

# Data Mining

## Tools Used by Hackers to Glean Protected Health Information (PHI) and How to Counter Them

Presented by Gordon Smith  
President and CEO  
**Canaudit, Inc.**

# Session Objectives

- Network Access
- Avoiding Detection
- Cataloging the Environment
- Targeting Sensitive Data
- Compromising Databases
- Breaching Firewalls

# Live Demonstrations

This presentation includes live demonstrations of:

- Targeting software and scanners
- Remote breach of the firewall (inside-out, outside-in exploit)
- Gaining Database Administrator (DBA) access to Oracle and Microsoft SQL databases
- Capturing and downloading Electronic Protected Health Information (ePHI)

# Network Access

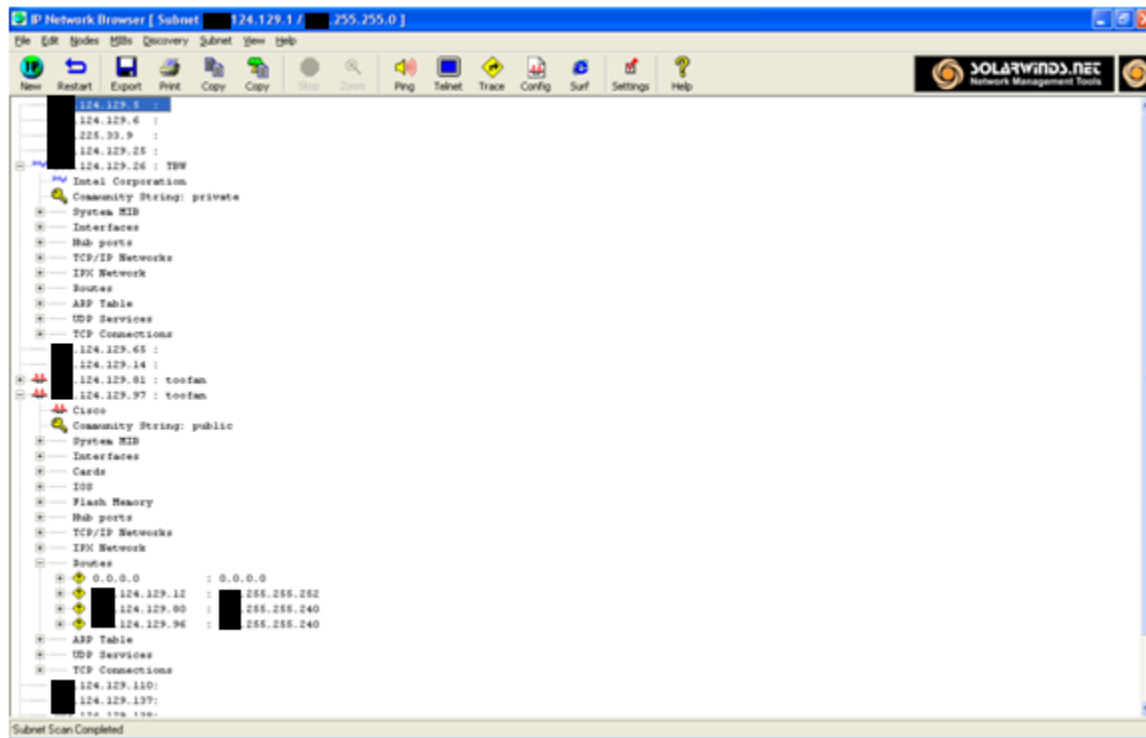
- Walk in, sit down, plug in
- Unencrypted and poorly protected wireless
- Compromising the virtual private network (VPN)
- Poorly secured associated practices and trading partners
- Poorly protected web mail and web applications

# Avoiding Detection

- Most organizations do not have an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) so there is nothing to avoid
- If IDS is present, use the Windows NetView command to document the Active Directory without setting off sensors
- If IPS is present, masquerade as a printer, VoIP, or video conferencing device

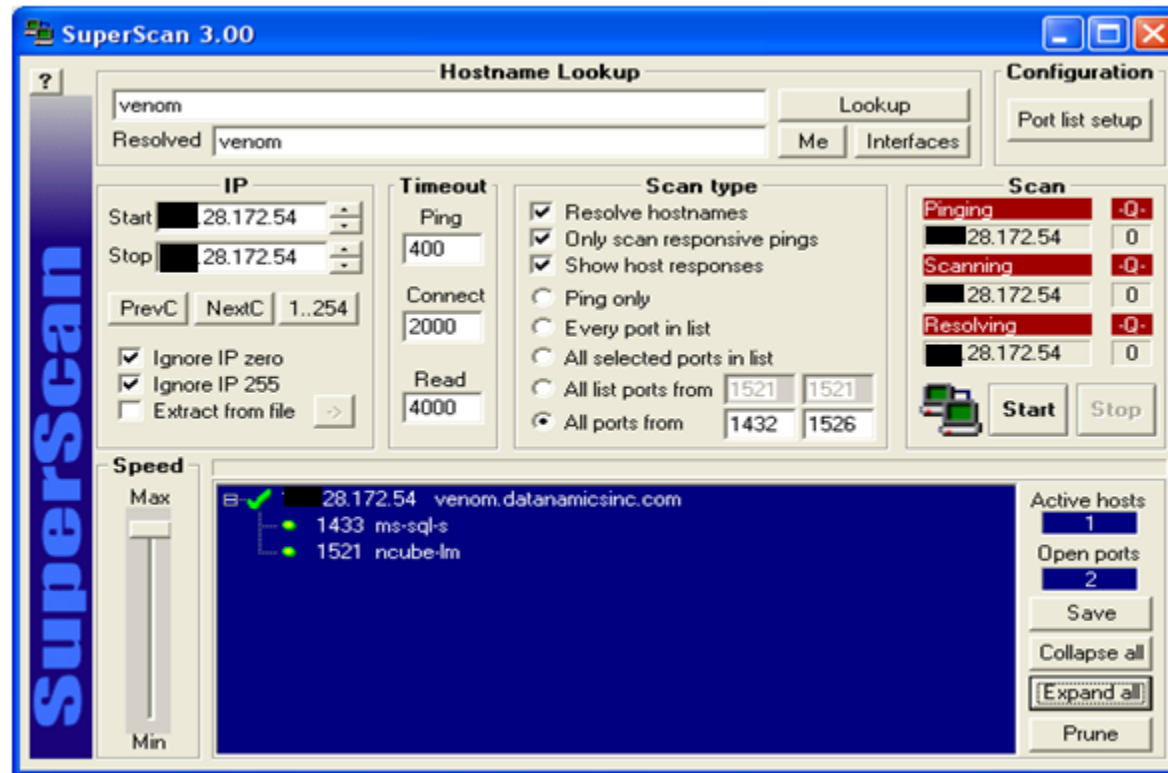
# Cataloguing the Environment

- Use non-invasive scanners such as SolarWinds IP Network Browser



# Search for Databases

- Use tools like SuperScan to catalogue the environment and to locate databases

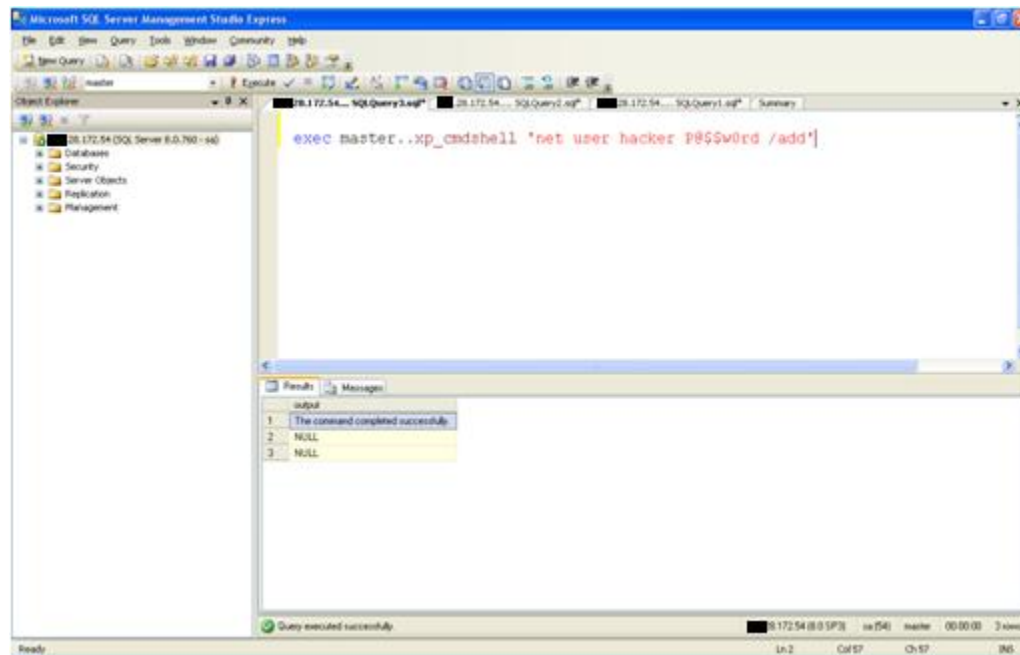


# Cataloguing Machines for “Harvesting”

- Check the scans for machine names that indicate the presence of sensitive data
  - Machines names are the hackers guide
  - Cerner, PSoft, McKesson, Pyxis, Lab, etc. are just a few
- Descriptive names help the hacker quickly identify targets

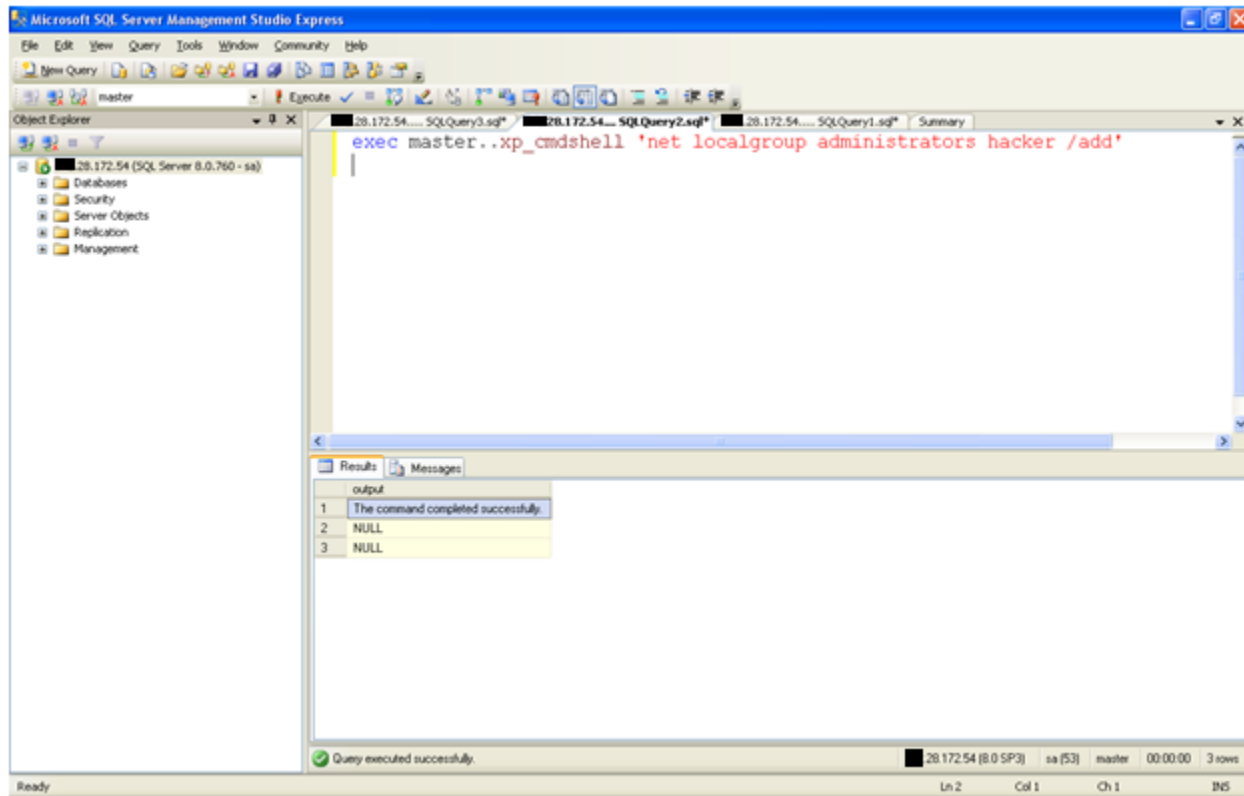
# Compromising Databases Microsoft SQL

- Live Demonstration
  - Adding an account to the machine hosting a compromised database



# Adding Admin Account to the Operating System

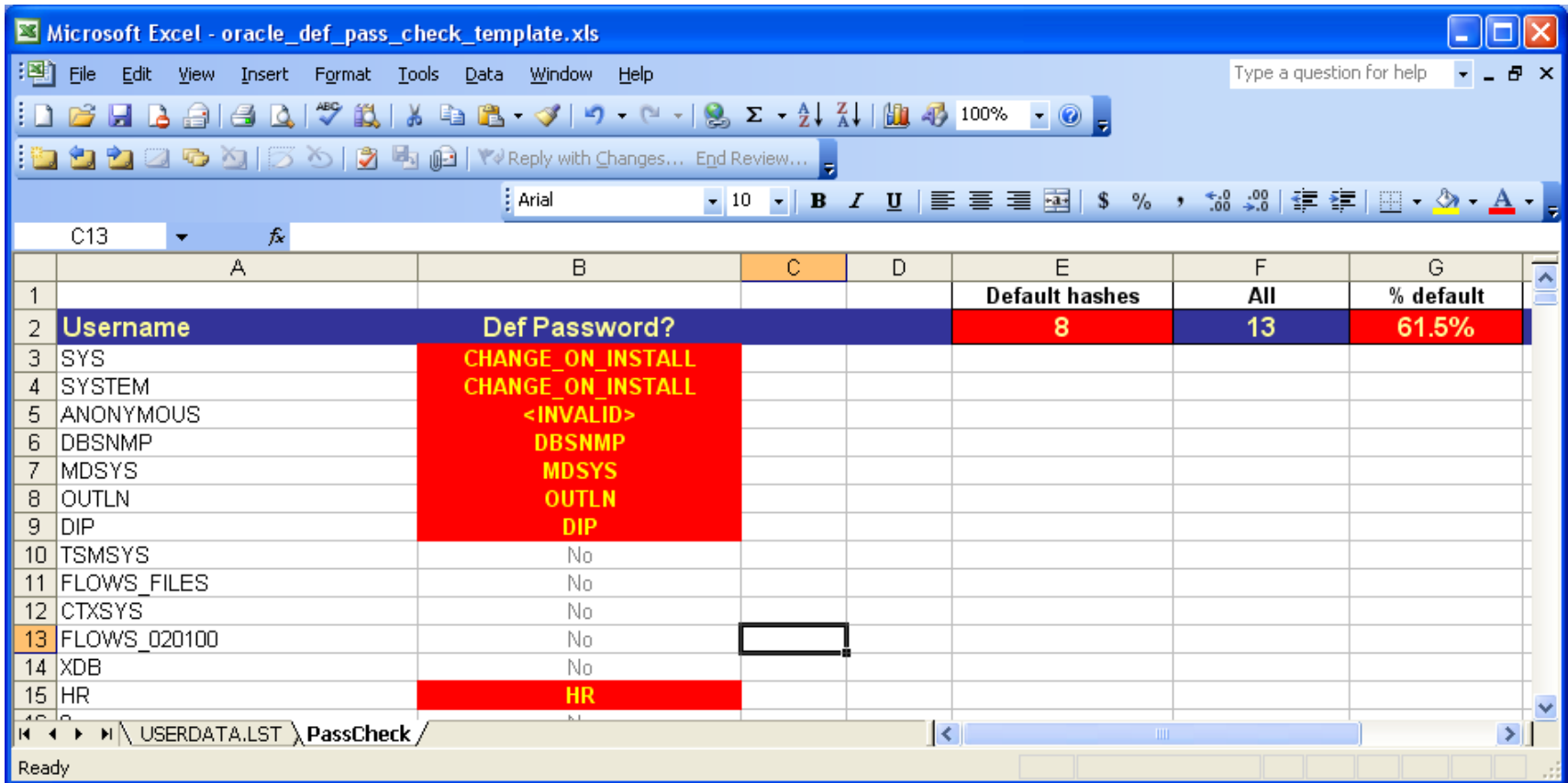
- Adding the account to the administrators group



# Compromising Oracle

- Live Demonstration
  - Notice how easy it is to gain Database Administrator (DBA) rights
  - Also notice the instantaneous password results

# Instant Gratification Oracle Password Cracker



The screenshot shows a Microsoft Excel spreadsheet titled "oracle\_def\_pass\_check\_template.xls". The spreadsheet has columns A through G. Row 1 contains headers: "Default hashes" in E, "All" in F, and "% default" in G. Row 2 contains "Username" in A, "Def Password?" in B, "8" in E, "13" in F, and "61.5%" in G. Rows 3-9 list Oracle users (SYS, SYSTEM, ANONYMOUS, DBSNMP, MDSYS, OUTLN, DIP) with their default passwords in column B, all highlighted in red. Row 10-12 show "No" in column B. Row 13 shows "No" in column B. Row 14 shows "No" in column B. Row 15 shows "HR" in column B, highlighted in red. The status bar at the bottom shows "Ready" and "PassCheck/".

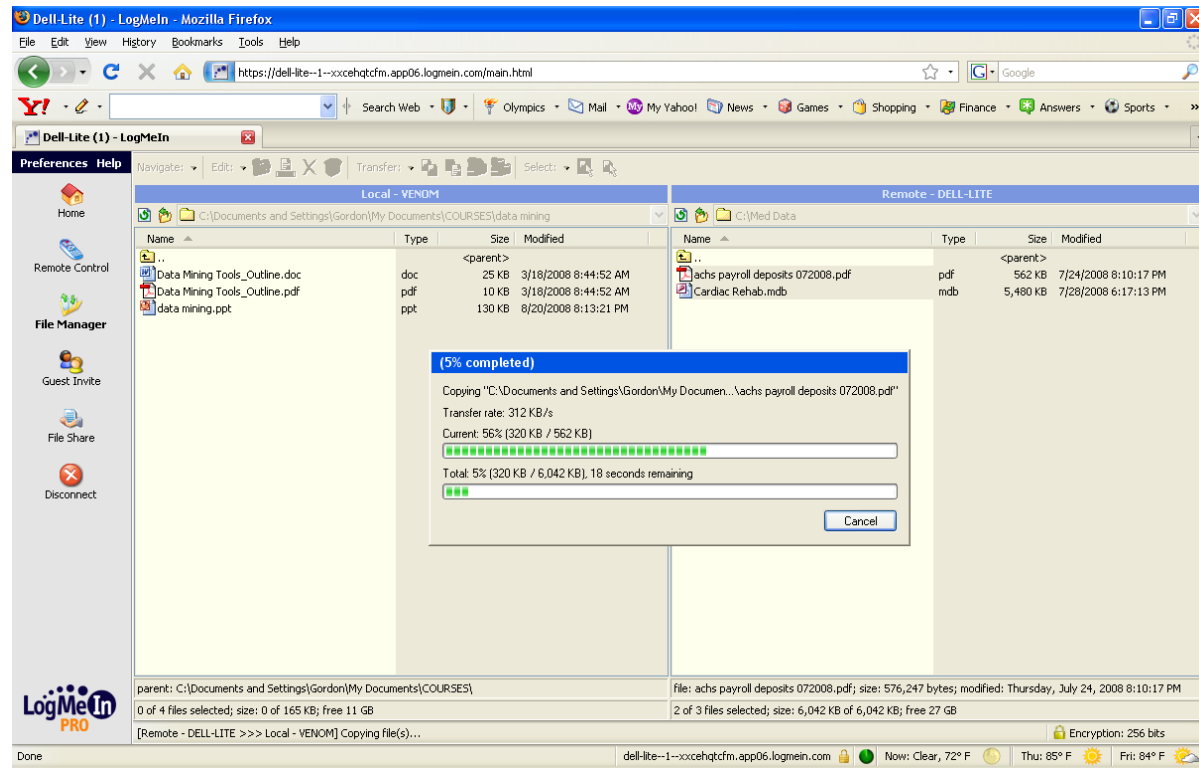
	A	B	C	D	E	F	G
1					Default hashes	All	% default
2	Username	Def Password?			8	13	61.5%
3	SYS	CHANGE_ON_INSTALL					
4	SYSTEM	CHANGE_ON_INSTALL					
5	ANONYMOUS	<INVALID>					
6	DBSNMP	DBSNMP					
7	MDSYS	MDSYS					
8	OUTLN	OUTLN					
9	DIP	DIP					
10	TSMSYS	No					
11	FLows_FILES	No					
12	CTXSYS	No					
13	FLows_020100	No					
14	XDB	No					
15	HR	HR					

# Targeting Sensitive Data

- Several methods to target sensitive data
  - Go for the database exports
    - World readable and can be easily copied
    - Large but easily copied over a high-speed network
  - Take critical files and databases
    - Cerner, etc.
    - Load them into Oracle Personal Edition

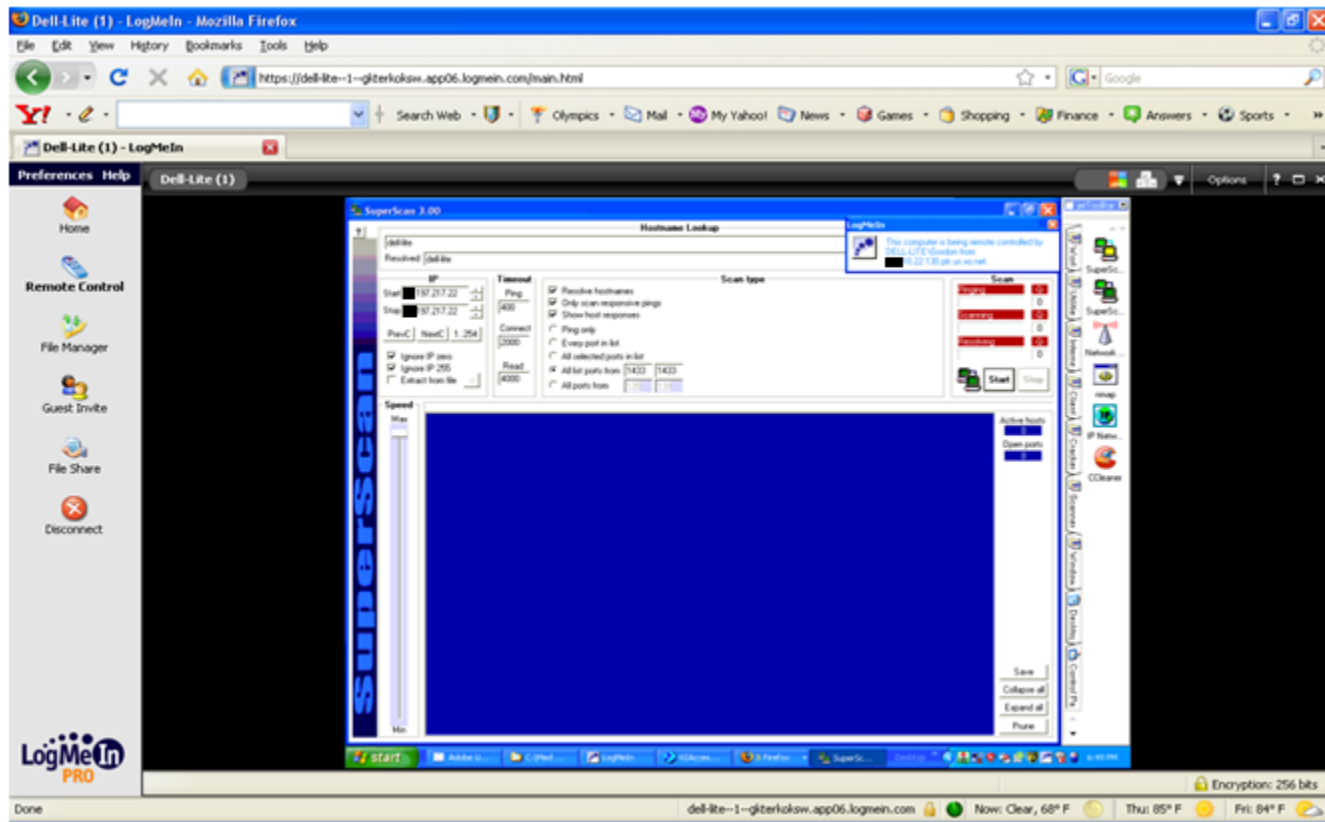
# Harvesting Sensitive Information

- Notice how easy it is to take medical records



# Breaking Through Firewall

- LogMeIn demonstration (example below)



# End of Presentation