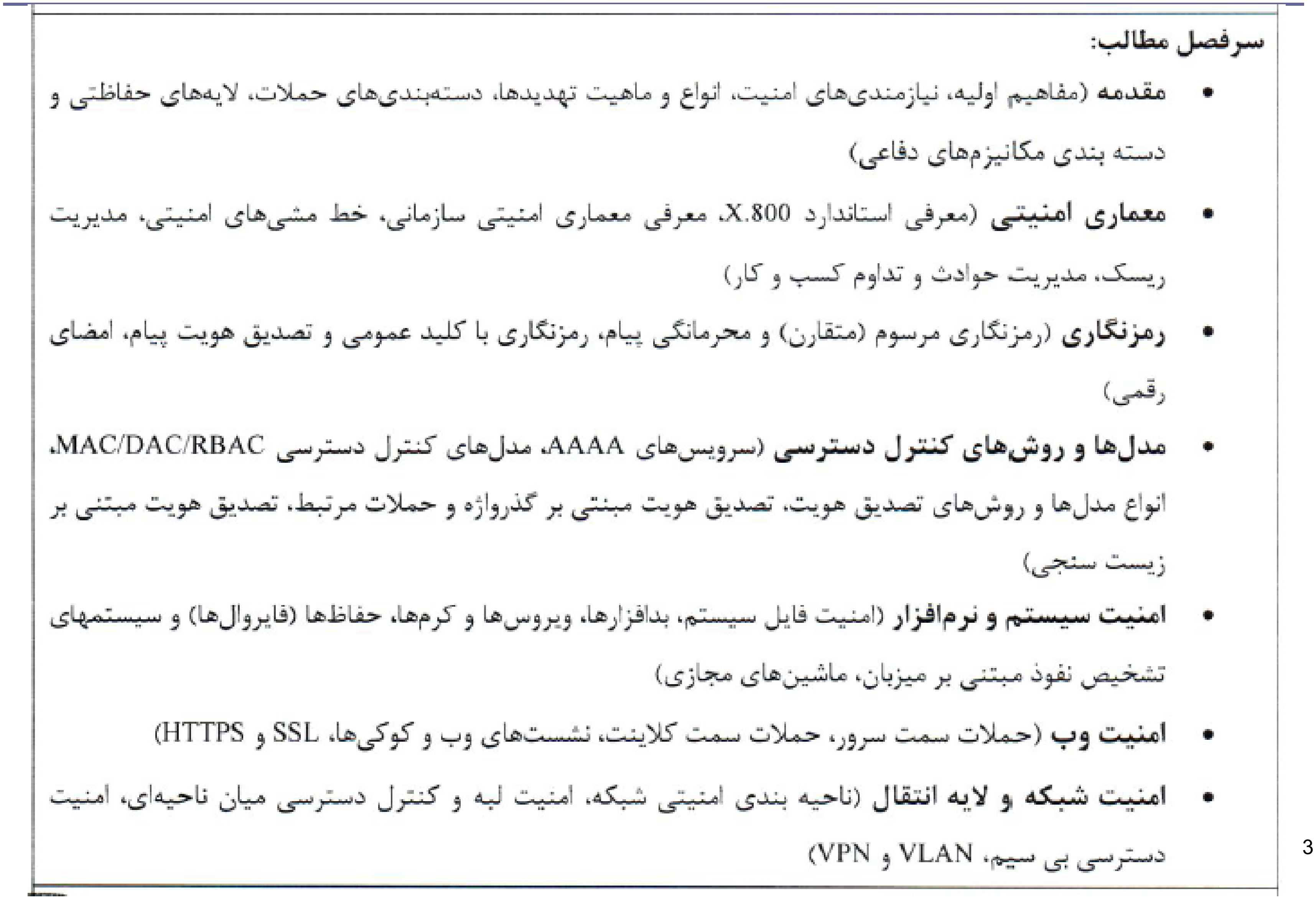
Information Security
Session 1

Hakim Sabzevari university
Dr.Malekzadeh

Grading

- Grading:
  - Midterm exam: 35% 15/9/1400
  - Final exam: 35%
  - Project: 30% (Due: max six days after final exam)
- Textbook: Kali
- Website:
  - piazza.com/hakimcomputer/spring2017/sec93
- Email: hakimcomputer93@gmail.com

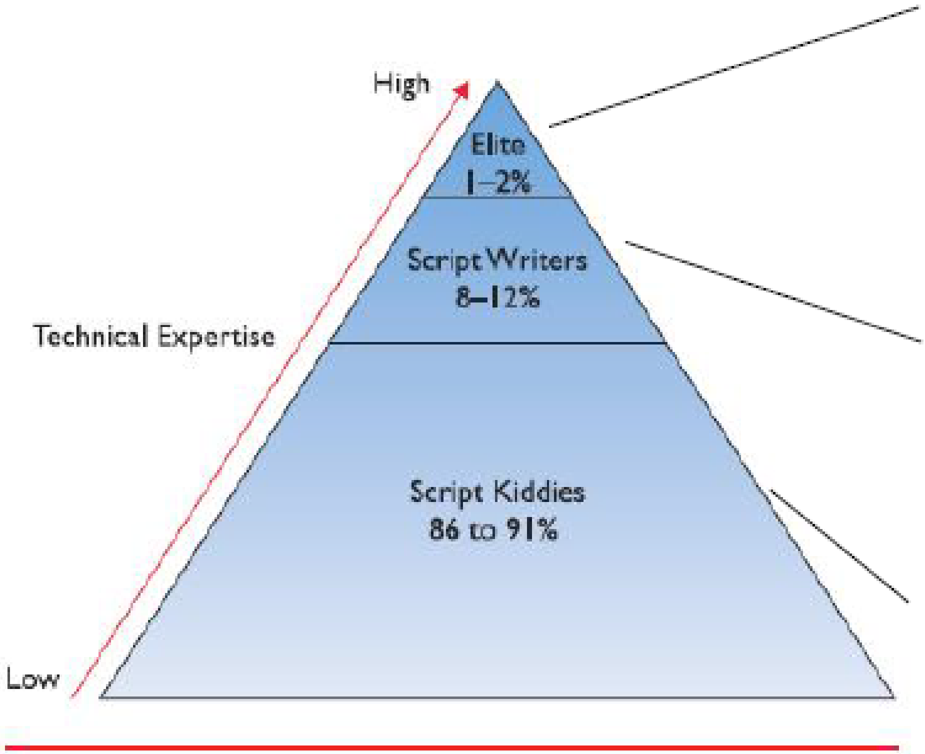


سرفصل مطالب:

- **مقدمه** (مفاهیم اولیه، نیازمندی‌های امنیت، انواع و ماهیت تهدیدها، دسته‌بندی‌های حملات، لایه‌های حفاظتی و دسته بندی مکانیزم‌های دفاعی)
- **معماری امنیتی** (معرفی استاندارد X.800، معرفی معماری امنیتی سازمانی، خط مشی‌های امنیتی، مدیریت ریسک، مدیریت حوادث و تداوم کسب و کار)
- **رمزنگاری** (رمزنگاری مرسوم (متقارن) و محرمانگی پیام، رمزنگاری با کلید عمومی و تصدیق هویت پیام، امضای رقمی)
- **مدل‌ها و روش‌های کنترل دسترسی** (سرویس‌های AAAA، مدل‌های کنترل دسترسی MAC/DAC/RBAC، انواع مدل‌ها و روش‌های تصدیق هویت، تصدیق هویت مبتنی بر گذرواژه و حملات مرتبط، تصدیق هویت مبتنی بر زیست سنجی)
- **امنیت سیستم و نرم‌افزار** (امنیت فایل سیستم، بدافزارها، ویروس‌ها و کرم‌ها، حفاظها (فایروال‌ها) و سیستمهای تشخیص نفوذ مبتنی بر میزبان، ماشین‌های مجازی)
- **امنیت وب** (حملات سمت سرور، حملات سمت کلاینت، نشست‌های وب و کوکی‌ها، SSL و HTTPS)
- **امنیت شبکه و لایه انتقال** (ناحیه بندی امنیتی شبکه، امنیت لبه و کنترل دسترسی میان ناحیه‌ای، امنیت دسترسی بی سیم، VLAN و VPN)

Hackers

- Hacker is a person that conducts a deliberate computer attack.



• Figure 1.1 Distribution of attacker skill levels

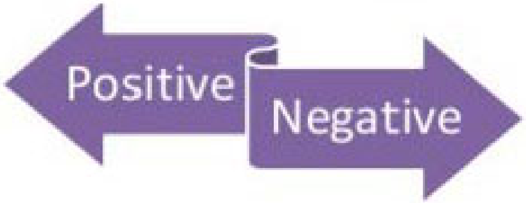
Elite Hackers: Individuals capable of discovering new vulnerabilities and writing scripts that exploit those vulnerabilities.

Script Writers: Individuals capable of writing scripts to exploit known vulnerabilities.

Script Kiddies: Individuals with (only) enough understanding of computer systems to be able to download and run scripts that others have developed. Vast majority of attack activity on the Internet is carried out by these individuals.

Hackers cont…

Hacking



Ethical Hacking: Penetration testing focusing on **securing and protecting** IT systems.

'good guys' hired to discover security vulnerabilities in a system

illegally access a system, but generally do not exploit the discovered vulnerability

'bad guys' (criminals) use their skills to conduct malicious activities

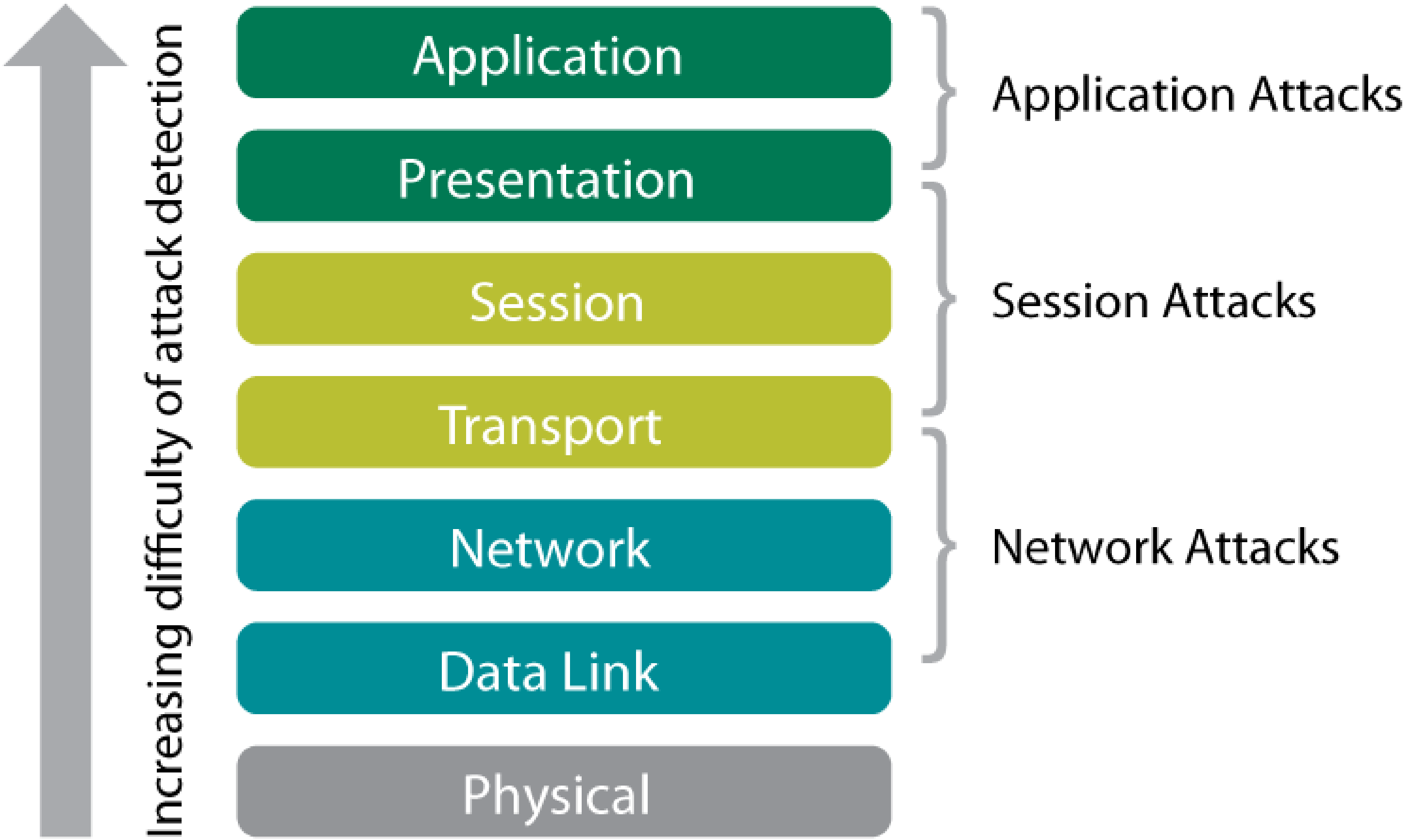
Security threats

Security threats levels

- Security must be performed at four levels to be effective:
  - Human
  - Physical
  - Operating System
  - Networking

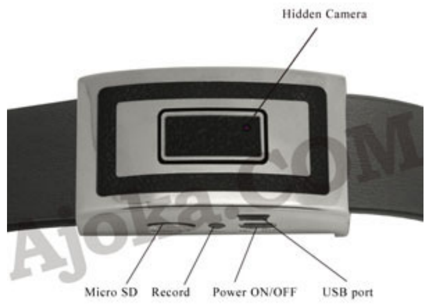
- Security is as weak as the weakest link in the chain.

Security threats levels cont…



Why we need to know cyber attack techniques?

- To protect yourself from cyber-criminals' malicious intentions, you have to first know what techniques they use to breach your internet security and get to your privacy.

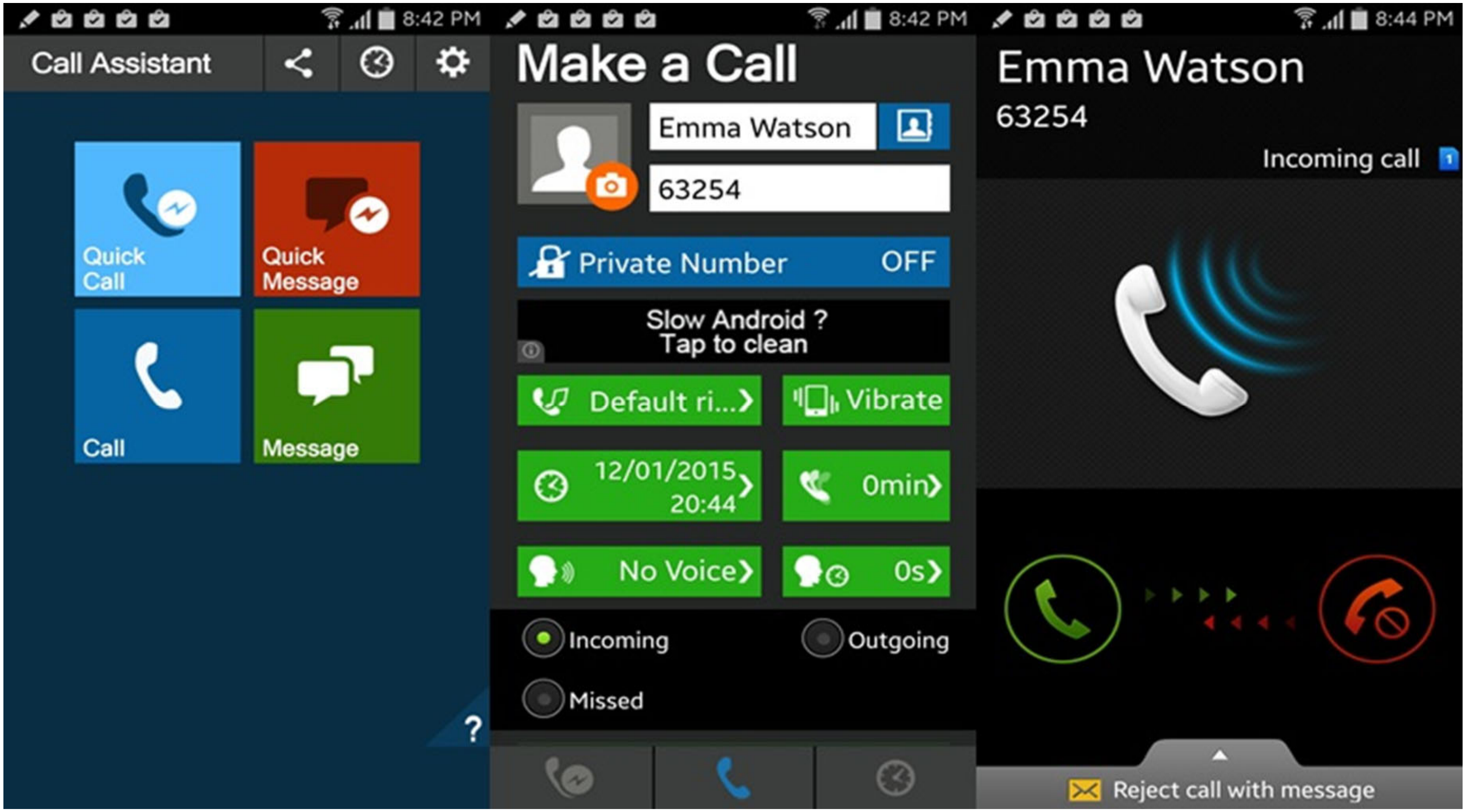


Spoofing

- In the context of information security, a spoofing attack is when a person or program masquerades/forges (جعل) as another by falsifying data, to gain an illegitimate advantage.

- Types of spoofing:
  - IP address Spoofing: creation of packets with a forged source/destination IP address, e.g. for the purpose of passing through a firewall.
  - ARP spoofing: is a technique that allows an attacker to create a "fake" ARP packet that looks like it came from a different source, or has a fake MAC address in it.
  - Email Address Spoofing: creation of email messages with a forged sender address, e.g. for the purposes of social engineering and data phishing
  - Caller ID spoofing
  - Referrer Spoofing
  - ...

Caller ID spoofing



Make a Call

Emma Watson

63254

Private Number OFF

Default ri...

Vibrate

12/01/2015 20:44

0min

No Voice

0s

● Incoming ○ Outgoing

○ Missed

Emma Watson

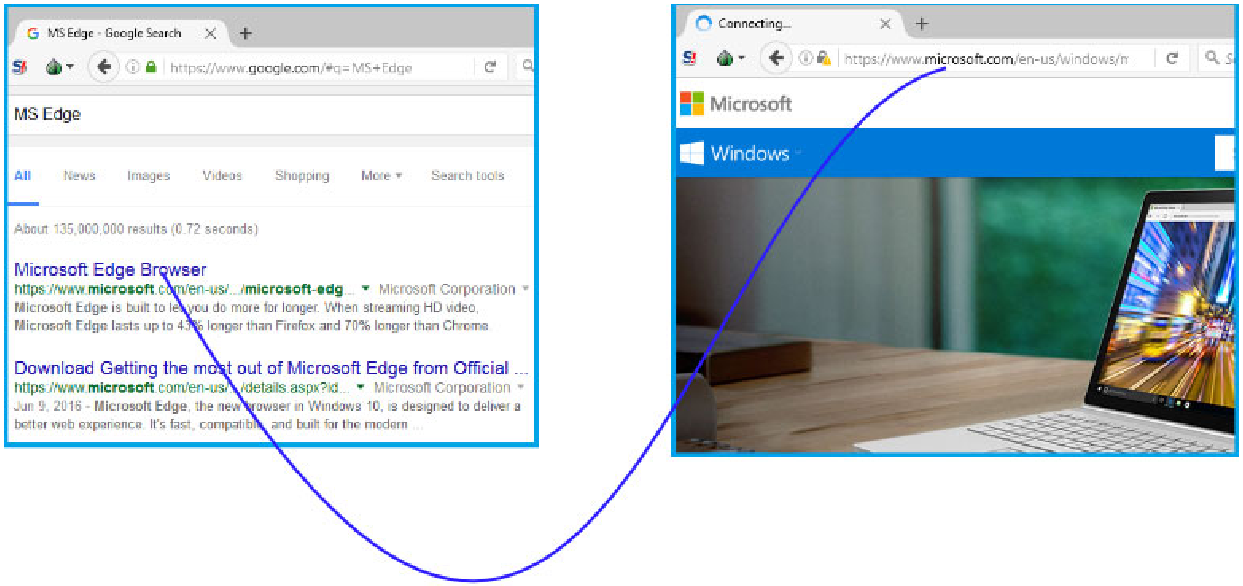
63254

Incoming call

Referrer

https://www.whatismyreferer.com/

- The referer is an HTTP header that allows a site to identify where the request is coming from. For example, if we search for “MS Edge” in Google and click on the first link, the browser will navigate to microsoft.com sending google.com as the referer. Microsoft will know that we are coming from Google because the referer is sent by the browser when doing the request.
- The referrer should be the URL that initiated the request.
- The referer is not only sent when clicking on a link but also on every resource that is requested.



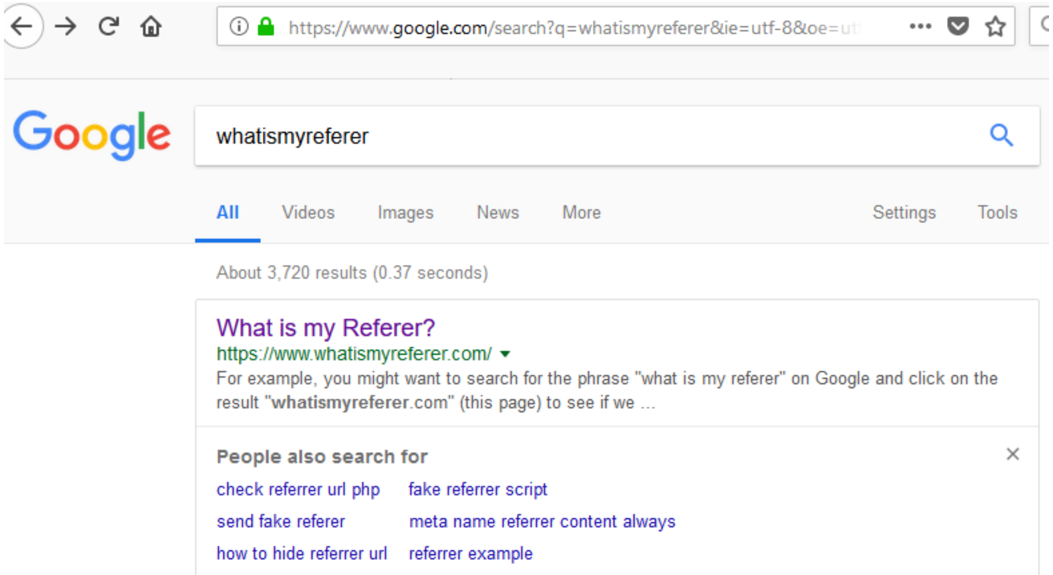
About 135,000,000 results (0.72 seconds)

Microsoft Edge Browser
https://www.microsoft.com/en-us/.../microsoft-edg... ▾ Microsoft Corporation ▾
Microsoft Edge is built to let you do more for longer. When streaming HD video, Microsoft Edge lasts up to 43% longer than Firefox and 70% longer than Chrome ...

Download Getting the most out of Microsoft Edge from Official ...
https://www.microsoft.com/en-us/.../details.aspx?id... ▾ Microsoft Corporation ▾
Jun 9, 2016 - Microsoft Edge, the new browser in Windows 10, is designed to deliver a better web experience. It's fast, compatible, and built for the modern ...

When we click on the link, the browser will send the HTTP REFERER to the new site. In other words, microsoft.com will know the URL where we are coming from.

Referrer cont…


https://www.google.com/search?q=whatismyreferer&ie=utf-8&oe=ut
Google
All
Videos
Images
News
More
Settings
Tools

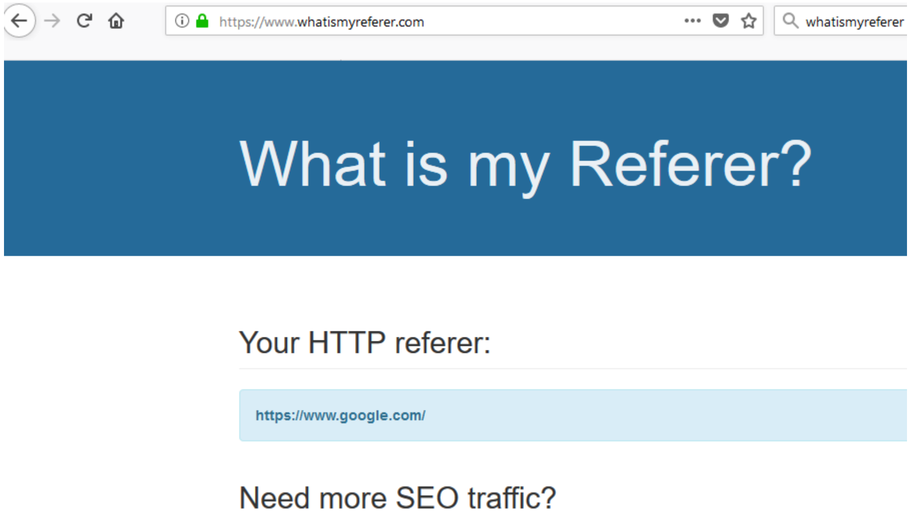
whatismyreferer

About 3,720 results (0.37 seconds)

What is my Referer?
https://www.whatismyreferer.com/
For example, you might want to search for the phrase "what is my referer" on Google and click on the result "**whatismyreferer**.com" (this page) to see if we ...

People also search for

check referrer url php
fake referrer script
send fake referer
meta name referrer content always
how to hide referrer url
referrer example



What is my Referer?

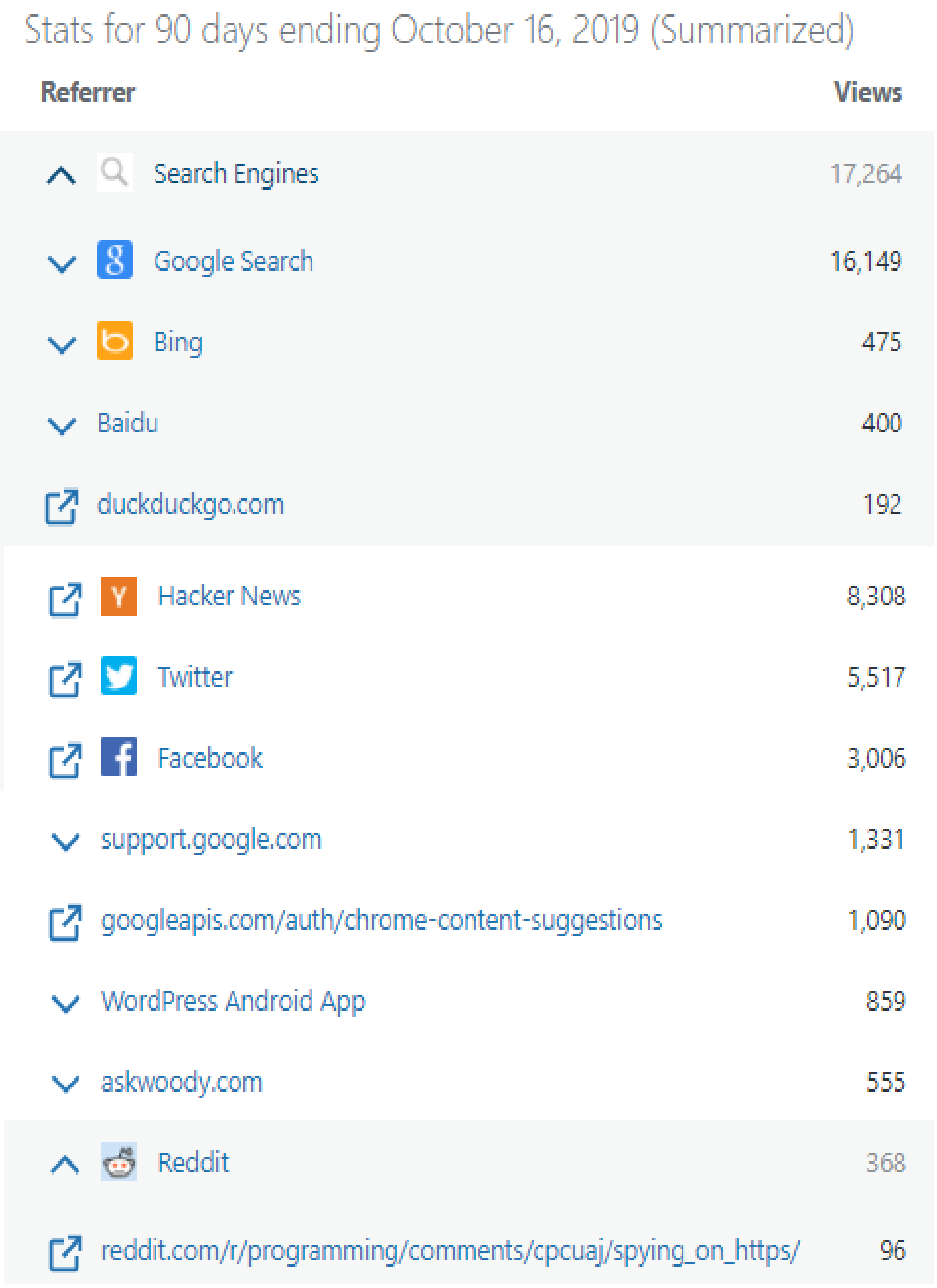
Your HTTP referer:

https://www.google.com/

Need more SEO traffic?

Referrer cont…

- The Referrer mechanism can be very useful, because it helps a site owner understand from where their traffic is originating. For instance, WordPress automatically generates this dashboard which shows where the blog gets its visitors.



Stats for 90 days ending October 16, 2019 (Summarized)

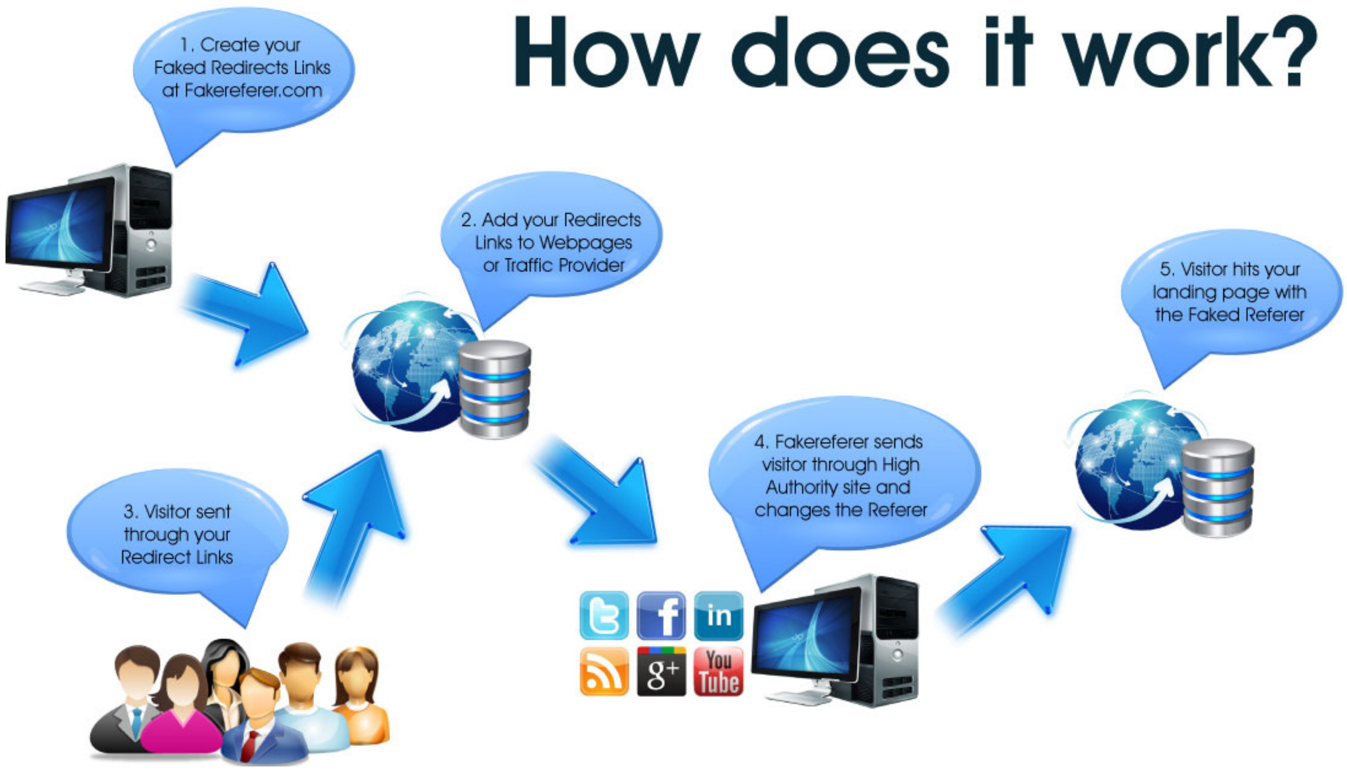
Referrer	Views
Search Engines	17,264
Google Search	16,149
Bing	475
Baidu	400
duckduckgo.com	192
Hacker News	8,308
Twitter	5,517
Facebook	3,006
support.google.com	1,331
googleapis.com/auth/chrome-content-suggestions	1,090
WordPress Android App	859
askwoody.com	555
Reddit	368
reddit.com/r/programming/comments/cpcuaj/spying_on_https/	96

Referrer cont…

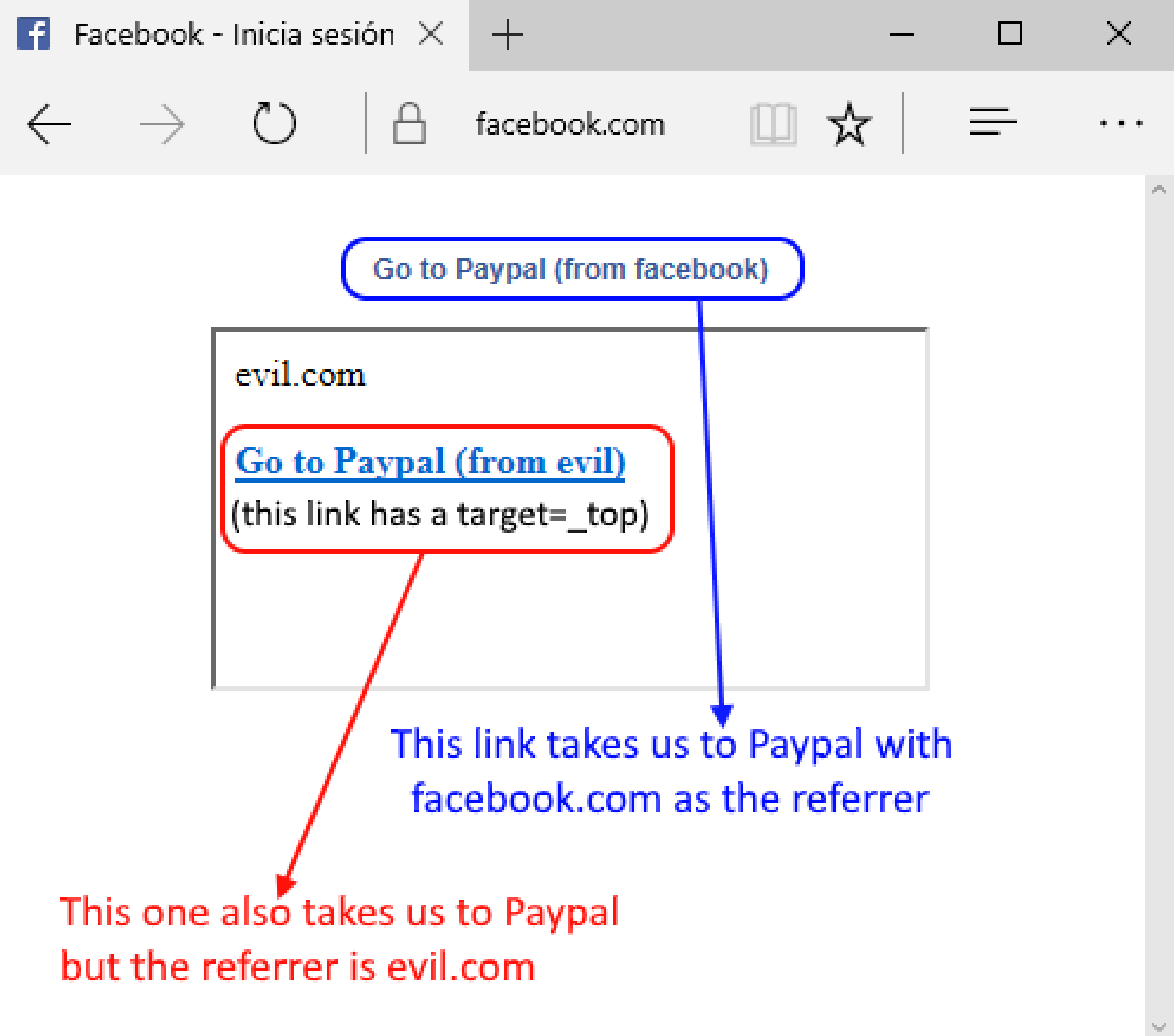
- The Referrer is omitted in some cases, including:
  - When the user navigates via some mechanism other than a link in the page (e.g. choosing a bookmark or using the address box)
  - When navigating from HTTPS pages to HTTP pages
  - When navigating from a resource served by a protocol other than HTTP(S)
  - When the page opts-out

Referrer cont…

- Spoofing the referrer means hiding where the traffic is coming from. i.e. If you're doing something the networks wouldn't necessarily approve of, you can hind that source and all they see is whatever you want them to see, more or less.
-


How does it work?
1. Create your Faked Redirects Links at Fakereferer.com
2. Add your Redirects Links to Webpages or Traffic Provider
3. Visitor sent through your Redirect Links
4. Fakereferer sends visitor through High Authority site and changes the Referer
5. Visitor hits your landing page with the Faked Referer
in
You Tube

Referrer cont…



Go to Paypal (from facebook)

evil.com

Go to Paypal (from evil)
(this link has a target=_top)

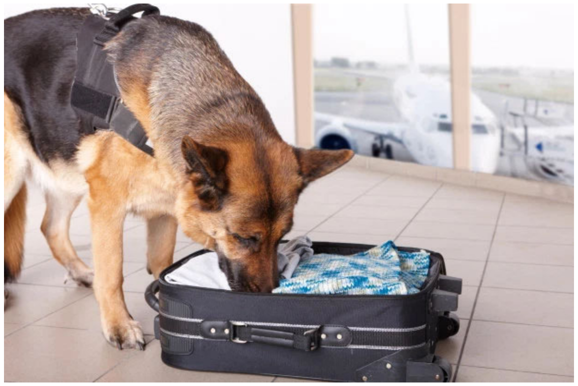
This link takes us to Paypal with facebook.com as the referrer

This one also takes us to Paypal but the referrer is evil.com

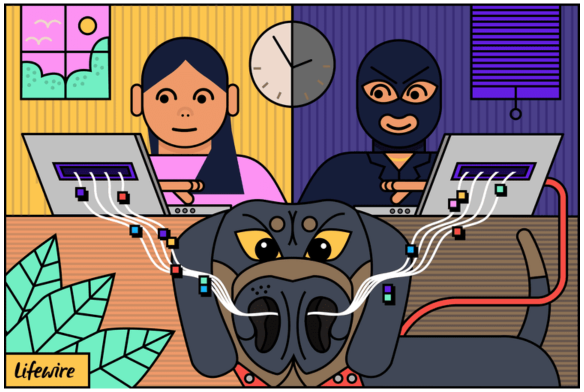
Sniffing

- Sniffing is a process of monitoring

Bomb-sniffing dogs



Drug-sniffing dogs



packet sniffing

Sniffing cont…

- Sniffing/Snooping is use of a program or device that can monitor data traveling over a network.

- Unauthorized sniffers can be very dangerous as they cannot be detected, yet they can sniff/extract critical information from the packets traveling over the network.

- Wireless sniffing is particularly simple, due to the ‘open’ nature of the wireless medium.

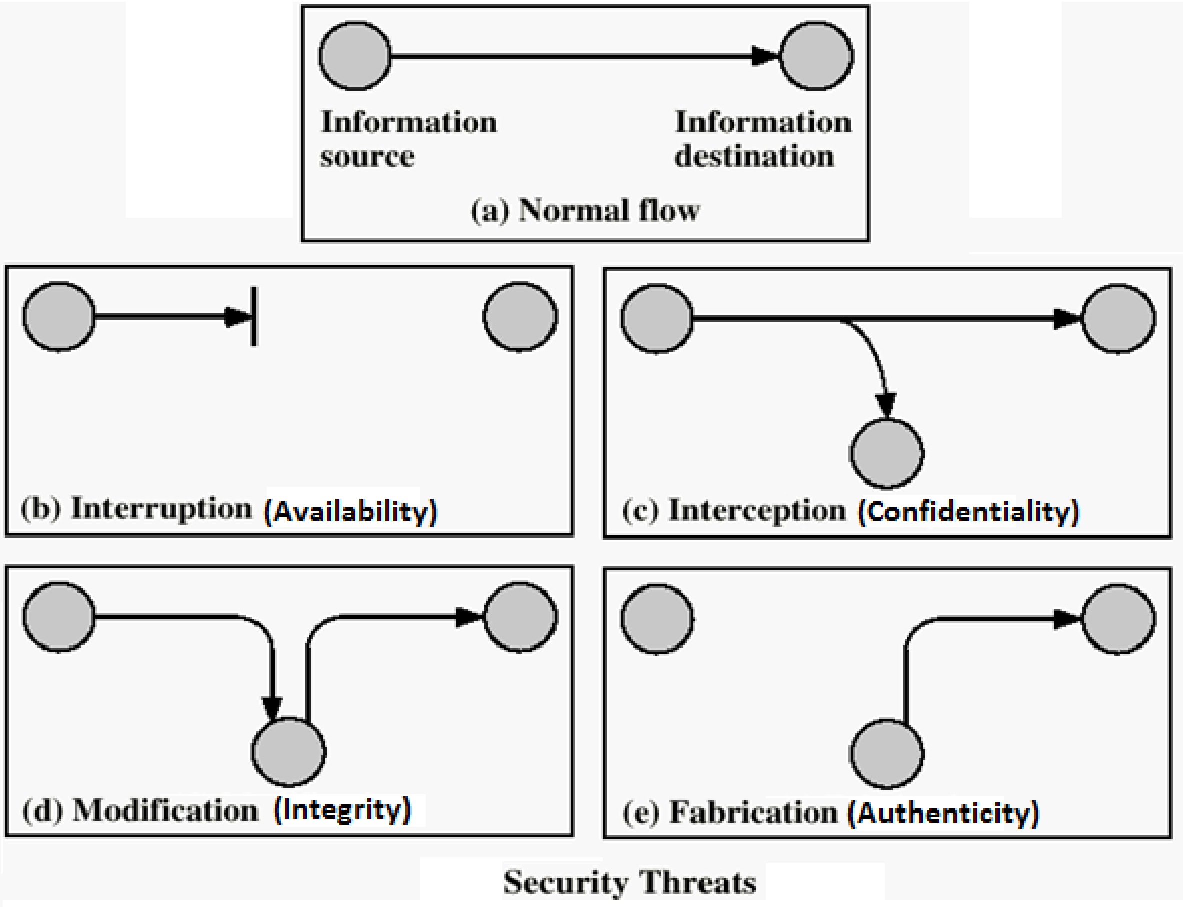
- Popular sniffers:
  - Wireshark
  - Cain & Abel

Comparison

- Spoofing
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- Sniffer
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, and so on

Cyber attack techniques

- Cyber attacks are commonly classified in four general categories:
  - Reconnaissance attacks
  - Access attacks
    - Social engineering
    - Man-in-the-middle
    - Man-in-the-browser
    - Phishing
    - Pharming
    - Whois
    - Physical
  - DoS attacks
    - Ping of death
    - Replay
    - DDoS
  - Malware
    - keylogger
    - Spyware
    - Virus
    - Trojan
    - Worm


Information source
Information destination
(a) Normal flow
(b) Interruption (Availability)
(c) Interception (Confidentiality)
(d) Modification (Integrity)
(e) Fabrication (Authenticity)
Security Threats

Reconnaissance attacks

- The word reconnaissance is borrowed from its military use, where it refers to a mission into enemy territory to obtain information (e.g. drone).

- Reconnaissance attack is any form of information gathering activities about vulnerabilities by intruders which is used to compromise networks.

- Usually, software tools are used to figure out network resources and exploit potential weaknesses in the targeted networks, hosts, and applications.

Access attacks

- Data collected from Reconnaissance attack is used to start access attacks. Exploiting the discovered vulnerabilities enables the attacker to gain access to web account, e-mail accounts, databases, and other confidential or sensitive information.

- Access attacks:
  - Social engineering
  - Man-in-the-middle
  - Man-in-the-browser
  - Phishing
  - Pharming
  - Whois
  - Physical
  - …

Social engineering

- Social engineering is the art of manipulating (فریب) people so they give up confidential information. Social Engineering is all about deceiving people, not machines.

- Social engineering is usually highly successful because people are often willing to help or already know the person.

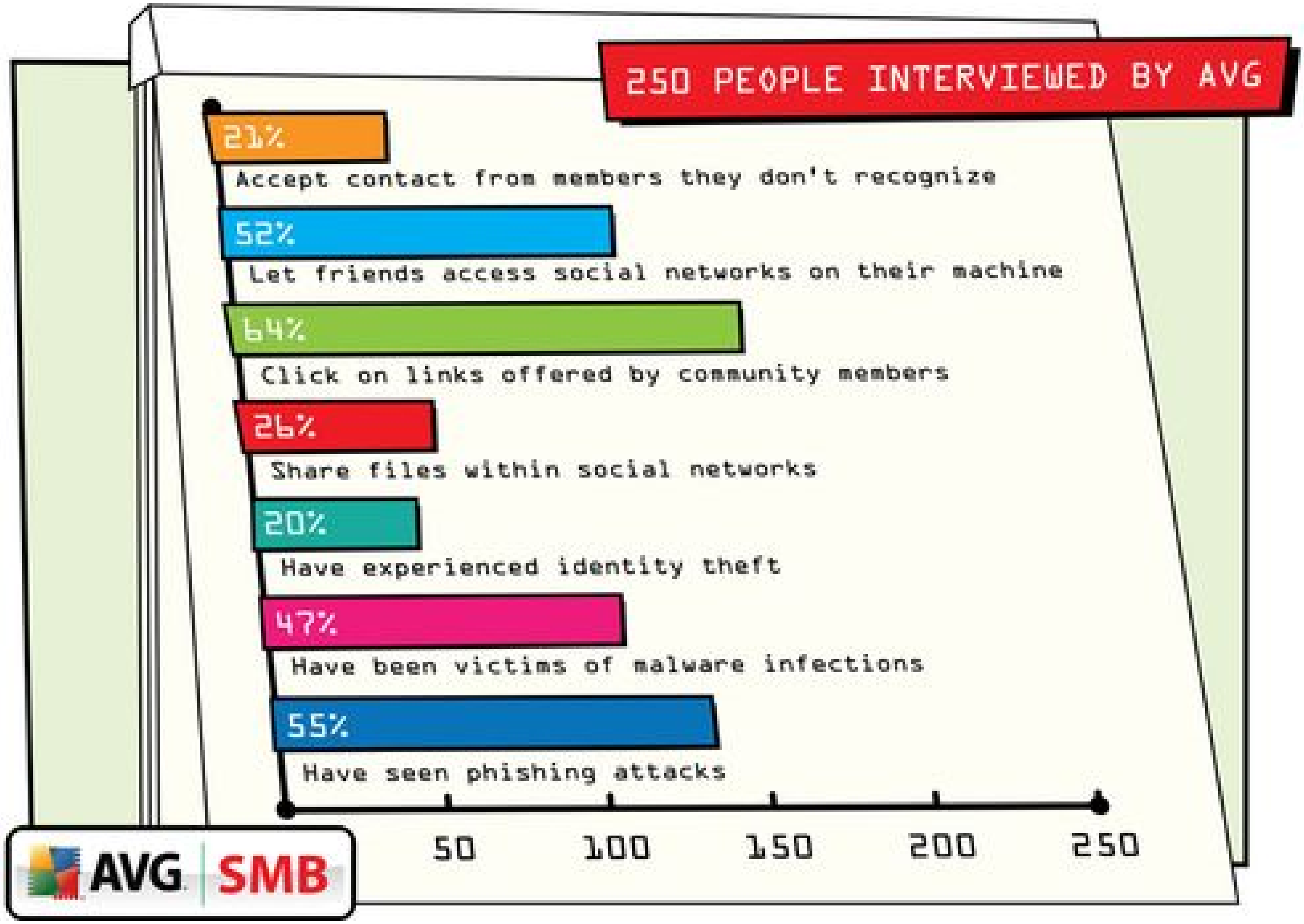
- The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Manipulate دستکاری کردن

Social engineering cont…

- Example:
  - Attacker uses spoofed caller ID (some phone companies sell such services)
  - Appears attacker has company phone number which may give attacker instant credibility

Social engineering cont…



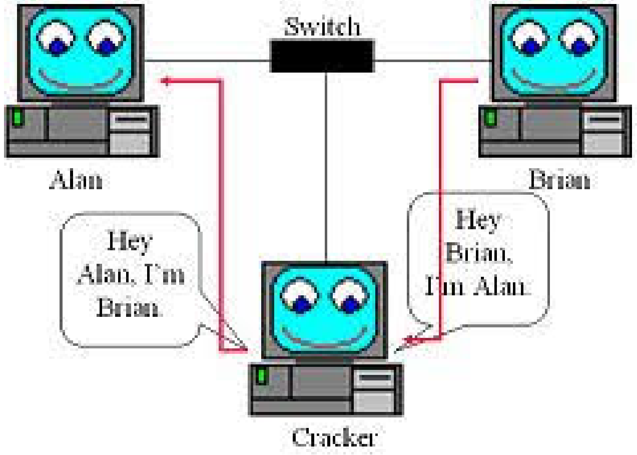
Social engineering defense

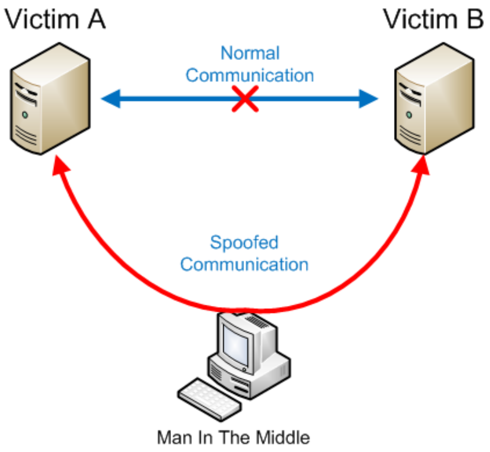
- These trusted friends help stealing company sensitive information. Thus, social engineering can defeat strongest security protocols while the attacker may not even touch keyboard.

- Social engineering is hard to defend because it is rooted in human nature. The best way to avoid this risk is to educate employees:
  - Do not give out sensitive info (passwords) based on friendship relations
  - Do not trust caller ID
  - …

Man-in-the-Middle attack

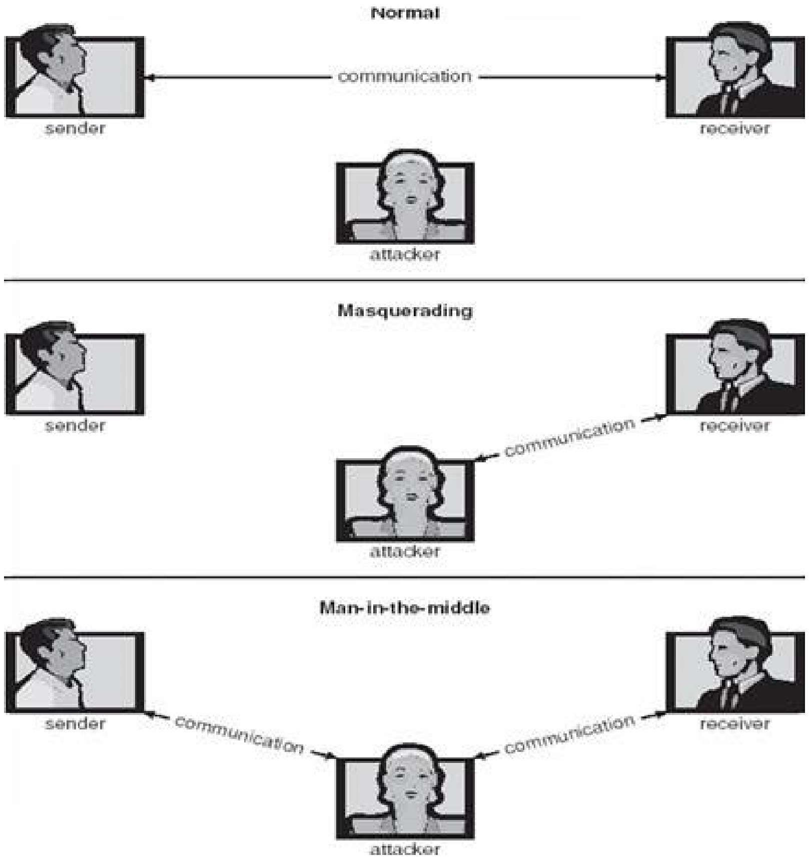
- In the man-in the-middle (MITM) attack, the attacker takes place in the middle of the customer computer and the bank web sites. The attacker:
  - first impersonates the identity of both customer computer and the bank
  - then communicates with one of them on behalf of the another one.
- The attacker intercepts all the information transmitted between the customer and the bank and investigates the data to find sensitive information such as passwords.
- Thus, MITM tries to make two computers to believe that they are communicating with each other, when actually they are sending and receiving data with the attacker.



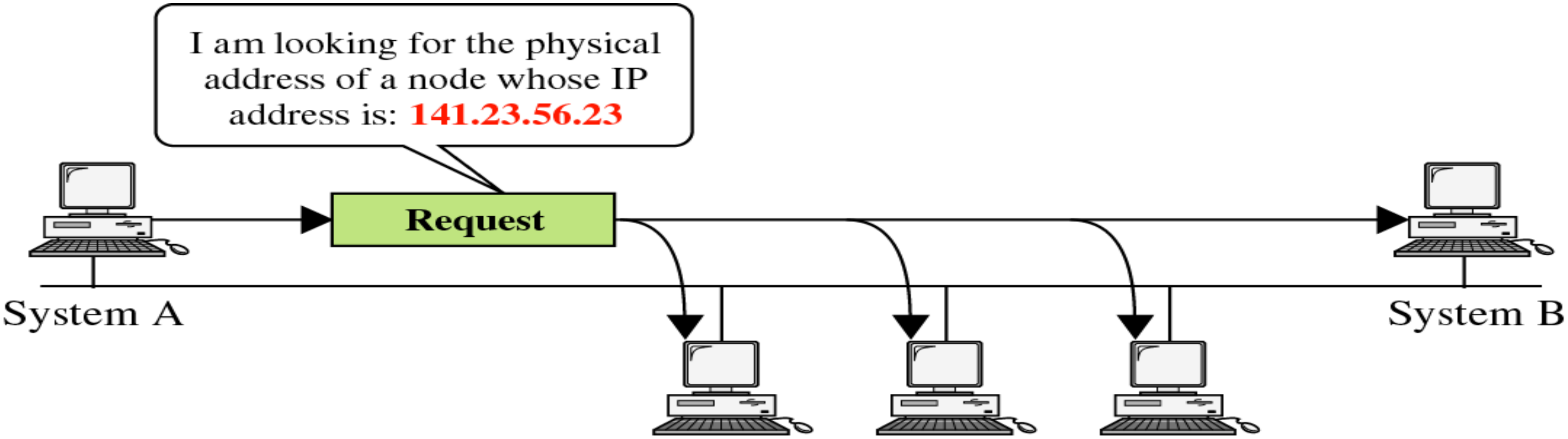


Man-in-the-Middle attack cont…

- Man in the Middle attack can be:
  - Passive attack: attacker captures sensitive data being transmitted and sends it to the original recipient without changing it.
  - Active attack: contents of the message are intercepted and altered before being sent on.
    - ARP Poisoning
    - DNS Poisoning

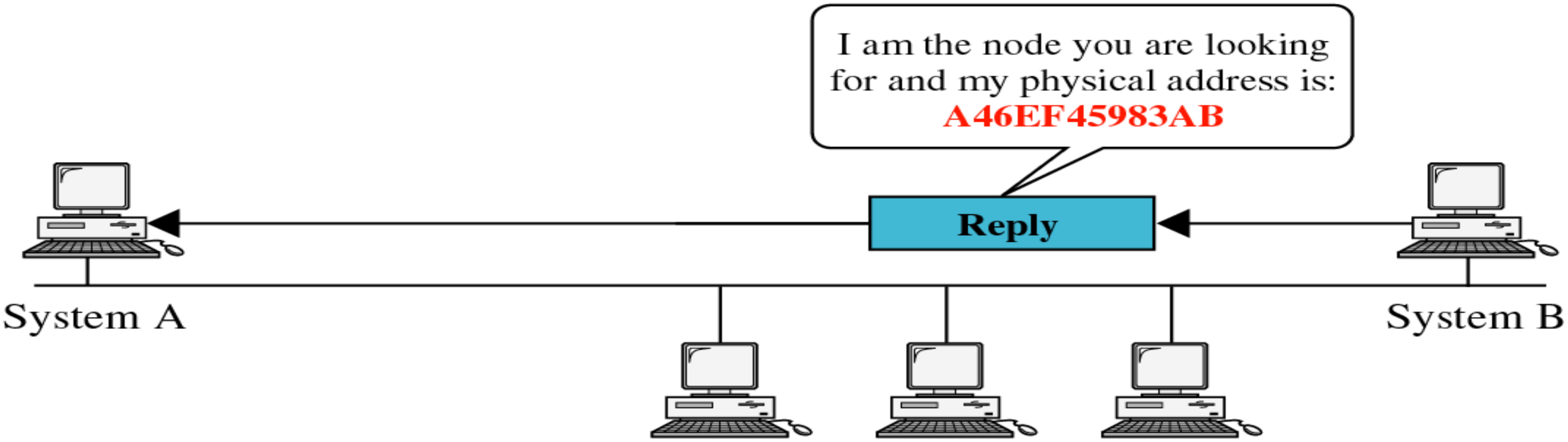


ARP operation



I am looking for the physical address of a node whose IP address is: **141.23.56.23**

a. ARP request is broadcast



I am the node you are looking for and my physical address is: **A46EF45983AB**

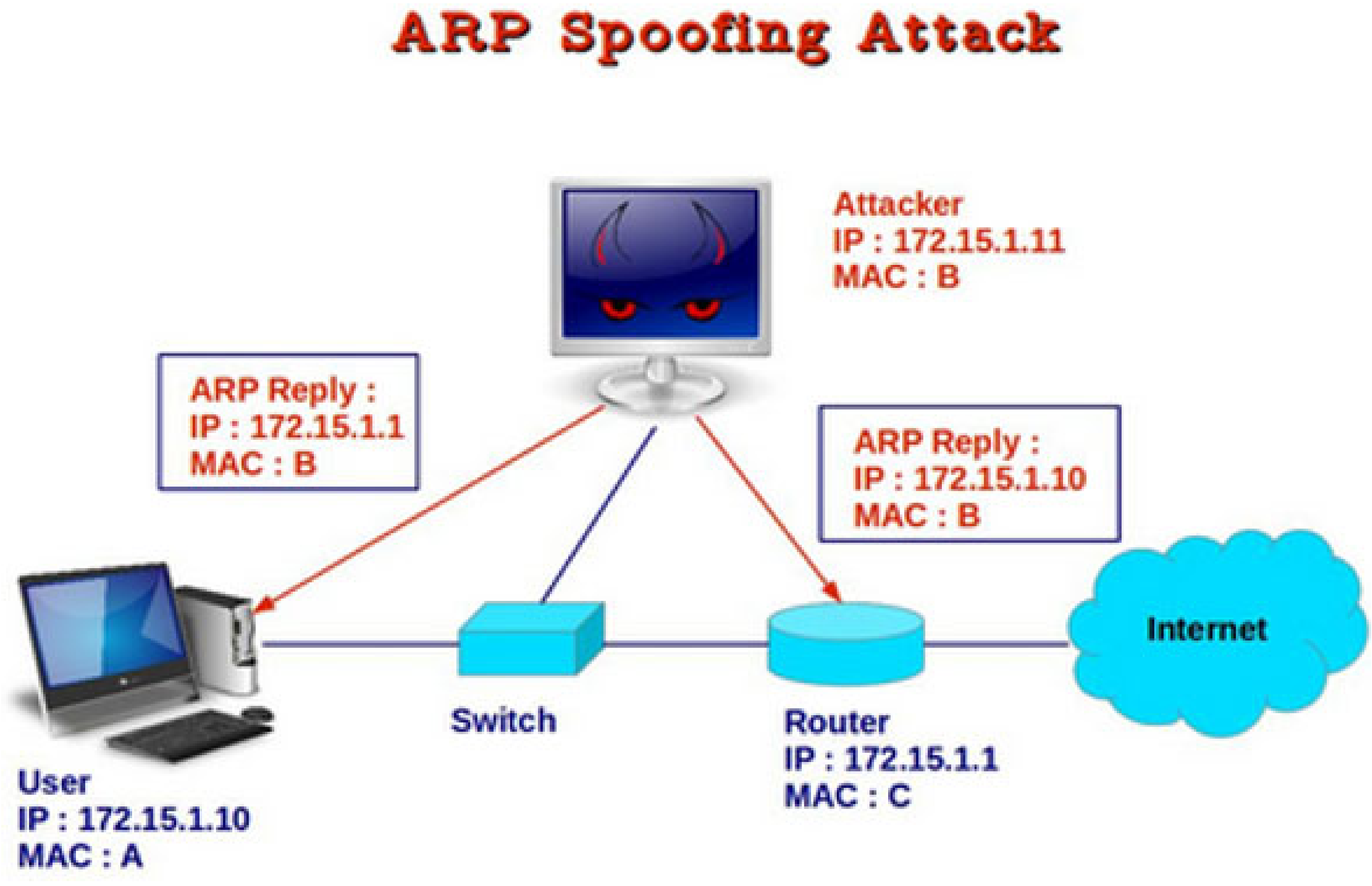
b. ARP reply is unicast

ARP poisoning

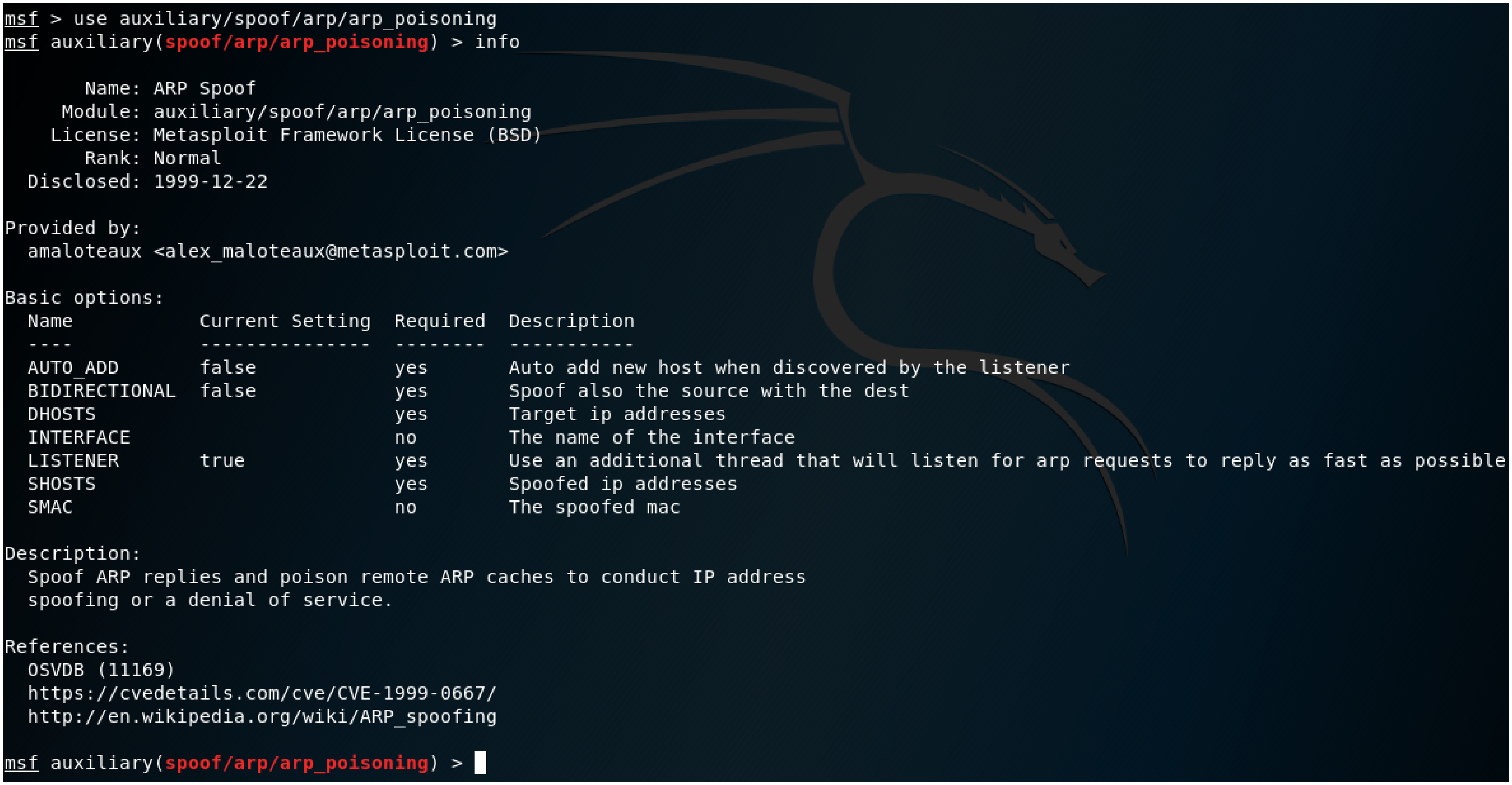
- ARP poisoning is an attack that is accomplished using the technique of ARP spoofing.

- An attacker uses the process of ARP spoofing to "poison" a victim's ARP table, so that it contains incorrect or altered IP-to-MAC address mappings for various attacks, such as a man-in-the-middle attack.

ARP poisoning cont…



ARP poisoning cont…



```
msf > use auxiliary/spoof/arp/arp_poisoning
msf auxiliary(spoof/arp/arp_poisoning) > info

       Name: ARP Spoof
     Module: auxiliary/spoof/arp/arp_poisoning
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 1999-12-22

Provided by:
  amaloteaux <alex_maloteaux@metasploit.com>

Basic options:
  Name           Current Setting  Required  Description
  ----           ---------------  --------  -----------
  AUTO_ADD       false            yes       Auto add new host when discovered by the listener
  BIDIRECTIONAL  false            yes       Spoof also the source with the dest
  DHOSTS                          yes       Target ip addresses
  INTERFACE                       no        The name of the interface
  LISTENER       true             yes       Use an additional thread that will listen for arp requests to reply as fast as possible
  SHOSTS                          yes       Spoofed ip addresses
  SMAC                            no        The spoofed mac

Description:
  Spoof ARP replies and poison remote ARP caches to conduct IP address
  spoofing or a denial of service.

References:
  OSVDB (11169)
  https://cvedetails.com/cve/CVE-1999-0667/
  http://en.wikipedia.org/wiki/ARP_spoofing

msf auxiliary(spoof/arp/arp_poisoning) > 
```

exploit (program or technique that exploits a vulnerability in other software)