CSCI369 Ethical Hacking

Lecture 1-1: Introduction to Ethical Hacking

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

About This Subject

- Lecturer: A/Prof Joonsang Baek
- Lectures
  - Lecture slides will be uploaded on the Moodle site.
  - Recorded lectures will be available from Moodle.

About This Subject

- Lab
  - Run by your tutors
  - Kali Linux (on VirtualBox from Windows PCs or on UTM from Mac machines –Apple silicon-) will be your main platform
  - Lab quiz will be administered during the lab.
  - Lab instructions will be uploaded in the Moodle site.

About This Subject

- Textbooks and learning material
  - ➢No textbook but you may want to have a look at various material related to the topics.
  - ➢You can refer to any online resources but they need to be referenced when you do homework

About This Subject

- Assessment
  - ➢Lab assessment (Three quizzes)
    - ✓20%: Theory (lectures) + Practice (lab)
  - ➢Assignment
    - ✓30%: Problem Solving + Programming
  - ➢Final
    - ✓50%: Theory + Problem Solving

Setting Up Your Environment

Please set up your ethical hacking environment for either Windows PC or Mac (with Apple silicon) following the instruction posted on our Moodle site.

- Kali Linux VM
  - ➢We will be using Kali Linux 2024.2. (2024.1 will do too)
- Metasploitable 2 VM
  - ➢This is usually a target (victim) machine. Setting up VM is a little tricky, but make sure you do it.
- Ubuntu & Windows VM
  - ➢VMs are for Ubuntu 22.04 LTS and Windows 11

UNIVERSITY OF WOLLONGONG AUSTRALIA

Defining “Hacker”

- The term “hacker”
  - ➢How my English dictionary defines a *hacker*:
    - ✓A person who uses computers to gain **unauthorised** access to data
    - ✓An enthusiastic and skilful computer programmer or user
- Different kinds of hackers
  - ➢Ethical Hackers (=white hat Hackers): Hackers characterised by having a code of ethics to work for the benefits of the public.

Defining “Hacker”

- Grey Hat Hackers: Hackers straddling the line between good sides and bad sides. Perhaps they have been “rehabilitated”.
- Black Hat Hackers: Hackers operating on the wrong side of the law. They may have an agenda or no agenda at all.
- Cyberterrorists: A new form of hackers trying to destroy targets and cause bodily harm. Sometimes their actions are not stealthy.

Motivation for Studying Ethical Hacking

- Cybercrime
  - The use of a computer or online network to commit crimes such as fraud, online image abuse, identity theft or threats and intimidation - Definition by Australian Cyber Security Centre (ACSC)
- Targets
  - As cybercrime becomes more sophisticated, criminals are targeting individuals, businesses, education institutes and governments.

Major Threats

- Botnet
- Malware
- Spammming
- Ransomware
- Hactivism
- Mass surveillance

UNIVERSITY OF WOLLONGONG AUSTRALIA

Botnet: Concept

- Botnet operation
  - ➢A botnet is a network of compromised computers. The botnet herder (or botmaster) can control the botnet using command and control (C&C) software.

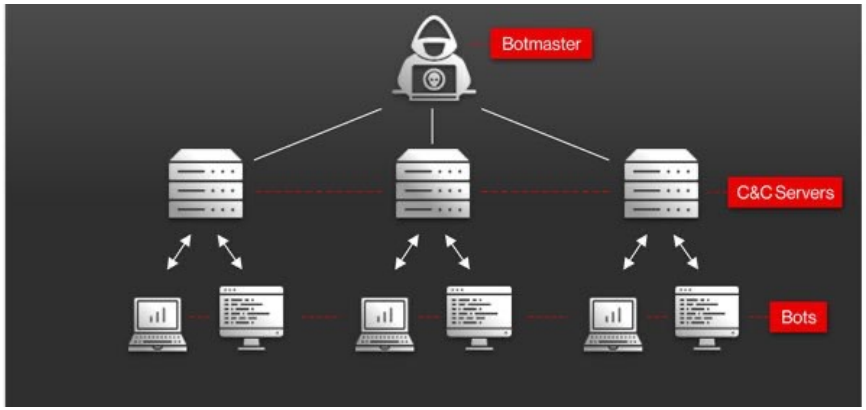

Image courtesy: Crowdstrike

Botnet: Some Well-Known Botnets

- Storm botnet
  - ➢ It infected machines mostly by malware in email attachments and had them use the eDonkey peer-to-peer network to find other infected machines.
  - ➢ It was used not just for spam but for Distributed Denial-of-Service (DDoS) and for harvesting credentials.
  - ➢ Defenders obtained lists of bot addresses so that the bots could be cleaned up. By late 2008, Storm had been cut to a tenth of the size.

Botnet: Some Well-Known Botnets

- Conficker botnet
  - A worm that spread by exploiting a Windows network service vulnerability
  - Generated 250 domain names every day, and infected machines are put in those domains which the botmaster had control
  - A later variant generated 50,000 domains a day and an industry working group made agreements with registrars that these domains cannot be used

Botnet: Some Well-Known Botnets

- Mirai botnet
  - A family of botnets that exploit *IoT devices*.
  - The first Mirai worm infected CCTV cameras that had been manufactured by Xiaomi and that had a known factory default password that could not be changed.
  - Mirai botnets scan the Internet's IPv4 address space for other vulnerable devices which typically get infected within minutes of being powered up.
  - The first major attack took down Twitter for six hours on the US eastern seaboard in October 2016.
  - There have been over a thousand variants, which researchers study to determine what's changed and to work out what countermeasures can be used.

Malware

- Malware: Hackers
  - ➢perform research on turning vulnerabilities into exploits.
  - ➢develop remote access Trojans that the deliver malware.
  - ➢build robust Domain Generation Algorithm (DGA) software for resilient command-and-control communications
    - ✓DGA: A program that generates numerous new domain names. Cybercriminals and botnet operators use DGA to frequently change the domains to make it hard for defenders to locate the botnet herder.
  - ➢design specialised payloads for various purposes

Malware

- Android malware
  - ➢Unpatched old Android phones (devices) in many countries are sources of malware infection.
- Difficulty in arresting malware operators
  - ➢It makes a difference for a while, but some are based in jurisdiction that do not extradite their nationals

Two Components of Malware

- Dropper
  - ➢A replication mechanism how malware can be transmitted
  - ➢Examples
    - ✓Worm: Malware that copies itself when it is run (Standalone!)
    - ✓Virus: Malware spread through other software as medium, such as macros in documents
    - ✓Trojan: Malware spread as a form of legitimate software, executed by the victim

Two Components of Malware

- Payload
  - ➢ An actual code that causes damages:
    - ✓ Exfiltrate the victim's data
    - ✓ Encrypt the victim's data
    - ✓ Steal important credentials (passwords, etc.)
    - ✓ Surveil the victim's machine
    - ✓ Steal CPU power (to, e.g., mine cryptocurrency)
    - ✓ Install some other malware

Spamming

- Early stage
  - Spamming arrived on a small scale
  - Earthlink spammer: Sending fishing lures in early 2000s
- *Unexpected outcome of spam*
  - Main beneficiaries of spam are large *webmail services* such as Yahoo, Gmail and Hotmail dues to their (better) spam filtering service.
- Cat-and-mouse game
  - Spam is now a highly specialised business, as getting past modern spam filters requires a whole toolbox of constantly-changing tricks.

Ransomware

- Features of ransomware
  - Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.
  - It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. (In a properly implemented ransomware, recovering the files without the decryption key is an intractable problem.)
  - Bitcoin and other cryptocurrencies are used as payment methods, making tracing and prosecuting the perpetrators difficult.

Ransomware

- Ransomware payment methods
  - By 2016–17, only 12% demanded cryptocurrency.
  - Currently, almost *98% of ransomware demand payment in cryptocurrency* (like Bitcoin).
- Dodge operation of ransomware
  - A lot of the low-end ransomware aimed at consumers is just scareware as it does not actually encrypt files at all.
  - *Ransomware-as-a- service* platforms; the operators who use these platforms are often amateurs and cannot decrypt even if the victim is willing to pay.

Ransomware

- Ransomware targeting public/healthcare sectors
  - ➢This has grown rapidly over 2019–20, with the most high-profile ransomware victims in the USA being *public-sector bodies*; several hundred local government bodies and a handful of *hospitals* have suffered service failures.
  - ➢During the pandemic, more hospitals have been targeted; the medical school at UCSF paid over $1m . It's an international phenomenon, though, and many private-sector firms fall victim too. Ransomware operators have also been threatening large-scale leaks of personal data to bully victims into paying.

Hactivism

- Hactivism = Activism on the Internet
  - ➢Purpose: Using online media to mobilise people to do conventional lobbying, such as writing to legislators;
  - ➢Early stage: Organisations such as Indymedia and Avaaz developed expertise at this during the 2000s.
- Utilising social media for hactivism
  - ➢Example: Wael Ghonim used social media to trigger the Arab Spring in 2011.
  - ➢Governments have started to crack down, and activism has spread into online hate campaigns and radicalisation.
  - ➢Players: Many hate campaigns are covertly funded by
    - ✓governments or opposition parties
    - ✓single-issue campaign groups

Hactivism

- Consequences
  - ➢Denial-of-service
    - ✓Attacks can interrupt operations: Companies or individuals cannot operate normally if they receive a lot of angry emails or tweets
  - ➢Brand damage
    - ✓*Doxing* can do real brand damage as well as causing distress to executives and staff
      - Doxing: search for and publish private or identifying information about a particular individual on the internet, typically with malicious intent.

Hactivism

- Online shaming
  - ➢A popular means of protest
  - ➢It can be quite spontaneous, with a flash mob of vigilantes forming when an incident goes viral.
    - ✓A notable example: In 2005 when a young lady in Seoul failed to clean up after her dog defecated in a subway carriage. Another passenger photographed the incident and put it online; within days the ‘dog poo girl’ had been hounded into hiding, abandoning her university course.

Hactivism

- Relations to politics
  - The harassment was coordinated on anonymous message boards and the attackers would gang up on a particular target – who then also got criticised by mainstream conservative journalists.
  - The movement appeared leaderless and evolved constantly, with one continuing theme being a rant against ‘social justice warriors’.
  - It appears to have contributed to the development of the alt-right movement which influenced the 2016 election two years later.

Hactivism

- A growing appreciation of the power of angry online mobs is leading politicians to provoke them, at all levels from local politicians trying to undermine their rivals to nation states trying to swing rival states' elections.
- Angry mobs are an unpleasant feature of modern politics

Hactivism

- Targeting companies
  - Companies are targeted less frequently, but it does happen.
  - The social-media companies are under pressure to censor online content, and as it is difficult for an AI program to tell the difference between a joke, abuse, a conspiracy theory and information warfare by a foreign government, they end up having to hire more and more moderators.

Mass Surveillance

- Governments have a range of tools for both passive surveillance of networks and active attacks on computer systems.
- Due to Edward Snowden's whistle-blowing, mass surveillance activities of *Five Eyes'* countries (US, UK, Australia, NZ and Canada).
- *Surveillance business*: Hundreds of firms sell equipment for wiretapping, for radio intercept, and for using various vulnerabilities to take over computers, phones and other digital devices.
- As user privacy becomes of prime importance, it is important for us to understand and be aware of mass surveillance technologies.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Mass Surveillance Technology: Tempora

- Purpose
  - A program to *collect intelligence from international fibre optic cables*.
- Operation
  - For example, in Cornwall, UK, 200 transatlantic fibres were tapped and 46 could be collected at any one time. As each of these carried 10Gb/s, the total data volume could be as high as 21Pb a day, so the incoming data feeds undergo massive volume reduction, discarding video, news and the like.
  - Material was then selected using selectors – not just phone numbers but more general search terms such as IP addresses – and stored for 30 days in case it turns out to be of interest.

Mass Surveillance Technology: Tempora

- UK involvement
  - Britain has physical access to about a quarter of the Internet's backbone, as modern cables tend to go where phone cables used to, and they were often laid between the same end stations as nineteenth-century telegraph cables. So one of the UK's major intelligence assets turns out to be the legacy of the communications infrastructure it built to control its nineteenth-century empire.

Mass Surveillance Technology: Muscular

- Purpose
  - ➢To collect data as it flowed between the *data centres* of large service firms such as Yahoo and Google.
- Operation
  - ➢Our mail may have been encrypted using SSL en route to the service's front end, but it then flowed in the clear between each company's data centres.
    - ✓Many Internet communications that appear to be encrypted are not really, as modern websites use *content delivery networks* (CDNs) such as Akamai and Cloudflare; while the web traffic is encrypted from the user's laptop or phone to the CDN's point of presence at their ISP, it isn't encrypted on the backhaul unless they pay extra (which most of them don't). So the customer thinks the link is encrypted, and it's protected from casual eavesdropping but not from nation states or from firms who can read backbone traffic.

Mass Surveillance Technology: XKeyScore

- Purpose
  - *NSA's search engine*
  - The Five Eyes search computer data using Xkeyscore, a distributed database that enables an analyst to search collected data remotely and assemble the results.
- Operation
  - NSA documents (exposed on July 31, 2013) describe it as its *widest-reaching* system for developing intelligence;
  - Enabling an analyst to search emails, SMSes, chats, address book entries and browsing histories.
- Examples from 2008 training slides
  - "My target speaks German but is in Pakistan. How can I find him?" "Show me all the encrypted Word documents from Iran" and "Show me all PGP usage in Iran".
    - ✓ By searching for anomalous behaviour, the analyst can find suspects and identify strong selectors (such as email addresses, phone numbers or IP addresses) for more conventional collection.

Mass Surveillance Technology: XKeyScore

- Extraction
  - Tasked items are extracted and sent on to whoever requested them, and there's a notification system (Traffic thief) for tipping off analysts when their targets do anything of interest.
- Target discovery
  - Xkeyscore can also be used for target discovery: one of the training queries is “Show me all the exploitable machines in country X” (machine fingerprints are compiled by a crawler called Mugshot).

Mass Surveillance Technology: XKeyScore

- Intriguing facts
  - According to an interview with Snowden in 2014, Xkeyscore also allows an analyst to build a fingerprint of any target's online activity so that they can be followed automatically round the world.
  - The successes of this system are claimed to include the capture of over 300 terrorists; in one case, Al-Qaida's Sheikh Atiyatallah blew his cover by googling himself, his various aliases, an associate and the name of his book.

Cybercrime Law

- Scope
  - ➢The part of cyberlaw relevant to our Ethical Hacking subject is "cybercrime law"
- Cybercrime laws
  - ➢US: 18 U.S.C. $1028 (read as "Title 18, United States Code Section 1028"), $1029, $1030, $1037,…
    - ✓For example, $1037 is "Fraud and related activity in connection with electronic mail"
  - ➢Australia: Cybercrime Act 2001
    - ✓For example, Cybercrime Act 2001 Part 10.7 Division 477 Subsection 477.1 specifies "Unauthorised access, modification or impairment with intent to commit a serious offence"

Categories of Cybercrime According to Law

- Identity theft
  - Stealing of the information that allow a person to impersonate other person(s) for illegal purposes, mainly financial gains such as opening credit card/bank account, obtaining rental properties and etc.
- Theft of service
  - Use of phone, Internet, streaming movies or similar items without permission; it usually involves password cracking
  - Example: Sharing a Netflix account with even friends can be considered as theft and can be prosecuted in certain states of US.

Categories of Cybercrime According to Law

- Network intrusion or unauthorised access
  - Most common type of attack; it leads to other cybercrimes
  - Example: Breaking into your neighbour's WiFi network will open a lot of opportunities of attack.
- Posting and/or transmitting illegal material
  - Distribution of pirated software/movies, child pornography
  - Getting hard to stop it due to file sharing services, encryption and etc.
- Fraud
  - Deceiving another party or parties to illicit information or access typically for financial gain or to cause damage

UNIVERSITY OF WOLLONGONG AUSTRALIA

Categories of Cybercrime According to Law

- Embezzlement
  - A form of financial fraud involving theft and/or redirection of funds
- Dumpster Diving
  - Gathering information from discarded/unattended material (ATM receipt, credit card statement and etc.)
  - Going through rubbish itself is not illegal but going through rubbish in private property is

Categories of Cybercrime According to Law

- Writing malicious codes
  - Malicious codes refer to items like viruses, worms, spyware, adware, rootkits, ransomware and other types of malware
  - This crimes is to cause havoc and/or disruption
- Unauthorised destruction or alteration of information
  - This covers modifying, destroying and tampering with information without appropriate permission
- DoS (Denial of Service) /DDoS (Distributed Denial of Service)
  - Overloading a system's resources so that it cannot provide the required services to legitimate users
  - DDoS is performed in a larger scale – It is not possible to prevent DoS by blocking one source

Categories of Cybercrime According to Law

- Cyberstalking/Cyberbullying
  - A relatively new crime on the list. The attacker uses online resources and other means to gather information about an individual and uses this to track, in some cases, to meet the person (cyberstalking); to harass the person (cyberbullying)
- Cyberterrorism
  - Attackers make use of the internet to cause significant bodily harm to achieve political gains
  - The scope of cyberterrorism is controversial
  - Related to information warfare