VIT®

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering
Digital Assignment, OCTOBER 2020
B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	G2
FACULTY	Prof. THANDEESWARAN R.

COMODO INTERNET SECURITY

The rapid acceptance and deployment of the internet has transformed how we build and share information today. Financial transactions, healthcare records, personal information, and government data all pass instantly through technology systems at record pace. Internet technologies have revolutionized the way people communicate, governments manage, businesses operate and society functions.

But with innovation always comes risk. Security is always the last layer to be added in any transformational idea, and malware and cyberattacks now threaten the economic and societal progress that these technology tools provide. They have created an environment of vulnerability and exposure, where individuals and corporations can't feel they trust the experience of being online, of collaborating across geographies, of exchanging information safely.

Enter Comodo, a company that has been built upon the very foundation of trust, believing that every single digital transaction must have a built-in layer of trust and security. Thousands of companies and organizations rely on Comodo's technology to authenticate, validate and secure their most precious asset – information - and to combat constant malware threats and cyberattacks that are creating havoc on a global scale.

From the individual to the corporation, everyone has the right to a trustworthy and secure environment and it is the job of Comodo to provide the technology solutions that secure and preserve that experience. For the employees of Comodo, this is their life's work – creating an environment of trust for their current and future customers.

Comodo's innovative software and services do this by:

Authenticating Individuals, Businesses Websites and Content:
Authentication is at the heart of trust – it's the process of confirming that something or someone is genuine. Hackers are counterfeiters and impersonators - they thrive on deception. Trust is created when individuals, businesses, websites or software publishers are authenticated to ensure that they are who they say they are, and that their information has not been tampered with. This trust is the core of successful online businesses and trusted online interactions.

- **Extended Validation SSL Certificates**
  Provide the highest level of business authentication available according to standards set forth by the CA/Browser Forum. The green HTTPS browser address bar assures visitors they are interacting with a verified business on a secured domain

- **Secure E-Mail**
  Provides assurance of who e-mail really came from and that it has not been read or altered during transmission.

- **Two-Factor Authentication**
  Provides stronger authentication of people attempting to log in to systems, such as electronic banking, webmail or collaboration applications.

- **Code-Signing Certificates**
  Provide assurance of a software publisher's identity and that a software program being installed has not been modified or altered since creation.

- **Verification Engine**
  Provides visual verification that a website is a legitimate, rather than an impersonated/phishing site, and that the site's SSL certificate includes business validation.

- **Content Verification Certificates**
  Provide authentication of company logos, login boxes, order forms, authorized to accept credit card indicators, rate and price information, and other critical website content.

Securing Information:
Encrypting sensitive information at all stages of its lifecycle is a proven method of keeping it safe from hackers. Strong Public Key Infrastructure (PKI) encryption through digital certificates ensures that the encrypted information can only be used by authorized parties.

- Digital Certificates Servers of all types exchanging information over the Internet use SSL/Digital Certificates to create a private, encrypted channel of communications with those accessing them, preventing unauthorized access of that information by hackers.

Securing Websites and E-Commerce:
Uncovering and alerting IT organizations to vulnerabilities in their server/site's technical configuration or security procedures that could be exploited by hackers, and providing advice or solutions to eliminate them.

- **Scanning and Compliance Services**
  A PCI Security Standards Council-approved scanning service that scans for vulnerabilities and provides reports, mitigation advice and the necessary documents to indicate quarterly PCI compliance. A Comodo Trustmark increases trust by informing visitors that the site is regularly scanned.

- **Digital Certificates**
  The industry's broadest array of digital certificates encrypt the information exchanged between a site and a site visitor, preventing unauthorized use of that information by hackers. Website visitors recognize a site using digital certificates when they see a yellow padlock or green browser address bar

Securing and Maintaining PCs:
Denying hackers access to the information and resources they need to succeed, such as your personal or business financial information, and at a more fundamental level, your computer's internet connection and processing capacity.

- **Desktop Software**
  A complete set of software applications to increase PC security, performance and peace of mind. Award-winning Comodo software offers the latest innovations, and most of it is available for free to individual users.

- **PC Support and Maintenance Services**
  A personal computer geek or small businesses virtual IT Department delivered 24x7 through the Internet. Comodo handles just about any computer support and maintenance issue through a secure, remote Internet connection instead of having someone come to a home or office.

Meeting tomorrow's challenges requires both leadership and innovation in their customer offerings as well as the way they run their businesses.

Providing Free Internet Security so Every PC can be Protected:
Paying an annual license fee for security software is an economic hardship for a large percentage of the world's computer owners, so Comodo provides full versions of ours for free, resulting in fewer unprotected computers that can be turned against us. More security software means fewer infected PCs to distribute scam e-mails, and malware or be part of a botnet executing a denial-of-service attack

Driving Down the Cost of Website Security (SSL) Certificates that Meaningfully Validate a Site's Identity:
Website security (SSL) certificates that validate key business details of a site are more difficult to obtain by cyber-criminals and are therefore more trustworthy than those that don't. Comodo technology and process innovation made us one of the first Certification Authorities to provide High Assurance SSL certificates well within the reach of even the smallest businesses today.

Bringing Key Industry Players Together to Meet Major Security and Trust Challenges for the benefit 1.2 billion Internet users:
Trusting the effectiveness and even the legitimacy of security software has become increasingly difficult. This is due to a lack of standards, and to cyber-criminals pretending to be security companies. So Comodo founded the Common Computing Security Standards Forum to mitigate malware risk and better protect consumers.

Trusting the gold padlock of a website security (SSL) certificates has become increasingly risky due to their increased use by cyber-criminals on fraudulent websites, so Comodo founded the CA/Browser Forum to establish identity validation standards and devise industry-wide approaches to re-establish trust such as the revolutionary Extended Validation SSL Certificate.

Today, the Comodo family of companies has
- more than 85 million desktop security software installations,
- more than 700,000 business customers and 8,000 global partners and affiliates
- market share leadership, being the #1 SSL Certificate Authority in the world, with more than 36% of the market, according to w3techs.com (as of July 1, 2015)

Comodo Timeline:

2001: Comodo CA launches its first certificate product.
2002: INSTANTSSL Launched.
2003: Comodo CA earns WEBTRUST Seal of assurance.
2004: USERTRUST acquisition.
2005: Personal Firewall launched.
2006: Hackerguardian launched.
2007: Extended validation SSL Certificates launched.
2008: Comodo Revolutionizes the Internet Security Suite.
2009: Comodo initiates founding of the common computing security standards forum.
2010: Comodo SSL Certificates available through parallels partner storefront.
2011: Info security products guide names Comodo CEO Entrepreneur of the year.
2012: Comodo launches a range of mobile apps including Mobile Security Suite, Anti-Theft, Backup and Battery Doctor.
2013: Matousec ranks Comodo Internet Security 6 #1 for the entire year.
2014: Comodo Mobile Device Manager Puts Focus on User.

Significant Innovations by the Comodo Companies

Default-Deny Protection:
Comodo changed the Internet security suite protection paradigm from "default allow," where all programs are allowed to run unless they are on a "blacklist' of known malware, to "default deny" where all programs are denied permission to run unless they are on a "whitelist" of known safe programs. Implemented through Comodo Internet Security's "Defense+" feature, default- deny protection introduces prevention as the first line of malware defence, greatly reducing the probability of malware infection.

Content Verification
Comodo attacked the problems of phishing and website impersonation through the introduction of Content Verification Certificates (CVCs). CVCs use X.509 certificates to digitally bind sensitive content on a website such as a company logo, login box, credit card or affiliation logos with domain location information. Like the holographic logo on officially licensed merchandise, users accessing the legitimate site experience a conspicuous "Authenticated by Comodo" indicator when accessing protected content. While cyber-criminals can copy text and graphics onto an impersonated website, the CVC is not transferrable, nor is the "Authenticated by Comodo" indicator present on that counterfeit site. The lack of verification alerts users to its potential illegitimacy.

Session Certificate
As a leading provider of secure email certificates, Comodo understands both the benefits and the challenges of PKI-secured/authenticated e-mail. Comodo's deep experience in this area led to our development of the patent-pending One-Time Session Certificate as a means of overcoming one of this technology's major challenges – the need to pre-exchange certificates prior to communicating. When a recipient's digital certificate is not present, Comodo Secure E-mail automatically generates a one-time session certificate that encrypts the message but also provides a means for the intended recipient to decrypt and view the message contents.

Local Area Network Remote Vulnerability Scanning

Comodo expanded the flexibility and cost-effectiveness of cloud-based vulnerability scanning to include both external and internal network vulnerability scanning. This hardware-free innovation permits scanning of any network asset from a single, cloud-based solution.
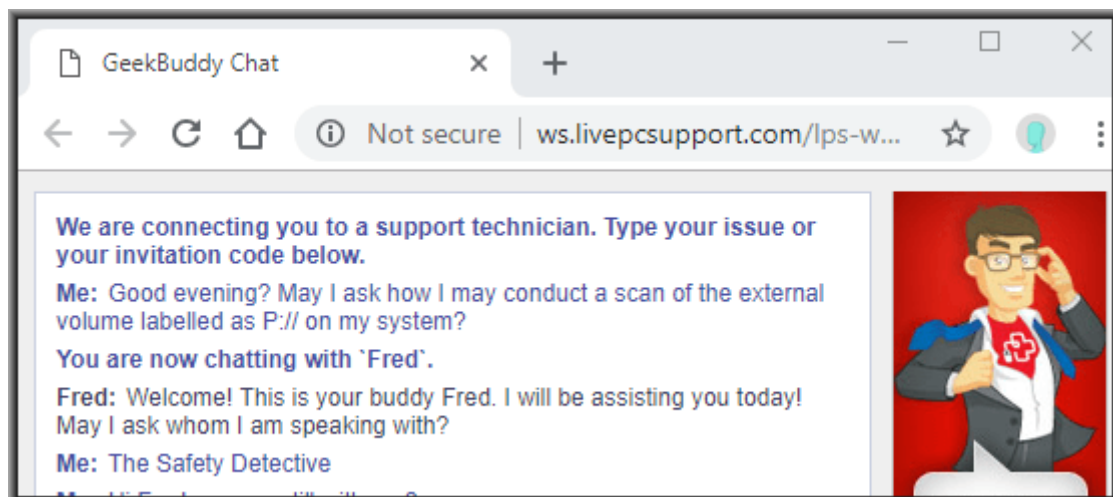
Extended Validation SSL

Comodo was among the first in the Internet community to recognize the erosion of trust in the SSL gold padlock. It identified the need for standardized, rigorous validation of entities requesting SSL credentials, and for a new, highly-conspicuous indicator of SSL security. Comodo initiated the founding the CA/Browser Forum to establish identity validation standards and create the Extended Validation SSL Certificate which displays a green browser address bar in addition to a padlock on SSL-secured web pages.
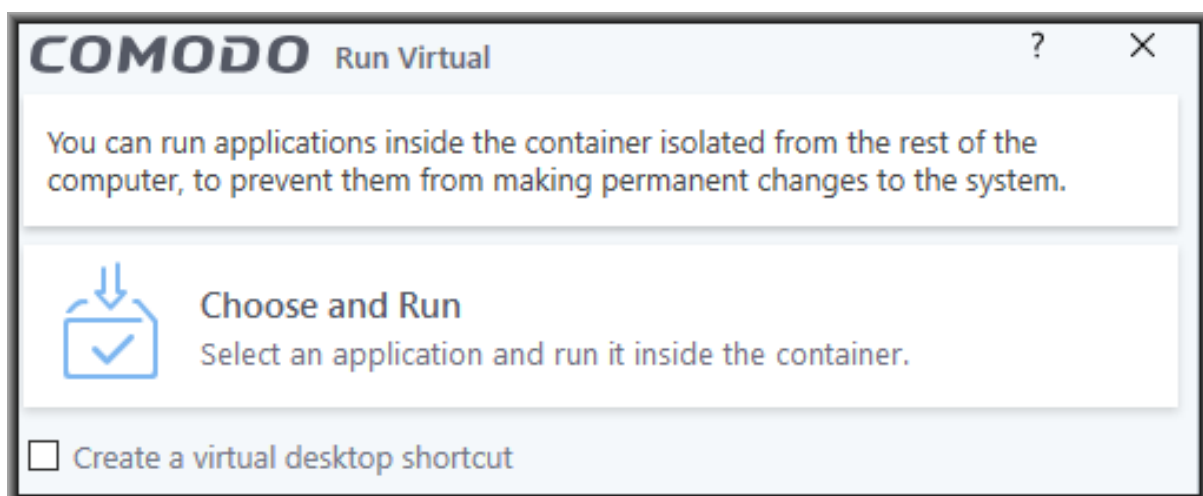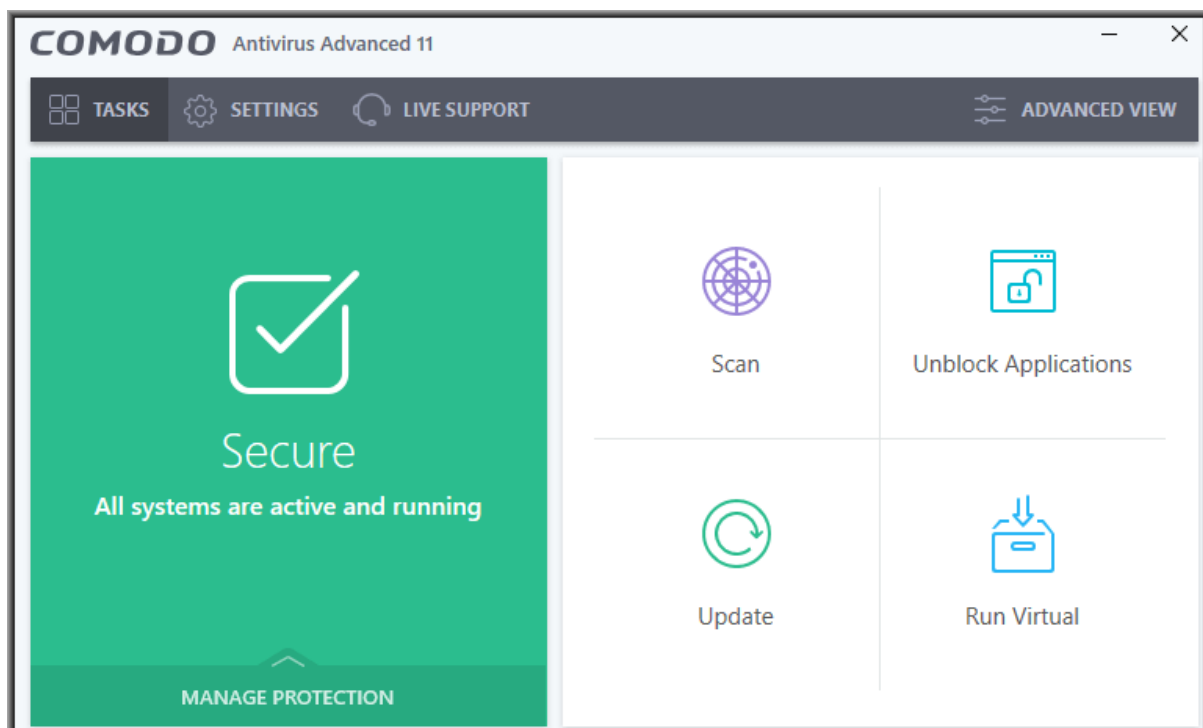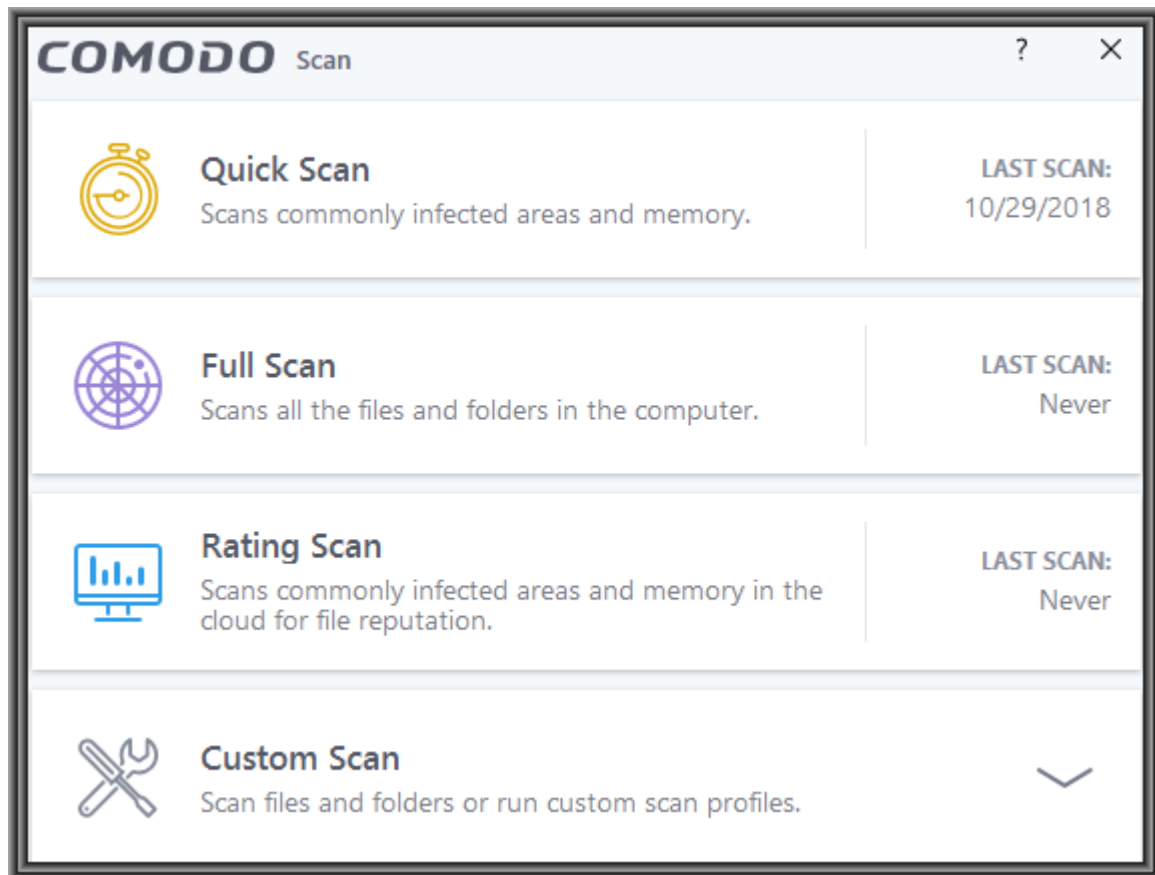
Comodo's **support** is centred around its online portal which includes both a ticket answering system as well as a live chat window. Comodo can be justifiably proud of its well-deserved reputation for responsiveness: Most tickets receive a response within an hour. Comodo's live chat assistance is always quick and courteous.

****