Google Hacking:
Tame the internet

Information Assurance Group 2011

What is Google Hacking?

- My Def:
  Using Google in a clever way to find things that shouldn't be found.

- Wikipedia:
  Gogle hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Advanced Search Operators

- OPERATOR:*KEYWORD*
- intitle / allintitle - in The title bar
- inurl / allinurl – in the URL
- link – pages that link to
- site - only that site
- filetype – only with a certain extension
- cache – only search cached copies of pages.

Logic Operators + Numbers

- ##..## - Number ranges ie. 1..1000
- * - Wild card **"I * cats"** = I love cats, I hate cats, I eat cats…
- AND OR NOT –
  - AND, is default, it tries to find both. TRIES.
  - OR , **I love (dogs OR cats)** , but not both. Use pipe symbol |
  - NOT , use a "minus sign" **I love pets –dogs** , all but dogs.
  - + , use a "plus sign" to force a word to be included.
  - ( ) , Use parentheses for grouping
  - " " , Use quotes for phrases

Getting Creative

- Can you think of a way to find social security numbers?
- 100000000..199999999
- What happens? Google knows you're up to no good.
- Try numrange:100000000-199999999 instead
- Suggest you are looking for social security numbers, add ssn
- Get rid of garbage using the NOT operator -123456789
- Specify only SQL Databases. filetype:sql

Using the GHDB

- Luckily, there is a database of Google Hacks to find all sorts of things.
- http://www.exploit-db.com/google-dorks/
- Vulnerable Servers / Files, Login Portals, Passwords, Errors, and more!
- Many older Hacks no longer return anything interesting.
- Why?

GHDB Demo 1

- DVR Login
  http://www.exploit-db.com/ghdb/1397/
- allintitle:"DVR Login"
- Filter out some garbage results by subtracting words
- -issue -failed -free -forum -download –youtube
- Click on some of the links.
- The Default login…. admin / admin , But wait!
- Lets talk legality….

Is it Legal?

- Is it Legal to type admin / admin to see if you can log in?
- What about if it didn't work?
- Is it legal to search for these things in google?
- Is it legal to click on the search results?

Office Cams

- http://www.exploit-db.com/ghdb/1008/

GHDB Demo 2

- http://www.exploit-db.com/ghdb/3612/
- Somewhere in the links is http://210.75.8.13/level/15/exec/-/clear/ip/igmp/group
- A Whois reveals it is in china somewhere.
- You can execute commands
- But don't.

GHDB Demo 3

- filetype:sql "phpmyAdmin SQL Dump"
- First site, sql database dump. Emails, logins, passwords..

Smarter Google Hacking

- It's fun to just find examples of errors through google,
- Say you want to focus on something specific.
- Start with site:specificsite.com
- Then systematically look for:
  error pages, different file types, login pages….

One More Thing.

- Way Back Machine
- Allows you to view web sites from the past.
- www.archive.org

- Try looking at IUP's website, in 1999? 2001?

END

Information Assurance Group 2011

"Build that Virtual Lab you always wanted"

Information Assurance Group 2011

If you didn't download yet ☹

- Windows:
  Get a Workstation Trial (Don't Install it yet)
  https://www.vmware.com/tryvmware/?p=workstation&lp=1

- Mac:
  Get a Fusion Trial (Don't Install it yet)
  https://www.vmware.com/tryvmware/?p=vmware-fusion31&lp=1

- Everyone

  Download the Windows XP Pro .iso file that I have hosted
  https://files.me.com/goetic/73y4d9

  Also Download the BackTrack5 R1 VM-Image
  http://www.backtrack-linux.org/ajax/download_redirect.php?id=BT5R1-GNOME-VM-32.7z

Steps

- Install VMWare
- Create New Virtual Machine
- Install Windows into that Virtual Machine
- Load BackTrack5 Virtual Machine
- Test

Install VMWare Product

- You should all know how to install software.
- Double Click the install file
- Use the serial key you got from registering, in your email?

Click to Create a New VM

- Continue without CD
- Disc Image File
- Find the SW CD Windows XP SP3 .iso file
- Default Settings are fine, when you start the virtual machine it will begin installing windows
- Enter -> F8 -> Enter -> (Quick Format)
- Windows is installing, this isn't quick

While we wait…

- What is virtualization?
- http://lmgtfy.com/?q=What+is+virtualization%3F&l=1
- 1 Laptop = Many Virtual Machines
- Your Laptop -> Host, Virtual Machines -> Guests
- No extra hardware cost
- Better than dual booting, you loose a lot of disc space, and can only use one at a time.

Ok

- Next Next Next… Blah Blah Blah
- Windows Serial Key? Uh-Oh
- Some versions of Windows Allow trial installs, this isn't one
- So I found a Serial Key on Youtube.
- First, Disable your Virtual Machine's Network Adapter
- Virtual Machine –> Network Adapter -> Disconnect
- QW4HD-DQCRG-HM64M-6GJRK-8K83T

Windows!

- First things first, Install VMWare Tools
- Virtual Machine -> Install VMWare Tools
- Next -> Next -> Next……
- Now you can Copy Paste Host to Guest and drag files across

SnapShots

- Virtual Machine -> Snapshots -> Take Snapshot

- Do this now, the License key we used is crap. If you connect to the internet it's probably going to deactivate.
- If you have a snapshot, you can always roll it back to a working state.
- You can take more snapshots later, and go back to any snapshot at any time.
- (new Snapshots don't overwrite the last one)

Network Adapters

- Host Only -> No Internet, Can communicate with your Host machine and other guest os's in Host Only Mode
- NAT -> Only good for getting on the internet, The host forwards requests to the guest, your router doesn't know the difference.
- Bridged -> The Guest pretends it is connected to the network physically. The router knows about it, and they share your network card through a virtual interface. But they have separate MAC's and IP addresses.
- Stick with Host-Only for now, to prevent windows from deactivating.

BackTrack5

- Linux Distribution with a Bunch of Security Tools already installed.
- What is BackTrack? LMGTFY?
- Backtrack file you downloaded, is Zipped I think. You should grab 7Zip to extract it, WinRAR might work too.
- Once it is extracted, you just need to open it in VMWare

VMWare Tools In Linux

- This is a pain, and I haven't tested it yet….
- Open up a terminal window:

  tar -zxvf VMwareTools*
  cd vmware-tools-distrib
  perl vmware-install.pl

  Select defaults, it will complain that it cannot find the linux C headers. Point the directory to /usr/src/linux/include. Everything should now compile properly.

Making a Trial Work for You

- You could purchase VMWare with an educational discount making it about 40$.
- Or you can just change your system's date back to when it was registered. This works on Windows and Mac for sure.
- Change Time, Start Virtual Machine, change time back.
- Note if you leave your date changed, you will have trouble browsing the web because all SSL Certificates will be invalid.

VMWare Player

- Or if you are using Windows, You can download VMWare Player.
- It is free
- You can open virtual machines
- but you can’t create new ones.

Information Assurance Group

09.06.11

Sign - In

- Sign In Sheet somewhere
- Put your Name
- and 4 character ID

US Cyber Challenge

- http://USCC.CyberQuests.org/
- Wireshark
- recognize WebApp Vulns
- Can win scholarships / invites to other events

Info Systems Security Association

- http://pittsburgh.issa.org
- **Tuesday September 13th.**
- $5 for students
- **Botnet's, Hacktivists, and High Technology Cyber Crime'.**
- Deadline for advance registration is September 9th,

IA Scholarship Program

- http://cio-nii.defense.gov/sites/iasp2/
- Must be 18
- GPA of 3.2 or Higher
- See Dr. Shumba if interested

Current Officers

- President: Joshua Schwartz
- Vice President: Christopher Gould
- Secretary: Carrie Este
- Web Contact Manager: Christopher Gould

- *Does anyone want to run, resign, or reconsider?*

Hacking Time!

- Start VMWare Workstation from Desktop
- File -> Open -> C:\IAVMS\
- There is a Windows XP SP3 VM
- And a BT5-GNOME-32 VM
- Open both and make sure network settings are set to “Host Only”

Login

- Windows
  - **ID: dude2**
  - **PW: dude2**
- BackTrack5
  - **ID: root**
  - **PW: toor**
  - Then type **startx**