KỸ THUẬT TẤN CÔNG VÀ PHÒNG THỦ TRÊN KHÔNG GIAN MẠNG

NỘI DUNG

- Module 01: Tổng quan An ninh mạng
- Module 02: Kỹ thuật tấn công
- Module 03: Kỹ thuật mã hóa
- Module 04: Bảo mật hệ điều hành
- Module 05: Bảo mật ứng dụng
- Module 06: Virus và mã độc
- Module 07: Các công cụ phân tích an ninh mạng
- Module 08: Chính sách bảo mật và phục hồi thảm họa dữ liệu
- Ôn tập
- Báo cáo cuối khóa

Module 02: KỸ THUẬT TẤN CÔNG

- Lesson 01: Footprinting và Reconnaissance
- Lesson 02: Google Hacking
- Lesson 03: Scanning Networks
- Lesson 04: Enumeration
- Lesson 05: System Hacking
- Lesson 06: Sniffer hệ thống mạng
- Lesson 07: Social Engineering
- Lesson 08: Denial of Service
- Lesson 09: Session Hijacking
- Lesson 10: SQL Injection
- Lesson 11: Hacking Wireless Networks
- Lesson 12: Buffer Overflow

Nội dung

- Giới thiệu Google
- Kỹ thuật tìm kiếm với Google

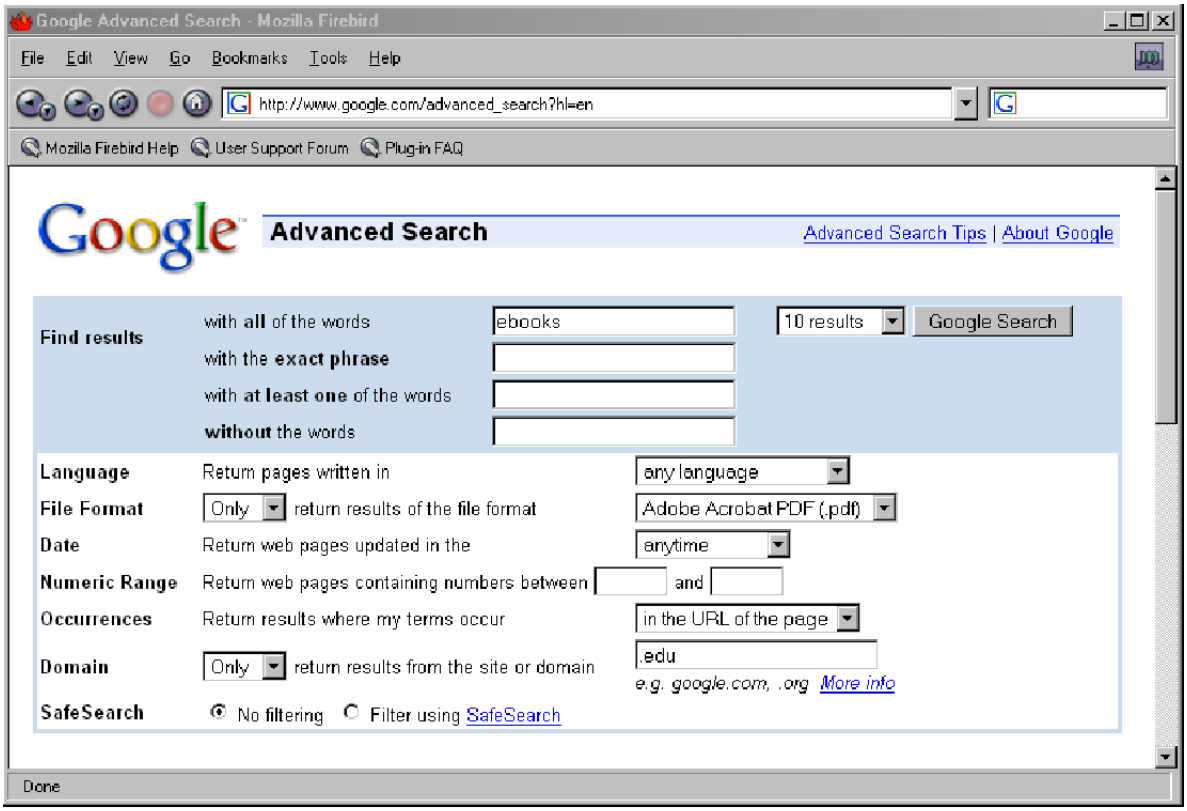
Giới thiệu Google

- Google là cỗ máy tìm kiếm mạnh mẽ và phổ biến nhất thế giới, nó có khả năng chấp nhận những lệnh được định nghĩa sẵn khi nhập vào và cho những kết quả rất hữu ích.
- Sử dụng Google để thu thập những thông tin bí mật và nhạy cảm, những cái mà không thể nhìn thấy qua những công cụ tìm kiếm thông thường.

Giới thiệu Google

- Các yếu tố cần khi tìm kiếm:
  - Niềm tin.
  - Tính kiên nhẫn.
  - Kinh nghiệm search.
  - Khả năng sử dụng công cụ tìm kiếm

Kỹ thuật tìm kiếm với Google



Kỹ thuật tìm kiếm với Google

- site (.edu, .gov, foundstone.com, usc.edu)
- filetype (txt, xls, mdb, pdf, .log)
- Daterange (julian date format)
- Intitle / allintitle
- Inurl / allinurl
- …

Kỹ thuật tìm kiếm với Google

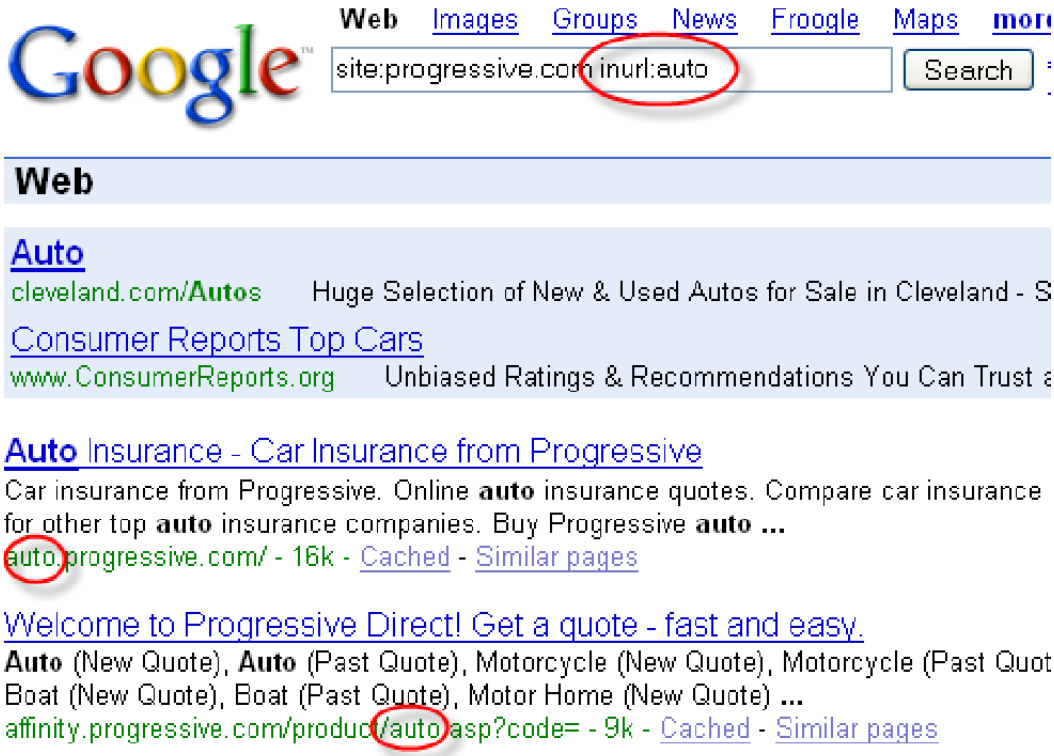
- Cú pháp "site:" giới hạn Google chỉ truy vấn những từ khóa xác định trong một site hoặc tên miền riêng biệt.

  vd: site (.edu, .gov, progressive.com, usc.edu)

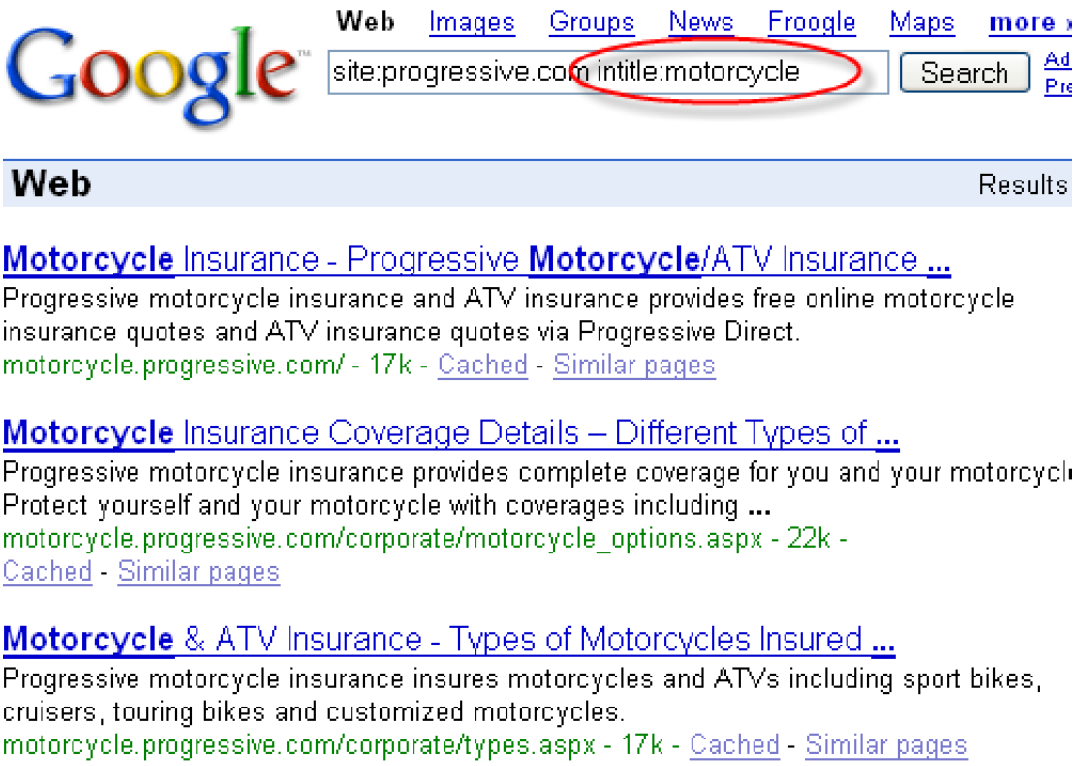
Kỹ thuật tìm kiếm với Google

- Cú pháp "inurl:" giới hạn kết quả tìm kiếm về những địa chỉ URL có chứa từ khóa tìm kiếm.
- Tương tự, nếu ta muốn truy vấn nhiều hơn một từ trong URL thì ta có thể dùng "allinurl:" thay cho "inurl" để được kết quả là những URL chứa tất cả những từ khóa tìm kiếm.

Kỹ thuật tìm kiếm với Google



Kỹ thuật tìm kiếm với Google



Kỹ thuật tìm kiếm với Google

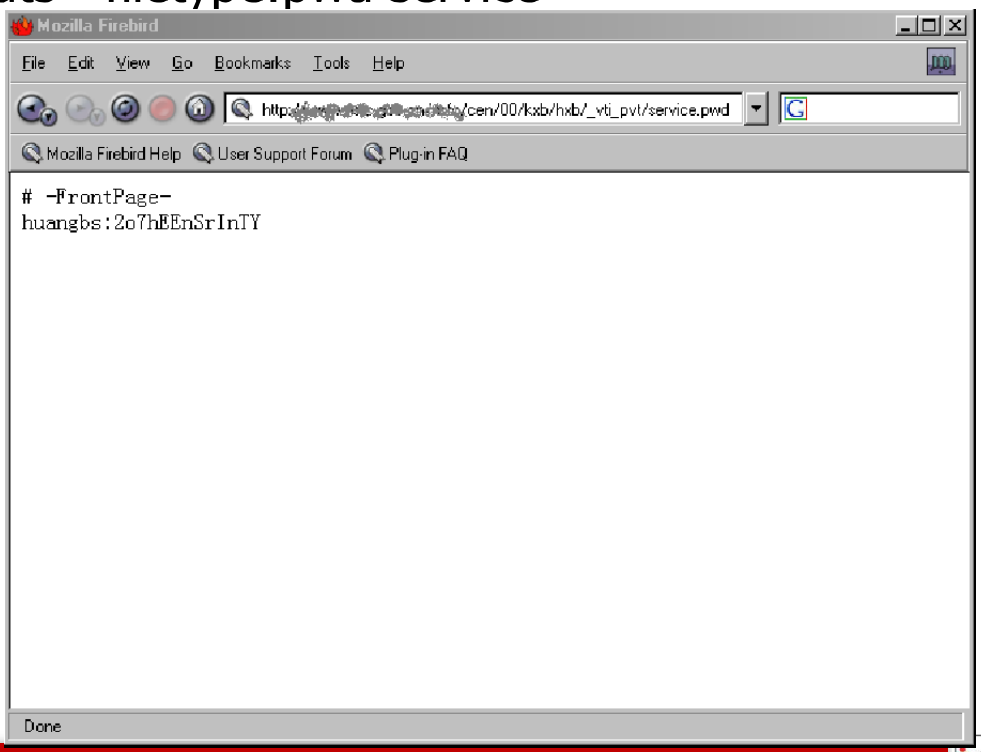
- Cú pháp "filetype:" giới hạn Google chỉ tìm kiếm những files trên internet có phần mở rộng riêng biệt (Ví dụ: doc, xml, pdf hay ppt v.v...).

Kỹ thuật tìm kiếm với Google

- Cú pháp "link:" sẽ liệt kê những trang web mà có các liên kết đến đến những trang web chỉ định.
- Cú pháp "related:" sẽ liệt kê các trang Web "tương tự" với trang Web chỉ định.
- Truy vấn "cache:" sẽ cho kết quả là phiên bản của trang Web mà mà Google đã lưu lại.
- Cú pháp "intext:" tìm kiếm các từ trong một website riêng biệt. Nó lượt bỏ các liên kết hoặc URL và tiêu đề của trang.
- "phonebook" tìm kiếm thông tin về các địa chỉ đường phố ở Mỹ và số điện thoại.

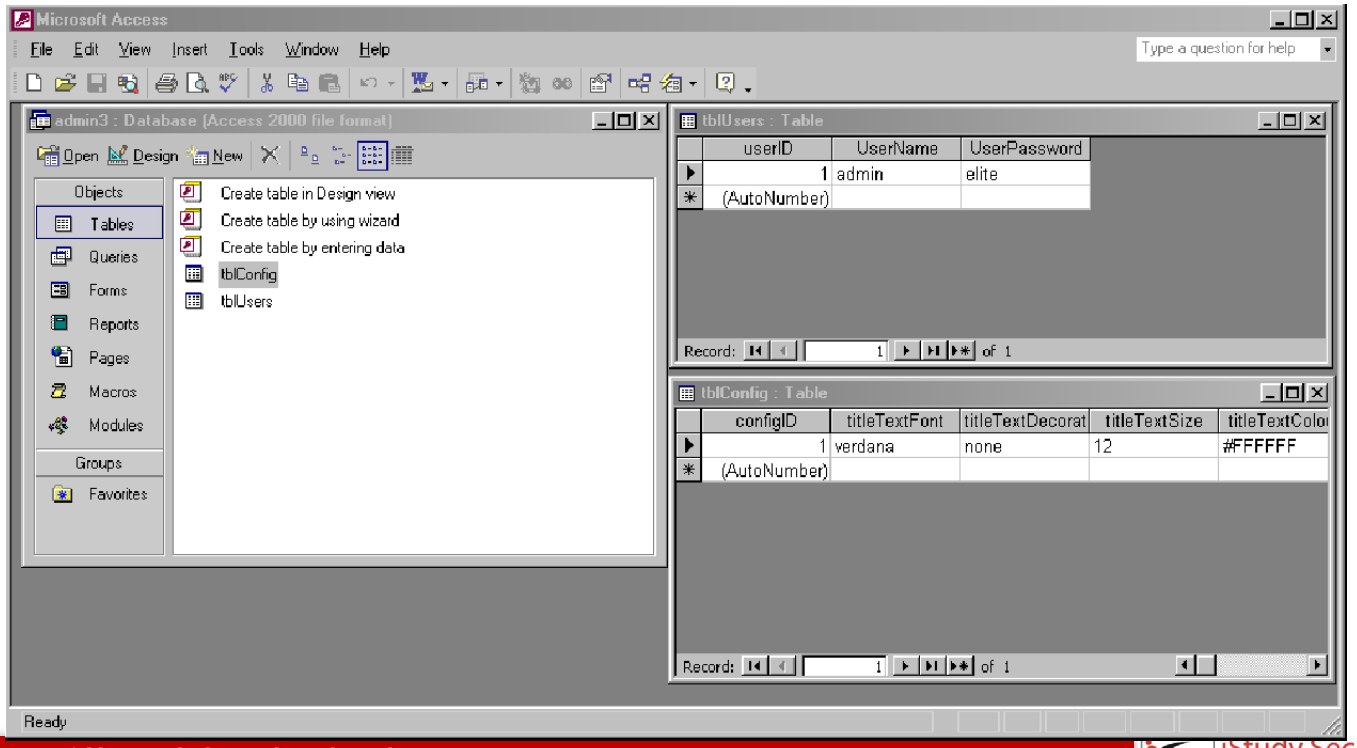
Kỹ thuật tìm kiếm với Google

- Threats - filetype:pwd service



Kỹ thuật tìm kiếm với Google

- Threats – allinurl: admin mdb



Kỹ thuật tìm kiếm với Google

- Cú pháp tìm kiếm nâng cao với Google
  - *Sử dụng cú pháp "Index of " để tìm kiếm các site cho phép duyệt chỉ mục:*

    Index of /admin
    Index of /passwd
    Index of /password
    Index of /mail
    "Index of /" +passwd
    "Index of /" +password.txt
    "Index of /" +.htaccess
    "Index of /secret"
    "Index of /confidential"
    "Index of /root"
    "Index of /cgi-bin"
    "Index of /credit-card"
    "Index of /logs"
    "Index of /config"

Kỹ thuật tìm kiếm với Google

- Cú pháp tìm kiếm nâng cao với Google
  - *Tìm kiếm các site hoặc server dễ bị tấn công sử dụng cú pháp "inurl:" hoặc "allinurl:"*

    inurl:admin filetype:txt
    inurl:admin filetype:db
    inurl:admin filetype:cfg
    inurl:mysql filetype:cfg
    inurl:passwd filetype:txt
    inurl:iisadmin
    inurl:auth_user_file.txt
    inurl:orders.txt
    inurl:"wwwroot/*."
    inurl:adpassword.txt
    inurl:webeditor.php
    inurl:file_upload.php
    inurl:gov filetypels "restricted"
    index of ftp +.mdb allinurl:/cgi-bin/ +mailto

Kỹ thuật tìm kiếm với Google

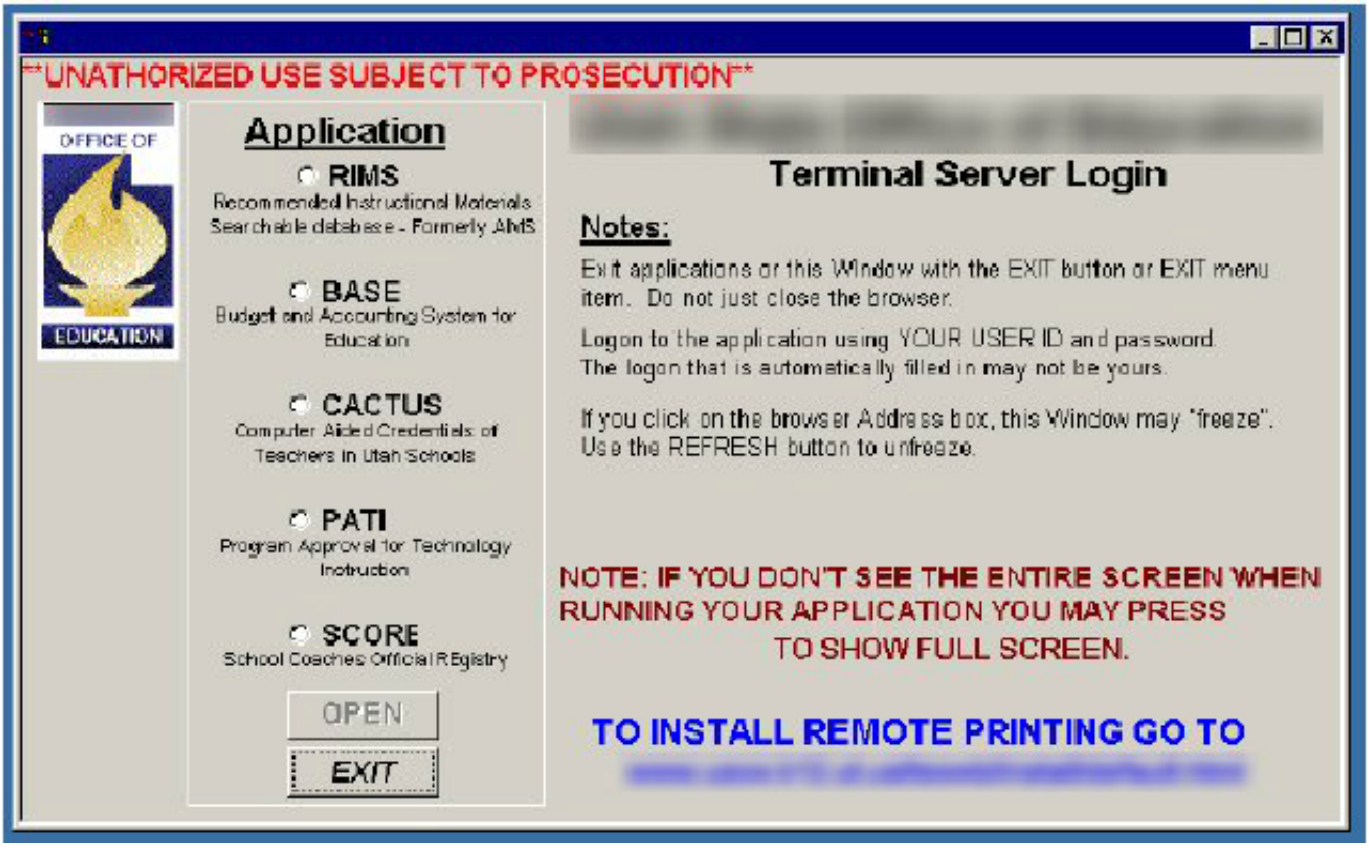
- Cú pháp tìm kiếm nâng cao với Google
  - *Tìm kiếm các site hoặc server dễ bị tấn công dùng "intitle:" hoặc "allintitle:"*

```
intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"index of" passwd
intitle:"index of" people.lst
intitle:"index of" pwd.db
intitle:"index of" etc/shadow
intitle:"index of" spwd
intitle:"index of" master.passwd
intitle:"index of" htpasswd
intitle:"index of" members OR accounts
intitle:"index of" user_carts OR user_cart
allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:gov
```

Kỹ thuật tìm kiếm với Google

- Cú pháp tìm kiếm nâng cao với Google
  - Để tìm những site dễ bị tấn công bằng phương pháp Cross-Sites Scripting (XSS):
    - allinurl:/scripts/cart32.exe
    - allinurl:/CuteNews/show_archives.php
    - allinurl:/phpinfo.php
  - Để tìm những site dễ bị tấn công bằng phương pháp SQL Injection:
    - allinurl:/privmsg.php
    - allinurl:/privmsg.php

Threats - intitle:Remote.Desktop.Web.Connection inurl:tsweb



TÓM LƯỢC BÀI HỌC

- Tìm kiếm với Google.
- Các kỹ thuật cần thiết.
- Các điểm cần lưu ý.

Q & A