack
- Chi-square attack
- Distinguishing statistical attack
- Blind classifier attack

## Clearing logs

- Techniques used for covering tracks
- Disabling auditing
- Clearing logs
- Manipulating logs
- Covering tracks on the network
- Covering tracks on the os
- Deleting files
- Disabling windows functionality

# MALWARE THREATS

## Malware concepts

- Introduction to malware
- Different ways for malware to enter a system
- Instant messenger applications
- Portable hardware media/removable devices
- Browser and email software bugs
- Insecure patch management
- Rouge/decoy applications
- Untrusted sites and free web applications/software
- Downloading files from internet
- Email attachments
- Network propagation
- File sharing
- Installation by other malware
- Bluetooth and wireless network

## Common techniques attackers use to distribute malware on the web

- Black hat search engine optimization (SEO)
- Social engineered click-jacking
- Spear-phishing sites
- Malverstising
- Compromised legitimate websites
- Drive-by downloads
- Spam emails

## Components of malware

- Crypter
- Downloader
- Dropper
- Exploit
- Injector
- Obfuscator
- Packer
- Payload
- Malicious code

**Characteristics of advanced persistent threat**
- Objectives
- Timeliness
- Resources
- Risk tolerance
- Skills and methods
- Actions
- Attack origination points
- Numbers involved in the attack
- Knowledge source
- Multi-phased
- Tailored to the vulnerabilities
- Multiple points to entries
- Evading signature-based detection systems
- Specific warning signs

**Advance persistent life-cycle**
- Preparation
- Initial intrusion
- Expansion
- Persistence
- Search and exfiltration
- clean-up

## Trojan concepts
- Types of Trojans
- Remote access Trojans
- Backdoor Trojans
- Botnet Trojans
- Rootkit Trojans
- E-banking Trojans
- Point-of-sale Trojans
- Defacement Trojans
- Service protocol Trojans
- Mobile Trojans
- IOT Trojans
- Security software disabler Trojans
- Destructive Trojans
- Ddos attack Trojans
- Command shell Trojans

## Virus and worms concepts
**Introduction to viruses**
**Characteristics of viruses**
**Stages of virus lifecycle**
- Design
- Replication
- Launch
- Detection
- Incorporation
- Execution of the damage routine

**Types of viruses**
- System or boot sector virus
- File virus
- Multipartite virus
- Macro virus
- Cluster virus
- Stealth/tunnelling virus
- Encryption virus
- Sparse infector virus
- Polymorphic virus
- Metamorphic virus
- Overwriting file or cavity virus
- Companion virus/camouflage virus
- Shell virus
- File extension virus
- Fat virus
- Logic bomb virus
- Web scripting virus
- Email virus
- Armored virus
- Add-on virus
- Intrusive virus
- Direct action or transient virus
- Terminate and stay resident virus

## Fileless malware concepts
- Fileless techniques used by attackers
- Phishing emails
- Legitimate applications
- Native applications
- Infection through laternal movement
- Malicious websites
- Registry manipulation
- Memory code injection
- Script based injection

**Taxonomy of fileless malware types**
- No file activity performed
- Indirect file activity
- Required files to operate
- Exploits
- Hardware
- Execution and injection

**Launching fileless malware through document exploits**
**Launching fileless malware through in-memory exploits**
**Launching fileless malware through script-based injection**
**Launching fileless malware by exploiting system admin tools**
**Launching fileless malware through phishing**
**Maintaining persistence with fileless techniques**

## SNIFFING

**Sniffing concepts**

**Types of sniffing**

- Active sniffing
- Mac flooding
- Dns poisoning
- Arp poisoning
- Dhcp attacks
- Switch port stealing
- Spoofing attack

**Passive sniffing**

- Compromising physical security
- Using a Trojan horse

**Protocols vulnerable for sniffing**

- Telnet and rlogin
- Http
- Snmp
- SMTP
- Nntp
- Pop
- Ftp
- Imap

**Wiretapping and methods**

- Active wiretapping
- Passive wiretapping

**Sniffing technique: MAC attacks Sniffing Technique: DHCP attacks**

**Sniffing Technique: ARP poisoning**

**Sniffing Technique: spoofing attacks**

**Sniffing Technique: DNS poisoning**

**Countermeasures**

**Sniffing Detection Techniques**

## SOCIAL ENGINEERING

**Social engineering concepts**

**Common targets of social engineering**

- Receptionists and help-desk personnel
- Technical support executives
- System administrators
- Users and clients
- Vendors of the target organization
- Senior executives

## Impact of social engineering

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitration
- Temporary or permanent closure

## Behaviours vulnerable to attacks

- Authority
- Intimidation
- Consensus or social proof
- Scarcity
- Urgency
- Familiarity or liking
- Trust
- Greed

## Factors that make companies vulnerable to attacks

- Insufficient security training
- Unregulated access to information
- Several organizational units
- Lack of security policies

## Phases of social engineering attacks

- Research the target company
- Select a target
- Develop a relationship
- Exploit the relationship

## Social engineering techniques

**Human based social engineering**

- Impersonation
- Vishing
- Tailgating
- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Reverse social engineering
- Piggybacking
- Diversion theft
- Honey trap
- Baiting
- Quid pro quo
- Elicitation

**Computer based social engineering**

- Phishing
- Spam mail
- Pop-up window attacks
- Scareware
- Instant chat messenger Mobile based social engineering
- Publishing malicious apps
- Using fake security applications
- Repackaging legitimate apps
- Smishing (sms phishing)

## Insider threats

**Types of insider threats**

- Malicious insider
- Negligent insider
- Professional insider
- Compromised insider

## Behavioural indications of an insider threat

- Alerts of data exfiltration
- Missing or modified network logs
- Changes in network usage patterns
- Multiple failed login attempts
- Behavioural and temporal changes
- Unusual time and location of access
- Missing or modified critical data
- Unauthorized download or copying of sensitive data
- Sending sensitive information to personal email account
- Logging of different user accounts from different systems
- Temporal changes in revenue or expenditure
- Unauthorized access to physical assets
- Increase or decrease in productivity of employee
- Inconsistent working hours, unusual business activities, and concealed or frequent foreign trips
- Extreme behaviour due to mental instability
- Signs of vulnerability (such as drug or alcohol abse, financial difficulties, gambling, illegal activities)
- Complaint on sensitive data leak
- Abnormal access of systems and user accounts
- Irresponsible social media behaviour
- Attempt to access restricted zones

**Impersonation on social networking sites**

## Identity theft

**Types of identity theft**

- Child identity theft
- Criminal identity theft
- Financial identity theft
- Driver license identity theft
- Insurance identity theft
- Medical identity theft
- Tax identity theft
- Identity cloning and concealment
- Synthetic identity theft
- Social identity theft

## Techniques attackers use to obtain identity

- Theft of wallets, phones
- Internet searches
- Social engineering
- Dumpster diving and shoulder surfing
- Phishing
- Skimming
- Pretexting
- Pharming
- Hacking
- Keyloggers and password stealers
- War diving
- Mail theft and rerouting

**Countermeasures**

## DENIAL OF SERVIC

**Dos/DDos concepts**

**Basic dos/ddos attack vectors**

- Volumetric attacks
- Protocol attacks
- Application layer attack
- Dos/DDOs attack techniques
- Udp flood attack
- ICMP flood attack
- Pod attack
- Smurf attack
- Pulse wave attack
- Zero-day attack
- Syn flood attack
- Fragmentation attack
- Ack flood attack
- Tcp state exhaustion attack
- Spoofed session flood attack
- Https get/post attack
- Slowloris attack
- Udp application layer flooded attack
- Multi-vector attack
- Peer-to-peer attack
- Permanent Dos (PDoS) attack
- Distributed reflection DoS (DRDoS) attack
- Countermeasures

## SESSION HIJACKING

**Session hijacking concepts**

**Types of session hijacking**

- Active session hijacking
- Passive session hijacking

### Session hijacking in OSI model

- Network level hijacking
- Application level hijacking

### Application level session hijacking

- Session sniffing
- Predictable session token
- Man-in-the-middle attack
- Man-in-the-browser attack
- cross-site-scripting attack
- Cross-site request forgery
- Session reply attack
- Session fixation attack
- CRIME attack
- Forbidden attack
- Session donation attack

### Network level session hijacking

- Blind attack
- Udp hijacking
- TCP/IP hijacking
- Rst hijacking
- Man-in-the-middle
- Ip spoofing

**Countermeasures**

### IDS, IPS, Firewall, and Honeypot concepts

### Types of intrusion detection systems

- Network-based intrusion detection system
- Host-based intrusion detection system

### Types of IDS alerts

- True positive
- False positive
- False negative
- True negative

### Firewall architecture

- Bastion host
- Screened subnet
- Multi homed firewall

### Demilitarized zone (DMZ)

### Types of firewalls

- Hardware firewalls
- Software firewalls

### Firewall technologies

- Packet filtering
- Circuit-level gateways
- Application-level firewall
- Stateful multilayer firewall
- Application proxies
- Virtual private network
- Network address translation

### Honeypots and types of honeypots

- Low-interaction honeypots
- Medium-interaction honeypots
- High-interaction honeypots
- Pure honeypots
- Production honeypots
- Research honeypots
- Malware honeypots
- Database honeypots
- Spam honeypots
- Email honeypots
- Spider honeypots
- Honey nets

### IDS, IPS, Firewall, and Honeypot solutions

### Evading IDS

### IDS evasion techniques

- Insertion attack
- Evasion
- Denial-of-service attack
- Obfuscation
- False positive generation
- Session splicing
- Unicode evasion
- Fragmentation attack
- Overlapping fragmentation
- Time-to-live attacks
- Invalid RST packets
- Urgency flag
- Polymorphic shell code
- ASCII shell code
- Application-layer attacks
- DE synchronization
- Encryption
- Flooding

CELEBRATING 12 YEARS

Quality Thought®

# Cyber Security

## Evading Firewalls

**Session hijacking concepts**
**Types of session hijacking**
- Port scanning
- Firewalking
- Banner grabbing
- ip address spoofing
- Source routing
- Tiny fragments
- Using an ip address in place of a url
- Using anonymous website surfing sites
- Using a proxy server
- Icmp tunnelling
- Ack tunnelling
- Http tunnelling
- Ssh tunnelling
- Dns tunnelling
- Through external systems
- Through mitm attack
- Through content
- Through xss attack

**Detecting honeypots**

## HACKING WEB SERVERS

**Web server concepts**
**Web server operations**
**Components of web server**
- Document root
- Server root
- Virtual Document root
- Virtual hosting
- Web proxy

### Web server attacks
- Dos/ddos attacks
- Domain name system (DNS) server hijacking
- DNS amplification
- Directory traversal
- Man in the middle/sniffing
- Phishing
- Website defacement
- Web server misconfiguration
- Http response splitting
- Web cache poisoning
- Secure shell brute force
- Web server password cracking
- Server side request forgery

### Web server methodology
- Information gathering
- Web server foot printing
- Website mirroring
- Vulnerable scanning
- Session hijacking
- Web server passwords hacking

**Countermeasures**

## HACKING WEB APPLICATIONS

### Web application concepts
- Introduction to web applications
- Web application architecture
- Vulnerability stack

### Web application threats
- Injection
- Sql injection
- Command injection
- shell injection
- Html injection
- File injection
- Ldap injection
- Server side js injection
- Log injection
- Crlf injection attack

### Broken authentication
- Session id in urls
- Password exploitation
- Timeout exploitation

**Sensitive data exposure**
**Xml external entity**
**Broken access control**

### Broken authentication
- Insecure direct object reference
- Missing function level access control

### Security misconfiguration
- Unvalidated inputs
- Parameter/form tampering
- Improper error handling
- Insufficient transport layer protection
- Server software flaws
- Enabling unnecessary services
- Improper authentication
- Unpatched security flaws
- Server configuration problems

## Cross site scripting

- Malicious script execution
- Redirecting to a malicious sever
- Exploiting user privileges
- Ads in hidden IFRAMES and popups
- Data manipulation
- Session hijacking
- Brute-force password cracking
- Data theft
- Intranet probing
- Key logging and remote monitoring

**Insecure deserialization**
**Using components with known vulnerabilities**
**Insufficient logging and monitoring**
**Directory traversal**
**Unvalidated redirects and forwards**
**Watering hole attack**
**Cross site request forgery**
**Cookie/session poisoning**
**Web server attacks**
**Cookie snooping**
**Hidden field manipulation**
**Authentication hijacking**
**Obfuscation application**
**Broken session management**
**Broken account management**
**Denial-of-service**
**Buffer-overflow**
**Captcha attacks**
**Platform exploits**
**Network access attacks**
**DMZ protocol attacks**
**Web based timing attacks**
**Marionet attack**
**Rc4 no more attack**
**Click jacking attack**
**Java script hijacking**
**DNS rebinding attack**

## Web application hacking methodology

- Footprint web infrastructure
- Analyse web applications
- Bypass client-side controls
- Attack authentication mechanisms
- Attack authorization schemes
- Attack access controls
- Attack application logic flaws
- Attack shared environments
- Attack database connectivity
- Attack web application clients
- Attack web services

## Web API, Web hooks, and Web shell

## Web service API's

- Soap API
- Rest (representation state transfer) API
- Restful API
- Xml-rpc Json-rpc

## Owasp top 10 API security risks

- Broken object authorization
- Broken user aUthentication
- Excessive data exposure
- Lack of resources and rate limiting
- Broken function level authorization
- Mass assignment
- Security misconfiguration
- Injection
- Improper assets management
- Insufficient logging and monitoring

**API vulnerabilities**
**Enumerated resources**
**Sharing resources via unsigned URLs**
**Vulnerabilities in third-party libraries**
**Improper use of cors**
**Code injections**
**RBAC privilege excalation**
**No ABAC validation**
**Bussiness Logic Flaws**
**Web API methodology**
**Detect security standards**

## Identify attack surface

- API metadata vulnerabilities
- API discovery
- Brute force Fuzzing
- Invalidate input attacks
- Malicious input attacks
- Injection attacks
- Insecure ssl configuration
- Insecure direct object reference
- Insecure session/authentication handling
- Login/credential stuffing attacks
- API ddos attacks
- Authorization attacks on API
- Reverse engineering
- User spoofing
- Man-in-the-middle attacks
- Session replay attack
- Social engineering

# Cyber Security

## Web application security

- Manual web application security testing
- Automated web application security testing
- Static application security testing
- Dynamic application security testing
- Web application fuzz testing
- Source code review

## SQL INJECTION

**Sql injection concepts**

- What is sql injection?
- Why bother about sql injection
- Sql injection and server-side technologies
- Understanding http post request
- Understanding normal sql query
- Understanding an sql injection query-code analysis

## Types of sql injection

**Sql injection concepts**

- What is sql injection?
- Why bother about sql injection
- Sql injection and server-side technologies
- Understanding http post request
- Understanding normal sql query
- Understanding an sql injection query-code analysis

## In-band sql injection

- Error-based sql injection
- System stored procedure
- Illegal/logical incorrect query
- Union sql injection
- Tautology
- End-of-line comment
- In-line comments
- Piggybacked query

## Blind/inferential sql injection

- No error message returned
- Waitfordelay
- Boolean exploitation and heavy query
- Out-of-band SQL injection

## Sql injection methodology

- Information gathering and Sql vulnerability detection
- Launch sql injection attacks
- Advanced SQL injection

**Countermeasures**

## HACKING WIRELESS NETWORKS

## Wireless concepts

## Wireless terminology

- Global system for mobile communications (GSM)
- Bandwidth
- Access point (AP)
- Basic service set identifier (BSSID)
- Industrial scientific and medical (ISM) band
- Hotspot
- Association
- Service set identifier (SSID)
- Orthogonal frequency-division multiplexing (OFDM)
- Multiple input, multiple output-orthogonal frequency- division multiplexing (MIMO-OFDM)
- Direct-sequence spread spectrum (DSSS)
- Frequency-hopping spread spectrum (FHSS)

## Wireless networks and types of wireless networks

- Extension to a wired network
- Multiple access points
- Lan-to-lan wireless network
- 3g/4g hotspot

## Wireless standards

- 802.11
- 802.11a
- 802.11b
- 802.11d
- IEEE 802.11e
- 802.11g
- 802.11i
- 802.11n
- 802.11ah
- 802.11ac
- 802.11ad
- 802.12
- 802.15 (bluetooth)
- 502.15.4 (zigbee)
- 802.15.5
- 802.16

## Service set identifier (SSID) wi-fi authentication modes

- Open system authentication process
- Shared key authentication process

## Wi-fi authentication process using a credentialized authentication server Types of wireless antennas

- Directional antenna
- Omni directional antenna
- Parabolic grid antenna
- Dipole antenna
- Reflector antennas

## Wireless encryption Types of wireless encryptions

- 802.11i
- eap
- wpa
- wpa2
- aes
- ccmp
- wpa2 enterprise
- radius
- peap
- wpa3
- wep
- leap
- tkim

## Wireless threats

- Access control threats
- Wardriving
- Rogue access points
- Mac spoofing
- AP misconfiguration
- Ad hoc association
- promiscuous client
- Client mis-association
- Unauthorized association

## Integrity attacks

- Data-frame injection
- Wep injection
- Bit-flipping attacks
- Extensible ap relay
- Data replay
- Initialization vector replay attacks
- Radius replay
- Wireless network viruses

## Availability attacks

- Access point theft
- Disassociation attacks
- Eap-failure
- Beacon flood
- Denial-of-service
- De-authenticate flood
- Routing attacks
- Authenticate flood
- Address resolution protocol (ARP)
- cache poisoning attacks
- Power saving attacks
- Tkip mic exploit

## Authentication attacks

- Psk cracking
- Leap cracking
- vpn login cracking
- Domain login cacking
- Key reinstallation attack
- Identity theft
- Shared key guessing
- Password speculation
- Application login theft
- Rogue ap attack
- Client mis-association
- Misconfigured ap attack
- Unauthorized association
- Ad-hoc connection attack
- Honeypot ap attack
- AP mac spoofing
- Denial-of-service attack
- Key reinstallation attack (KRACK)
- Jamming signal attack
- aLTEr attack
- Wormhole and sinkhole attacks

**Wi-Fi jamming devices**

**Wireless hacking methodology**

## Wi-fi discovery

- Active footprinting method
- Passive footprinting method

## Gps mapping

- Wireless traffic analysis
- Launch of wireless attacks
- Wi-fi encryption cracking
- Wi-fi network compromising

**Countermeasures**

# Hacking Mobile Platforms

**Mobile platform attack vectors**

- Owasp top 10 mobile risks
- Improper platform usage
- Insecure data storage
- Insecure communication
- Insecure authentication
- Insufficient cryptography
- Insecure authorization
- Client code quality
- Code tampering
- Reverse engineering
- Extraneous functionality

## Hacking android os

- Android os architecture
- Android device administrator
- API Android rooting

## Jail breaking ios
## Types of jail breaking

- User land exploit
- Iboot exploit
- Bootrom exploit

## Jail breaking techniques

- Untethered jail breaking
- Semi-tethered jail breaking
- Tethered jail breaking
- Semi-untethered jail breaking

**Mobile device management**

**Mobile security guidelines and tools**

# Iot And Ot Hacking

## Iot concepts

- Iot architecture
- Iot technologies and protocols
- Iot communication models
- Challenges of iot
- Iot threats
- Iot vulnerabilities

## Iot attacks

- DDos attack
- Exploit HVAC
- Rolling code attack
- Blue borne attack
- Jamming attack
- SDR-Based attack
- Fault injection attack
- Sybil attack
- Exploit kit
- Man-in-middle attack
- Replay attack
- Forged malicious attack
- Side-channel attack
- Ransomware attack

## Iot hacking methodology

- Information gathering
- Vulnerability scanning
- Launch attacks
- Gain remote access
- Maintain access

**Countermeasures**

# Cloud Computing

## Cloud computing concepts
## Module Objectives

- Understanding cloud computing concepts
- Overview of container technology and services computing
- Understanding cloud computing threats
- Understanding cloud hacking
- Understanding cloud computing security
- Overview of various cloud computing security tools

## Module Flow

- Cloud computing
- Container technology
- Server less computing
- Cloud computing threats
- Cloud hacking
- Cloud security

## Cloud Computing Concepts Introduction to cloud computing (Characteristics of cloud computing)

- On demand self service
- Distributed storage
- Rapid elasticity
- Automated Management
- Resource pooling
- Virtualization Technology

## Types of Cloud Computing Service

- Infrastructure-as-a-service (IaaS)
- Platform-as-a-service (PaaS)
- Software-as-a-service (SaaS)
- Identity-as-a-service (IDaaS)
- Security-as-a-service (SECaaS)
- container-as-a-service (CaaS)
- Function-as-a-service (FaaS)

## Separation of responsibilities in cloud

## Cloud Deployment Models

- Public cloud
- Private cloud
- Community Cloud
- Hybrid Cloud
- multi Cloud

**NIST Cloud Deployment Reference Architecture**
**Role of AI in Cloud Computing**
**Virtual Reality and Reality on Cloud**

## Cloud Service Providers

- Amazon Wed Services(AWS)
- Microsoft Azure
- Google Cloud Platform
- IBM cloud
- Container Technology

**What is Container?**
**Container VS Virtual Machine**

## What is Docker?

- Docker Engine
- Docker Architecture
- Docker Objects
- Docker Operations

**Micro services vs Docker**
**Docker Networking**
**Container Orchestration**
**What is Kuberenets?**
**Kuberbnets Vs Docker**

## Container Security Challenges

- Inflow of vulnerable source code
- Large attack surface
- Lack of visibility
- Compromising Secrets
- DevOps speed
- Noisy Neighbouring Containers
- Container breakout to the host
- Network-based attacks
- Bypassing isolation
- Ecosystem complexity

## Container Management Platforms

- Docker
- Amazon Elastic container service
- redhat open shift container platform
- Portainer Rancher

## Kuberenets Platforms

- Kuberenets
- Docker Kuberenets Service
- Knative

## Server less Computing

- What is serverless computing?
- Serverless Vs Containers
- Serverless computing frame works
- Microsoft Azure Functions

## Cloud computing threats

- OWASP top 10 Cloud security risks
- OWASP top 10 serverless security risk
- Cloud computing threat
- Container Vulnerabilities
- Kubernetes Vulnerabilities
- Cloud Attacks: Service hijacking using Social Engineering
- Cloud Attacks: Service hijacking using Network sniffing
- Cloud Attacks: Side-channel Attacks or Cross-guest VM breaches
- Cloud Attacks: Wrapping Attack
- Cloud Attacks: Man in the cloud (MITC) Attack
- Cloud Attack: Cloud Hooper Attack
- Cloud Attacks: Cloud Crypto jacking
- Cloud Attack: Cloud borne Attack

# Cyber Security

**Cloud hacking**
**What is Cloud Hacking?**
**Container Vulnerability Scanning Using Trivy**
**Kuberenets Vulnerability Scanning Using Sysd**
**Enumerating s3 Buckets**
**Identifying open S3 Buckets S3Scanner**
**Enumerating Kuberenets etcd**
**Enumerating AWS Account IDs**
**Enumerating IAM Roles**
**Enumerating Bucket Permissions using S3Inspector**
**Backdooring Docker Images Using Dock screen**
**AWS hacking Tool: AWS pwn**

## Cloud security

## Cloud Security Control Layers

- Application Layer
- Information layer
- management layer
- Network Layer
- Trusted Computing
- Computation and Storage
- Physical layer

**Placement of security controls in the cloud**
**NIST recommendations for cloud security**
**Kuberents Vulnerabilities and solutions**
**Serverless security risks and solutions**
**Best practices for Docker security**
**Best practices for kuberenets security**
**Best practices for serverless security**
**Zero trust Networks**
**International Cloud Security Organizations**
**Cloud security alliance**

## Cryptography

**Cryptography concepts**
**Objectives of cryptography**
**Types of cryptography**

- Symmetric encryption
- asymmetric encryption

**Government access to keys**
**Encryption algorithms**
**Ciphers**

## Types of ciphers

- Classical ciphers
- Modern ciphers Data encryption standard (DES)
- Triple Data encryption standard (3DES)
- Advanced encryption standard (AES)
- RC4, RC5, Rc6
- Blowfish
- Two fish and three fish Serpent
- Tea
- Cast-128
- Ghost Block cipher
- Camellia
- DSA and related signature schemes
- Rivest shamir adleman (RSA)
- Diffie-Hellman
- YAK
- Message digest (one-way hash) functions
- Message digest secure hashing algorithms RIPEMD-160
- HMAC
- CHAP
- EAP
- GOST-Hash function

## Public key infrastructure (PKI)

## Email encryption

- Digital signature
- Secure socket layer (ssl)
- Transport layer security (TLS)
- PGP (pretty good privacy)
- GNU privacy guard (GPG)
- Web of trust (WOT)

## Disk encryption Cryptanalysis

## Cryptanalysis methods

- Linear cryptanalysis
- Differential cryptanalysis
- Integral cryptanalysis

## Cryptography attacks

- Cipher text-only attack
- Adaptive chosen-plaintext attack
- Chosen-plaintext attack
- Related-key attack
- Dictionary attack
- Known-plaintext attack
- Chosen-cipher text attack
- Rubber hose attack
- Chosen-key attack
- Timing attack
- Man-in-the-middle attack

- Brute-force attack
- Birthday attack
- Side-channel attack
- Hash collision attack
- Duhk attack
- Rainbow table attack
- Padding oracle attack
- Drown attack

**Countermeasures**

## Lab Environment (LAB SETUP)

**Virtualization Lab**

- Virtual box

**Linux sytems**

- Kali linux
- Parrot
- ubuntu

**Windows systems**

- Windows 7
- Windows xp
- Windows 8
- Windows 10
- Windows 11

**Windows servers**

- Windows 2000
- Windows 2003
- Windows 2008
- Windows 2012
- Windows 2016
- Windows 2019

**Linux servers**

- Ubuntu server
- Debian server
- Fedora server
- Red hat enterprise linux

**Android os**

- Andoid4-9 versions

**Mac os**

**Multiple Vuln machines**

- DVWA
- BWAPP
- CTF Learn
- Defend the web
- Google gruyere
- Hack.me
- Hack the box
- Hack this site
- Overthewire
- Hellbound hackers
- Thisislegal
- Game of Hacks
- Metasploitable
- FTP vulnerable server
- Vulnerable wordpress exploits
- Vulnerable drupal services and exploits
- Zero day exploits

## PRIMARY TOOLS

### Foot printing tools

- Web spidering tools: Web extractor
- Website Mirroring Tools: HTTrack Web Site Copier
- Metadata Extraction Tools: Extract Metadata
- Web Updates Monitoring Tools: Follow That Page
- Email Tracking Tools: Email tracker pro
- tracking online reputation of target: Trackur
- Monitoring Website Traffic of Target Company: Clicky
- Competitive Intelligence Gathering: Similar Web
- Whois Lookup Tools: smartwhois
- IP Geolocation Lookup Tools: Ip2location
- Foot printing tools: maltego

## Scanning Tools

- Nmap
- Hping2/hping3
- Scanning tools for mobile: fing, net scanner
- Ping sweep tools: angry ip scanner
- creating customized packet: cola packet soft builder
- Proxy tools: proxy switcher
- Proxy tools for mobiles: proxy droid
- Network discovery and mapping tools: network topology mapper
- Network discovery tools for mobile: network analyzer

## Enumeration tools

- NetBIOS enumeration tools: NetBIOS enumerator
- Nmap
- Global network inventory
- Nsauditor network security auditor
- Snmp enumeration tools: snmpcheck
- LDAP enumeration tools: softerra LDAP administrator
- Ntp enumeration tools: prtg network monitor
- Nfs enumeration tools: RPCScan
- SMTP enumeration tools: smtp-user-enum

## Vulnerability Assessment Tools

- Vulnerability analysis: exploit database
- Vulnerability assessment tools: Acunetix web vulnerability scanner
- Vulnerability assessment tool: Nessus
- Vulnerability assessment tool: Burp suite

**System Hacking Tools:**

**Default passwords online tools**
- http://open-sez.me
- https://www.fortypoundhead.com
- https://cirt.net
- http://www.defaultpassword.us
- http://defaultpassword.in
- https://www.routerpasswords.com
- https://default-password.info

**Password recovery tools**
- password recovery toolkit
- Keepass password manager
- Kaspersky password checker

**Tools to extract password hashes**
- pwdump7

**Password cracking tools**
- L0phtcrack
- Ophcrack
- Rainbow crack
- John the ripper
- Hash cat
- The hydra
- Cain & Abel
- Ncrack

**Buffer overflow detection tools**
- Ollydbg
- Splint
- BOVSTT

**Privilege escalation tools**
- Beroot
- Linpostexp

**Tools for executing applications**
- Pupy

**Keyloggers**
- Spyrix keylogger

**Spyware tools**
- Spytech
- Power spy

**Desktop and child monitoring spyware**
- Activtrak

**Audio spyware**
- Spy voice recorder

**Video spyware**
- Free2x webcam recorder

**Cell phone spyware**
- Phone spy

**Gps spyware**
- Mspy

**Anti keylogger tools**
- Zemana anti-keylogger

**Anti-spyware tools**
- Super anti spyware

**Anti-rootkits**
- Malware bytes

## Steganography tools
- Image steganography: quick stego
- Document steganography: snow
- Video steganography: open puff
- Audio steganography: deep sound
- Folder steganography: folder lock
- Spam/email steganography tool: spam mimic
- Steganography tools for mobile: steganography master
- Steganography detection tools: zsteg
- S-tools steganography tool

**Track-covering tools**
- Ccleaner

**Phishing tools**
- Zphisher

**Android rooting tools**
- Kingoroot

**Android based sniffers**
- Packetcapture

**Android Hacking tools**
- Nexspy

**Android security tools**
- SEP mobile security

**Android vulnerability scanner**
- Vulners scanner

**Jail breaking tools**
- Apricot

**Ios hacking tools**
- Spyzie

**Ios Device Security tools**
- Avira mobile security
- Norton security for ios
- Lastpass password manager
- Lookout personal for ios
- Mcafee mobile security
- Trend micro mobile security

**IOS device tracking tools**
- Find my iPhone

**Mobile anti-spyware**
- Malwarebytes
- Antispy mobile
- Spyware detector
- Iamnotified
- Privacy scanner
- Centro iPhone

**Sniffing tools**
- Wireshark

**IOT vulnerability scanning tools**
- Bestorm
- Metasploit pro
- Iotsploit
- Iotseeker
- Bitdefender home scanner
- Iot inspector
- Tools to perform SDR-Based attacks
- Universal radio hacker
- BladeRF
- Rfcat
- HackRF
- Funcube Dongle
- Gqrx
- Iot hacking tools
- censys
- shodan

CELEBRATING 12 YEARS

Quality Thought®

# Cyber Security

## Information gathering tools for IOT
- Kamera-GUI
- Redpoint
- S7scan

## OT Hacking Tools
- ICS exploitation framework

## Cryptography tools
- Md5 calculator
- hash my files
- Md6 calculator
- All hash generator
- Md6 generator
- Md5 hash calculator
- Hashcalc

## Hash calculators for mobiles in playstore
- hash tools
- hash droid
- Md5 checker
- Hash checker
- Hashr-checksum & hash digest calculator
- Hash calculator
- hash calc

## Crypt tools
- BCTextEncoder
- AxCrypt
- Microsoft cryptography tools
- Concealer
- Sensiguard
- Challenger
- Cryptography tools for mobile in playstore
- Secret space encryptor
- secure everything
- Crypto
- encrypt file free
- Ego Secure Encryption Anywhere
- Cipher Sender
- Decrypto

## Cryptography toolkits
- Openssl
- keyczar
- Wolfssl
- AES crypto toolkit
- RELIC
- Pycrypto

## Email encryption tools
- Rmail
- Virtru
- Zixmail
- Egress secure email amd file transfer
- Proof point email protection
- Paubox

## Disk encryption tools
- Veracrypt
- Symantec frive encryption
- bit locker drive encryption
- Final crypt
- Seqrite encryption manager
- file vault
- Gillsoft full disk encryption
- Rohos disk encryption

## Cryptanalysis tools
- Cryp tool
- crypto sense
- RsaCtfTool
- Msieve
- Cryptol
- Crypto Bench

## Online md5 decryption tools
- Md5 decoder
- Crackstation
- Md5 encrypt & decrypt
- md5hashing
- Md5 decrypt
- Md5 decryption
- Md5 decrypter
- Onlinehashcrack
- hashkiller.co.uk
- Md5.my-Addr
- cmd5.org
- decode md5 hash
- Md5 decoder tool

CELEBRATING 12 YEARS

Quality Thought®

# Cyber Security


Quality Thought®

9032209710
95158 56058

**Quality Thought Infosystems India (P) Ltd.**

Flat No: 209, 2nd floor , Nilgiri Block, Ameerpet, Hyderabad - 500016 | www.qualitythought.in | info@qualitythought.in