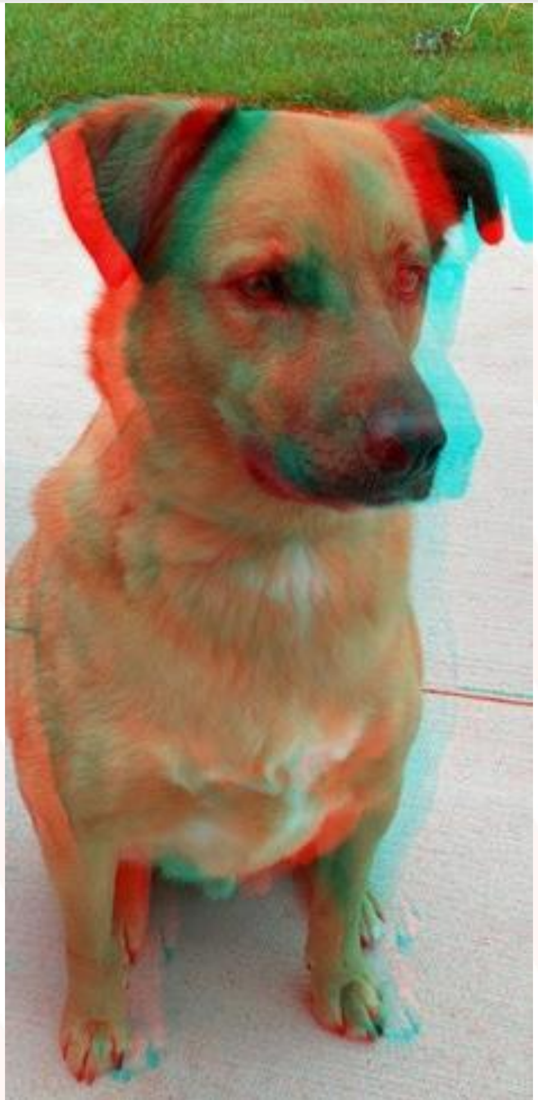
HIGH POINT
NETWORKS™

Getting Started with OSINT

Jamie Maguire

About Me

- Started on helpdesk, then network administration, then vulnerability management
- Senior Security Engineer at High Point Networks
- Focus on penetration testing and vulnerability assessments



Agenda

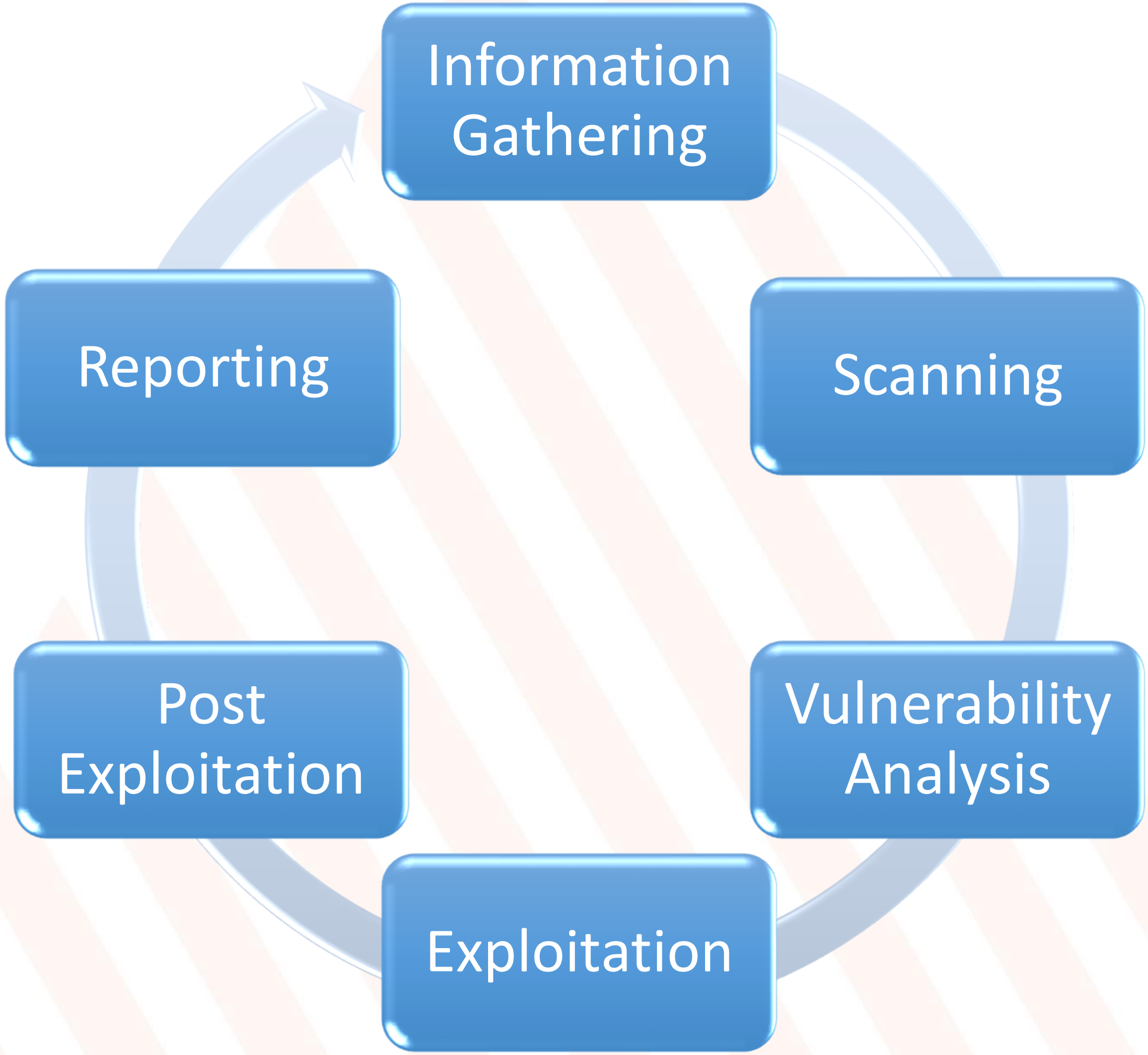
- Discuss OSINT
- See a few examples
- Discuss Recon-ng
- Recon-ng example

What this talk is and is not

- Everything today is passive Information Gathering
- This is not a complete guide for Information Gathering
- There's nothing here that has not been done before

Why does this matter?

- 1st phase of a penetration test
- Project scope

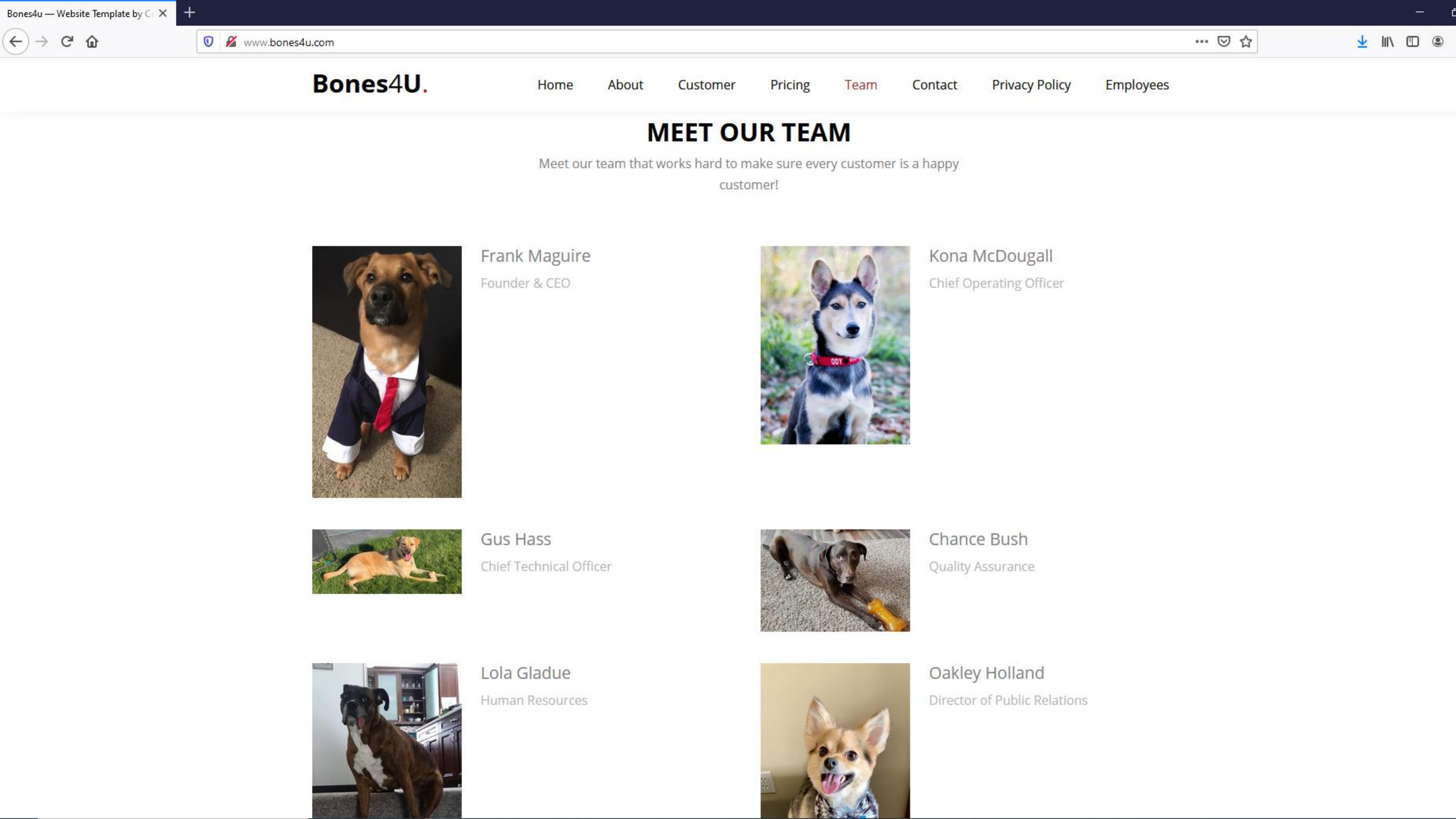


What information would we like?

- Names -> email addresses and usernames
- Internet Facing Hosts -> open ports
- Compromised Passwords -> Credential Stuffing

Where do we get information?

- The targets website
- LinkedIn
- Job Postings
- Search Engines (Shodan, Google, Bing)
- Documents such as PDF’s, spreadsheets or word documents
- Data Breaches



MEET OUR TEAM

Meet our team that works hard to make sure every customer is a happy customer!

Frank Maguire
Founder & CEO

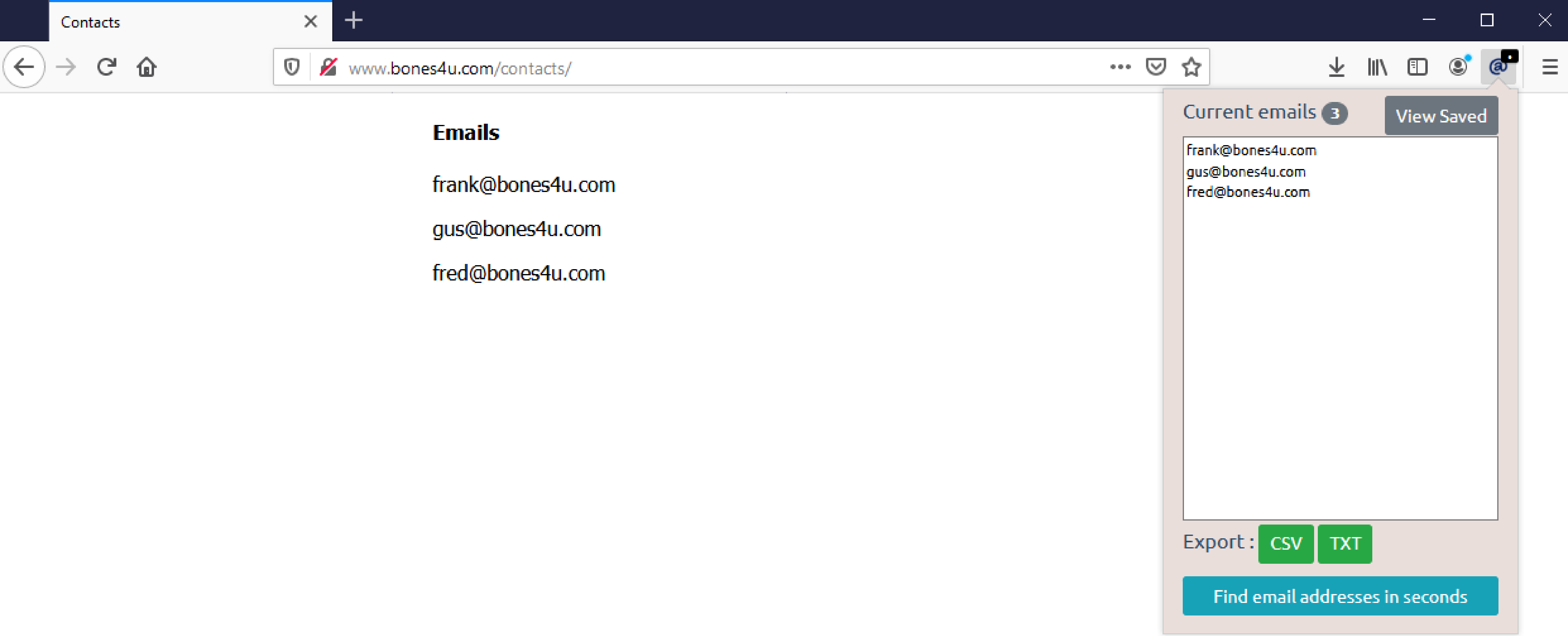
Kona McDougall
Chief Operating Officer

Gus Hass
Chief Technical Officer

Chance Bush
Quality Assurance

Lola Gladue
Human Resources

Oakley Holland
Director of Public Relations



Emails

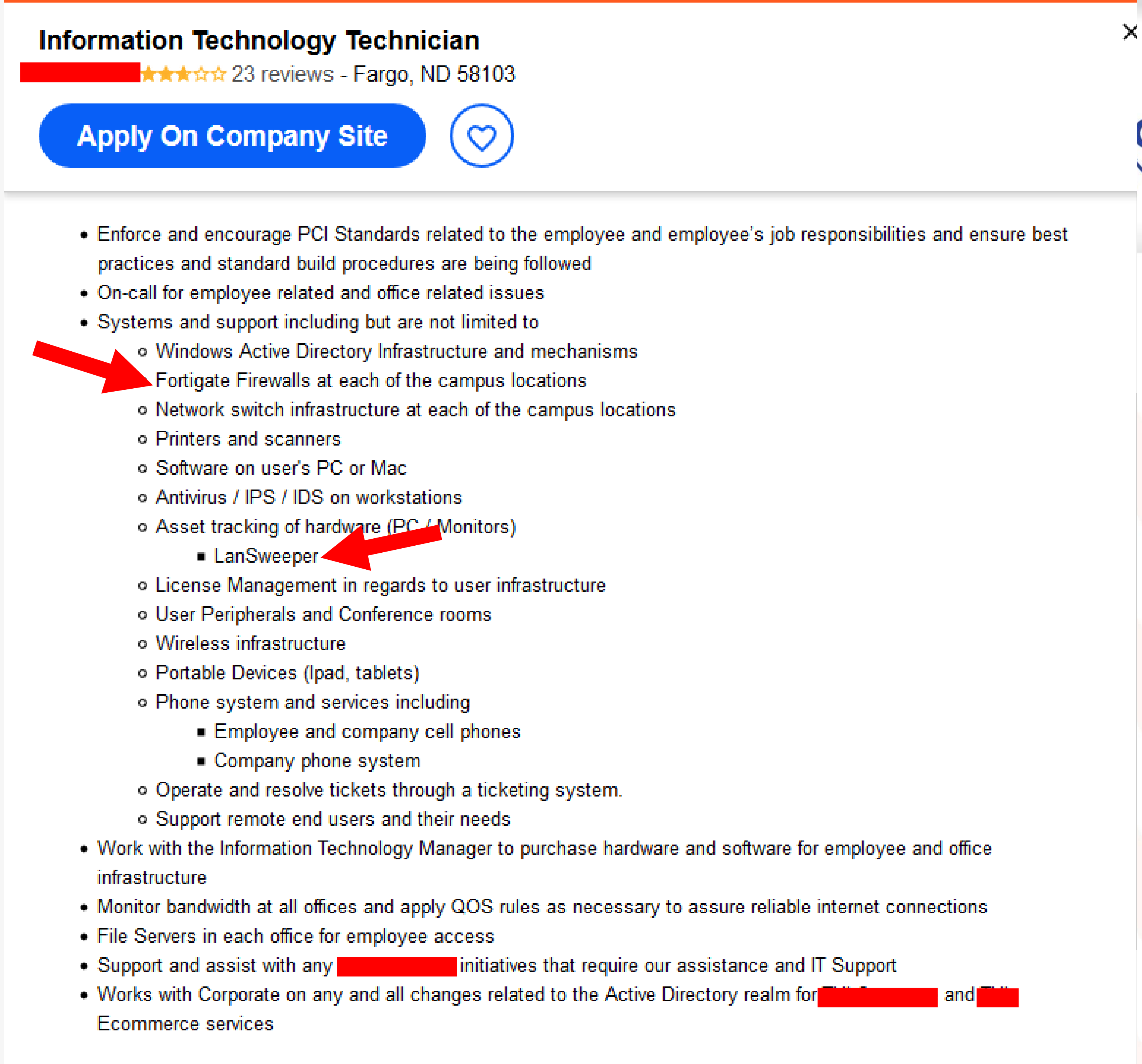
frank@bones4u.com

gus@bones4u.com

fred@bones4u.com

```
frank@bones4u.com
gus@bones4u.com
fred@bones4u.com
```

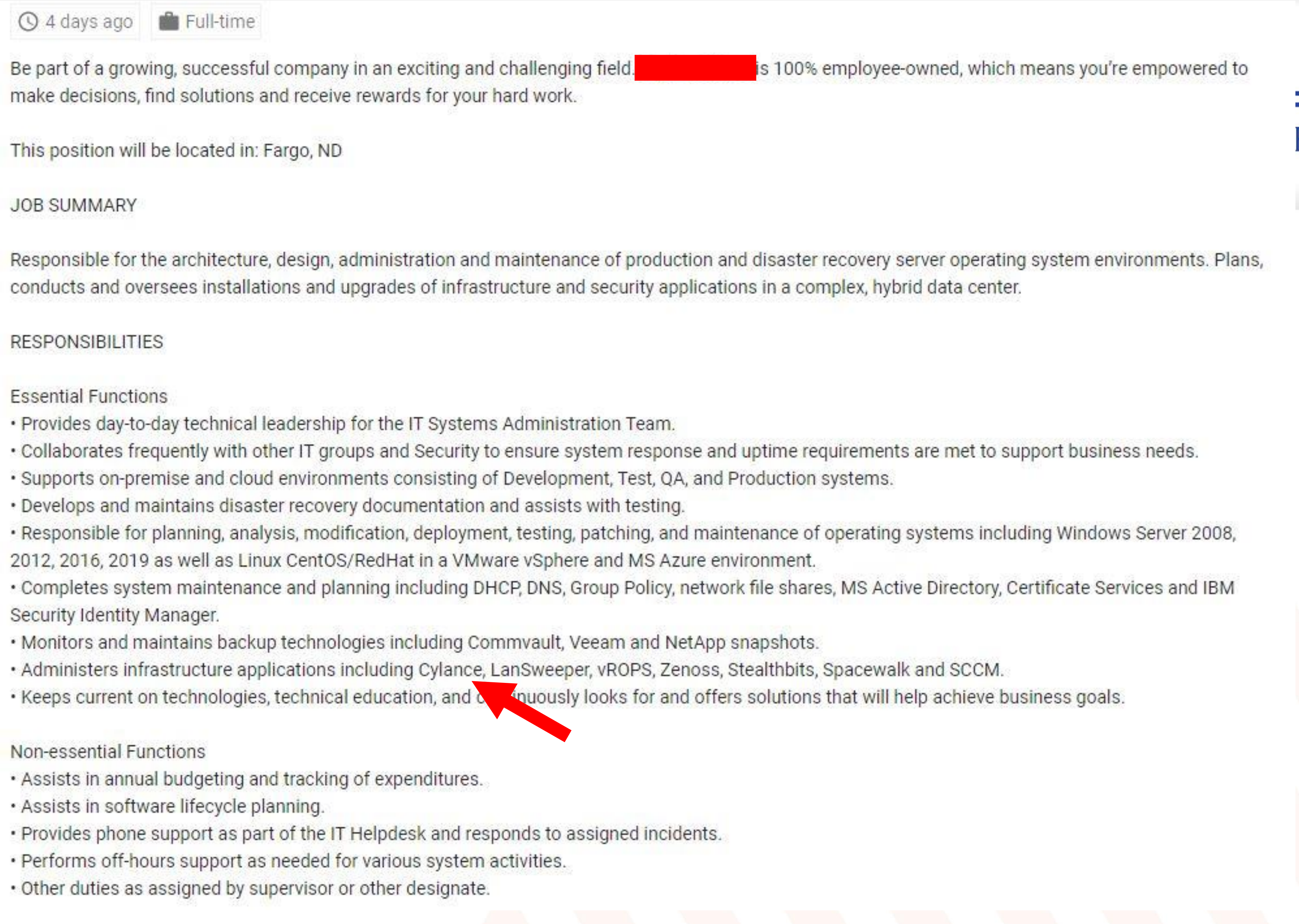
- Email Extractor browser extension



Information Technology Technician

[redacted] ★★★☆☆ 23 reviews - Fargo, ND 58103

- Enforce and encourage PCI Standards related to the employee and employee's job responsibilities and ensure best practices and standard build procedures are being followed
- On-call for employee related and office related issues
- Systems and support including but are not limited to
    - Windows Active Directory Infrastructure and mechanisms
    - Fortigate Firewalls at each of the campus locations
    - Network switch infrastructure at each of the campus locations
    - Printers and scanners
    - Software on user's PC or Mac
    - Antivirus / IPS / IDS on workstations
    - Asset tracking of hardware (PC / Monitors)
        - LanSweeper
    - License Management in regards to user infrastructure
    - User Peripherals and Conference rooms
    - Wireless infrastructure
    - Portable Devices (Ipad, tablets)
    - Phone system and services including
        - Employee and company cell phones
        - Company phone system
    - Operate and resolve tickets through a ticketing system.
    - Support remote end users and their needs
- Work with the Information Technology Manager to purchase hardware and software for employee and office infrastructure
- Monitor bandwidth at all offices and apply QOS rules as necessary to assure reliable internet connections
- File Servers in each office for employee access
- Support and assist with any [redacted] initiatives that require our assistance and IT Support
- Works with Corporate on any and all changes related to the Active Directory realm for [redacted] and [redacted] Ecommerce services



4 days ago | Full-time

Be part of a growing, successful company in an exciting and challenging field. [redacted] is 100% employee-owned, which means you're empowered to make decisions, find solutions and receive rewards for your hard work.

This position will be located in: Fargo, ND

JOB SUMMARY

Responsible for the architecture, design, administration and maintenance of production and disaster recovery server operating system environments. Plans, conducts and oversees installations and upgrades of infrastructure and security applications in a complex, hybrid data center.

RESPONSIBILITIES

Essential Functions

- Provides day-to-day technical leadership for the IT Systems Administration Team.
- Collaborates frequently with other IT groups and Security to ensure system response and uptime requirements are met to support business needs.
- Supports on-premise and cloud environments consisting of Development, Test, QA, and Production systems.
- Develops and maintains disaster recovery documentation and assists with testing.
- Responsible for planning, analysis, modification, deployment, testing, patching, and maintenance of operating systems including Windows Server 2008, 2012, 2016, 2019 as well as Linux CentOS/RedHat in a VMware vSphere and MS Azure environment.
- Completes system maintenance and planning including DHCP, DNS, Group Policy, network file shares, MS Active Directory, Certificate Services and IBM Security Identity Manager.
- Monitors and maintains backup technologies including Commvault, Veeam and NetApp snapshots.
- Administers infrastructure applications including Cylance, LanSweeper, vROPS, Zenoss, Stealthbits, Spacewalk and SCCM.
- Keeps current on technologies, technical education, and continuously looks for and offers solutions that will help achieve business goals.

Non-essential Functions

- Assists in annual budgeting and tracking of expenditures.
- Assists in software lifecycle planning.
- Provides phone support as part of the IT Helpdesk and responds to assigned incidents.
- Performs off-hours support as needed for various system activities.
- Other duties as assigned by supervisor or other designate.

theHarvester

- A simple script for gathering hostnames and emails based on a given Domain.

- https://github.com/laramies/theHarvester

- theHarvester usage:
  - ./theHarvester.py –d *example.com* –b *datasources* -f *outfile-name*

Document Metadata and Google Dorks

- We can analyze document metadata to discover usernames
- Gather documents using google dorks
- Analyze documents with something like Exiftool

- Site:<company.com> password
- Site:<company.com> filetype:xlsx
- Site:<company.com> filetype:pdf
- Site:<company.com> filetype:docx
- Google Hacking Databases:
  - http://www.exploit-db.com/google-dorks/
  - http://www.hackersforcharity.org/ghdb

FOCA

- Foca searches the internet for files on a given domains
- Foca can download and extract metadata for a large amount of files quickly
- https://github.com/ElevenPaths/FOCA
- Windows only

Databreaches

- Attackers use exposed passwords to conduct credential stuffing attacks
- Haveibeenpwned: requires API key to use with Recon-ng $3/month
- BreachCompilation: https://gist.github.com/scottlinux/9a3b11257ac575e4f71de811322ce6b3

Live Examples

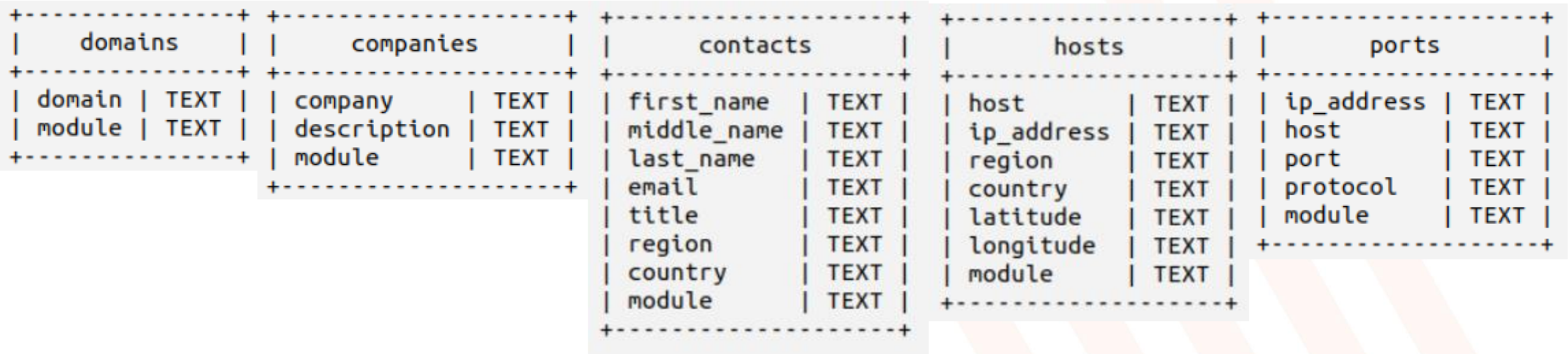
Bringing it together with Recon-NG

- *Open Source Intelligence gathering tool aimed at reducing the time spent harvesting information from open sources.*
- https://github.com/lanmaster53/recon-ng
- Menu driven, similar look to Metasploit or SET
- Allows us to export reports of the information we gather

Version 4 vs. Version 5

- Version 5 of Recon-ng is a major overhaul, commands have changed.
- No modules are preinstalled
- Kali Linux 2020.1 ships with version 5
- https://www.blackhillsinfosec.com/whats-changed-in-recon-ng-5x/

Recon-NG tables



```
+---------------+
|    domains    |
+---------------+
| domain | TEXT |
| module | TEXT |
+---------------+
```

```
+--------------------+
|     companies      |
+--------------------+
| company     | TEXT |
| description | TEXT |
| module      | TEXT |
+--------------------+
```

```
+--------------------+
|      contacts      |
+--------------------+
| first_name  | TEXT |
| middle_name | TEXT |
| last_name   | TEXT |
| email       | TEXT |
| title       | TEXT |
| region      | TEXT |
| country     | TEXT |
| module      | TEXT |
+--------------------+
```

```
+-------------------+
|       hosts       |
+-------------------+
| host       | TEXT |
| ip_address | TEXT |
| region     | TEXT |
| country    | TEXT |
| latitude   | TEXT |
| longitude  | TEXT |
| module     | TEXT |
+-------------------+
```

```
+-------------------+
|       ports       |
+-------------------+
| ip_address | TEXT |
| host       | TEXT |
| port       | TEXT |
| protocol   | TEXT |
| module     | TEXT |
+-------------------+
```

Recon-NG modules

- Import/list, import/csv
- Recon/domains-contacts/bing_linkedin_cache*
- Recon/contacts-contacts/mangle
- Recon/domains-hosts/hackertarget
- Recon/domains-hosts/certificate_transparency
- Recon/domains-hosts/brute_hosts
- Recon/domains-hosts/binaryedge*
- Recon/domains-hosts/ipinfodb*
- Recon/hosts-ports/binaryedge*
- Recon/hosts-ports/shodan_ip*

* Requires API key

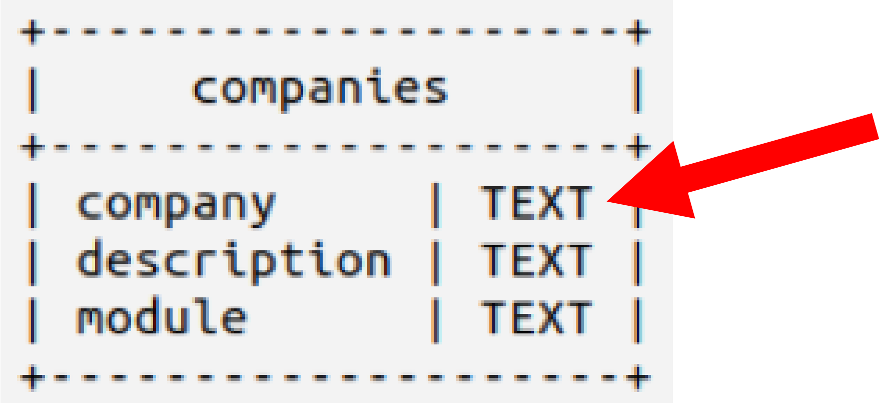
Recon-NG modules

Populate this table

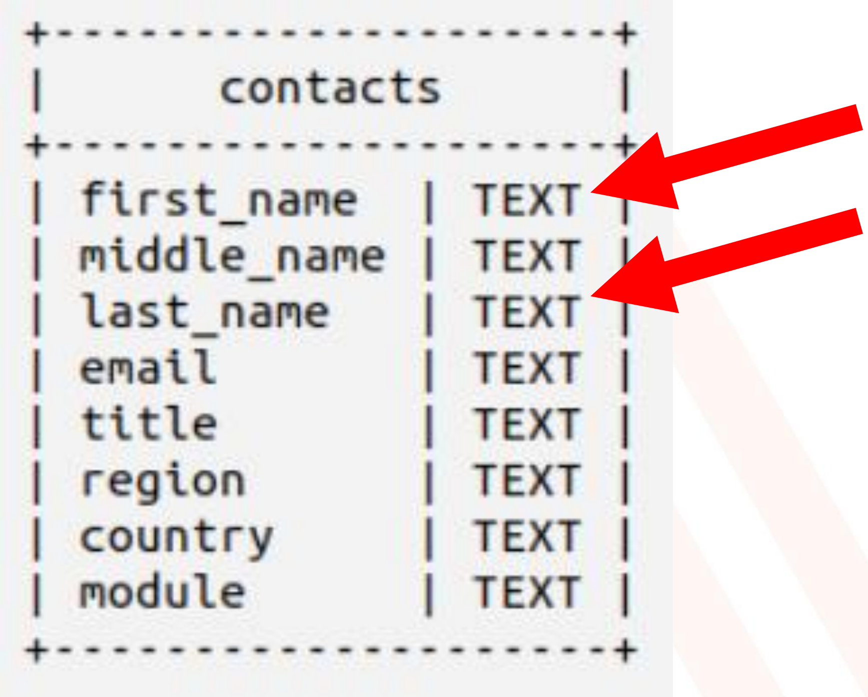
- Recon/companies-contacts/bing_linkedin_cache

Read from this table

companies-contacts/bing_linkedin_cache



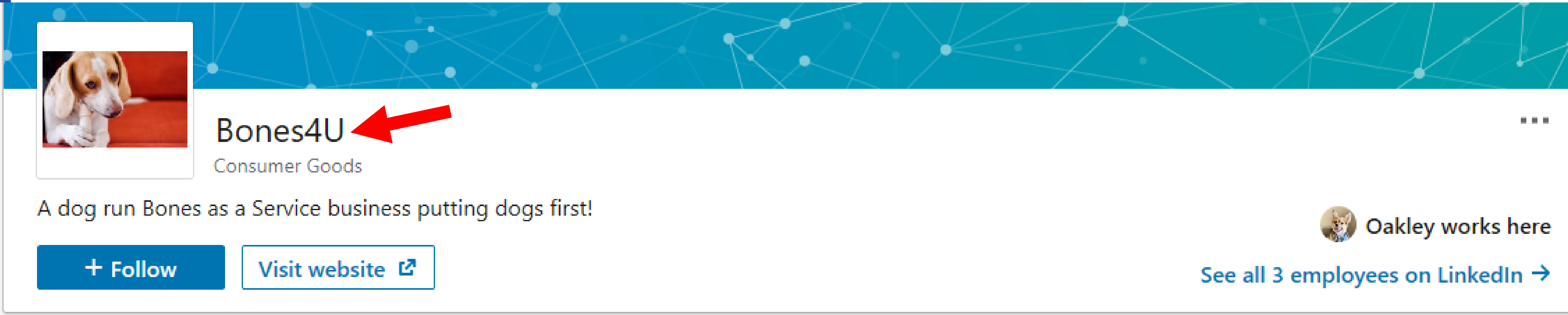
```
+--------------------+
|     companies      |
+--------------------+
| company     | TEXT |
| description | TEXT |
| module      | TEXT |
+--------------------+
```



```
+---------------------+
|      contacts       |
+---------------------+
| first_name   | TEXT |
| middle_name  | TEXT |
| last_name    | TEXT |
| email        | TEXT |
| title        | TEXT |
| region       | TEXT |
| country      | TEXT |
| module       | TEXT |
+---------------------+
```

Bing Search Module

- API Key: https://azure.microsoft.com/en-us/pricing/details/cognitive-services/search-api/
- Free for up to 1000 searches per month



Bones4U

Consumer Goods

A dog run Bones as a Service business putting dogs first!

Ipinfodb api

- Ipinfodb is a free service that allows you to geolocate IP addresses

- Sign up for a free API key at https://ipinfodb.com/api

- 1 request every 2 seconds

Shodan

- Shodan scans the internet and allows users to query the results
- Premium account is required for API access, usually $50 for life often on sale blackfriday/cybermonday
- Students receive free premium with .edu registration
- https://www.shodan.io/

Binary Edge

- Binary Edge scans the internet and allows users to query the results
- Free plan allows 250 queries/month
- $10 per month allows 5000 queries/month
- https://www.binaryedge.io/

Recon-ng Demo

End

- Thank you for attending!
- Try out Recon-ng for yourself
- Bones4u.com is available for testing