

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

The screenshot shows the Google Advanced Search page in a Mozilla Firebird browser window. The address bar displays the URL `http://www.google.com/advanced_search?hl=en`. The page features the Google logo and the title "Advanced Search". Below the logo, there are links for "Advanced Search Tips" and "About Google". The main search area includes a text input field containing "ebooks" and a dropdown menu showing "10 results". A "Google Search" button is located to the right of the input field. Below the search area, there are several filter options: "Find results" with radio buttons for "with all of the words", "with the exact phrase", "with at least one of the words", and "without the words"; "Language" with a dropdown menu set to "any language"; "File Format" with a dropdown menu set to "Adobe Acrobat PDF (.pdf)"; "Date" with a dropdown menu set to "anytime"; "Numeric Range" with two input fields for "between" and "and"; "Occurrences" with a dropdown menu set to "in the URL of the page"; "Domain" with a dropdown menu set to ".edu" and a link to "More info"; and "SafeSearch" with radio buttons for "No filtering" and "Filter using SafeSearch".

Google Advanced Search - Mozilla Firebird

File Edit View Go Bookmarks Tools Help

`http://www.google.com/advanced_search?hl=en`

Mozilla Firebird Help User Support Forum Plugin FAQ

Google™ Advanced Search [Advanced Search Tips](#) | [About Google](#)

Find results with all of the words with the exact phrase with at least one of the words without the words

Language Return pages written in any language

File Format Only return results of the file format Adobe Acrobat PDF (.pdf)

Date Return web pages updated in the anytime

Numeric Range Return web pages containing numbers between and

Occurrences Return results where my terms occur in the URL of the page

Domain Only return results from the site or domain .edu e.g. google.com, .org [More info](#)

SafeSearch ☒ No filtering ☐ Filter using [SafeSearch](#)

Done

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



Web

Auto

[cleveland.com/Autos](#) Huge Selection of New & Used Autos for Sale in Cleveland - S

[Consumer Reports Top Cars](#)

[www.ConsumerReports.org](#) Unbiased Ratings & Recommendations You Can Trust a

Auto Insurance - Car Insurance from Progressive

Car insurance from Progressive. Online **auto** insurance quotes. Compare car insurance for other top **auto** insurance companies. Buy Progressive **auto** ...

[auto.progressive.com/](#) - 16k - [Cached](#) - [Similar pages](#)

[Welcome to Progressive Direct! Get a quote - fast and easy.](#)

Auto (New Quote), **Auto** (Past Quote), Motorcycle (New Quote), Motorcycle (Past Quot
Boat (New Quote), Boat (Past Quote), Motor Home (New Quote) ...

[affinity.progressive.com/product/auto.asp?code=](#) - 9k - [Cached](#) - [Similar pages](#)

Kỹ thuật tìm kiếm với Google



Web

Results

[Motorcycle Insurance - Progressive Motorcycle/ATV Insurance ...](#)

Progressive motorcycle insurance and ATV insurance provides free online motorcycle insurance quotes and ATV insurance quotes via Progressive Direct.

[motorcycle.progressive.com/-](#) - 17k - [Cached](#) - [Similar pages](#)

[Motorcycle Insurance Coverage Details – Different Types of ...](#)

Progressive motorcycle insurance provides complete coverage for you and your motorcycle. Protect yourself and your motorcycle with coverages including ...

[motorcycle.progressive.com/corporate/motorcycle_options.aspx](#) - 22k -

[Cached](#) - [Similar pages](#)

[Motorcycle & ATV Insurance - Types of Motorcycles Insured ...](#)

Progressive motorcycle insurance insures motorcycles and ATVs including sport bikes, cruisers, touring bikes and customized motorcycles.

[motorcycle.progressive.com/corporate/types.aspx](#) - 17k - [Cached](#) - [Similar pages](#)

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...).



Web

[AL](#) [AK](#) [AZ](#) [CA](#) [CT](#) [DE](#) [FL](#) [GA](#) [IA](#) [ID](#) [IL](#) [IN](#) [KY](#) [MA](#) [MN](#) [MO](#) [MS](#) [MT](#) [NC](#) [ND](#) [NH](#) [N](#)

File Format: Unrecognized - [View as HTML](#)

[AL](#) [AK](#) [AZ](#) [CA](#) [CT](#) [DE](#) [FL](#) [GA](#) [IA](#) [ID](#) [IL](#) [IN](#) [KY](#) [MA](#) [MN](#) [MO](#) [MS](#) [MT](#) [NC](#) [ND](#) [NH](#) [NJ](#) [NM](#) [NY](#) [NY](#)
[OK](#) [OR](#) [PA](#) [SD](#) [TN](#) [TX](#) [WY](#).

[www.progressive.com/teens/DrivingTest/DrivingTestStates.xml](#) - [Similar pages](#)

[teens/slideshow/slide1.swf](#) 6 [teens/slideshow/slide2.swf](#) 6 [teens/...](#)

File Format: Unrecognized - [View as HTML](#)

[teens/slideshow/slide1.swf](#) 6 [teens/slideshow/slide2.swf](#) 6 [teens/slideshow/slide3.swf](#) 6.

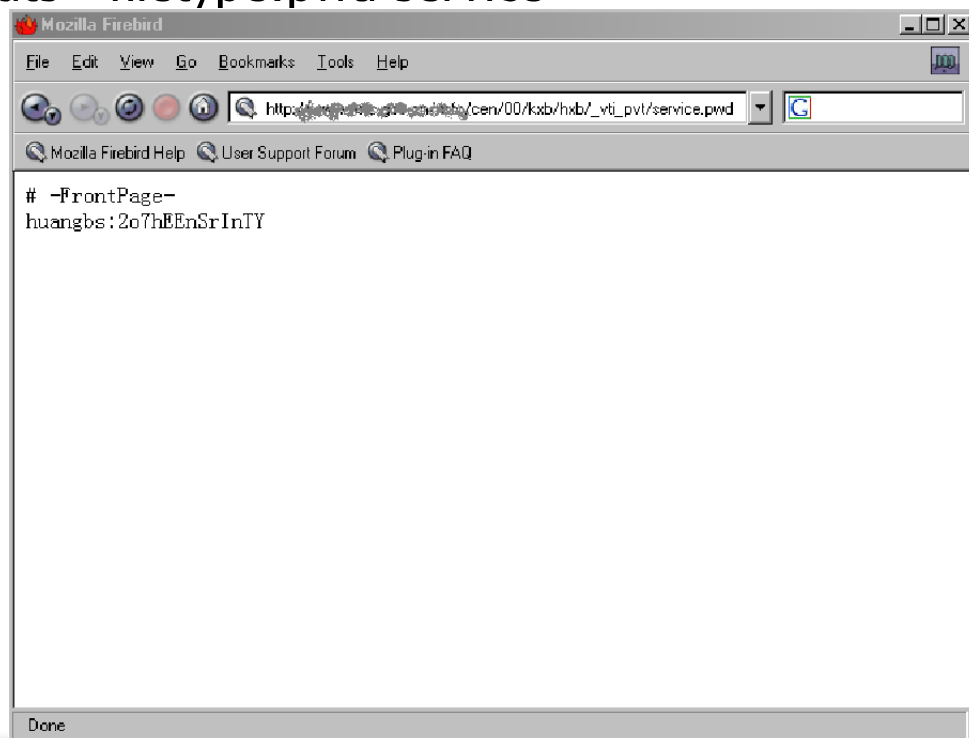
[www.progressive.com/teens/slideshow/slideshow.xml](#) - [Similar pages](#)

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 lược 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.

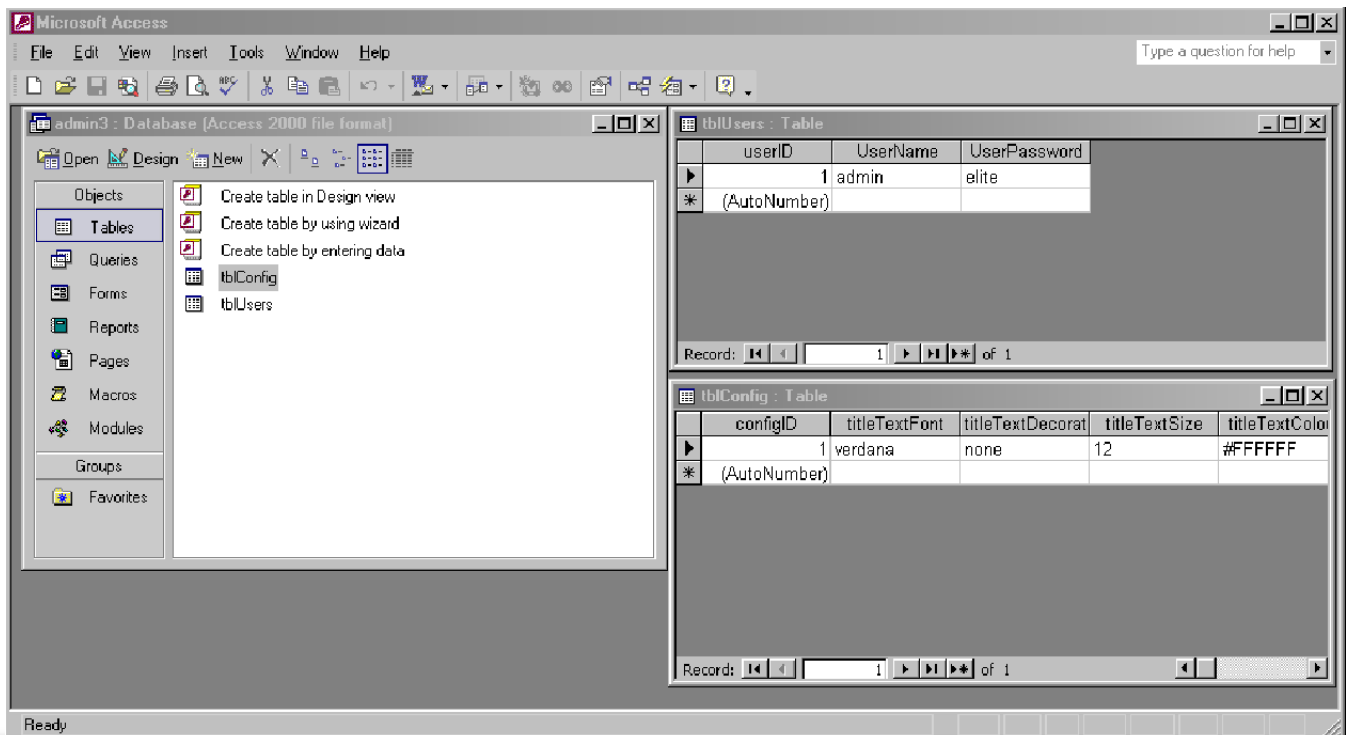
Kỹ thuật tìm kiếm với Google

- 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 filetype:pels "restricted"
 - index of ftp +.mdb allinurl:/cgi-bin/ +mailto

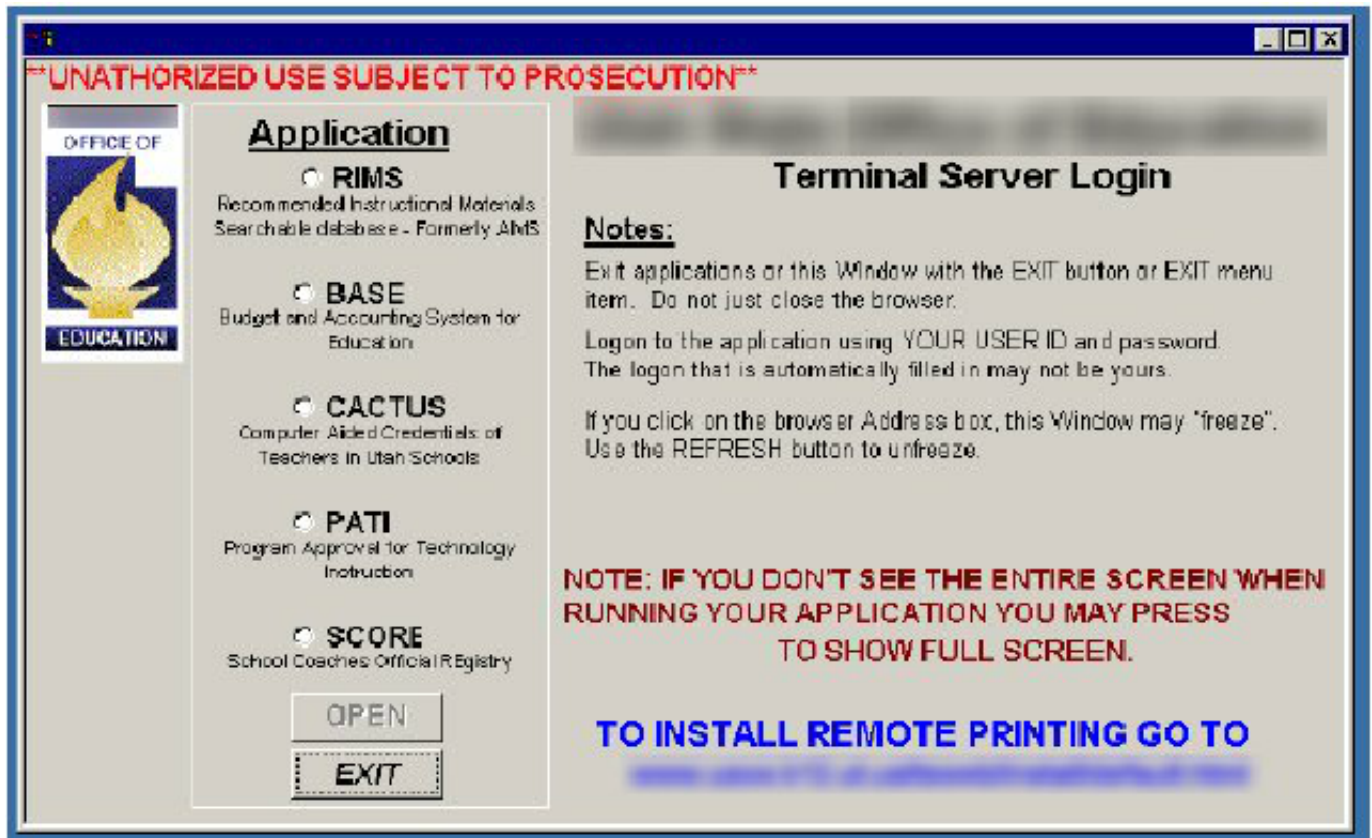
Kỹ thuật tìm kiếm với Google

- 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

