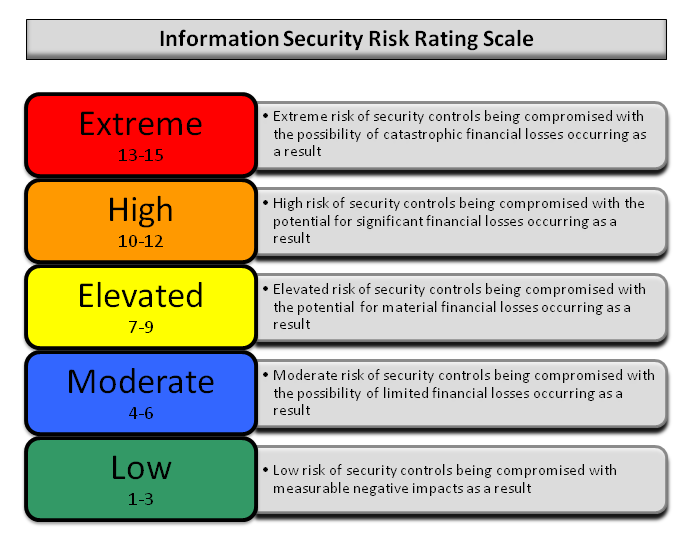
**The Executive Summary**

**Background:**

Vantage Credit Union tasked KNewman with performing an internal/external vulnerability assessment and penetration testing of specific systems located in our headquarters. These systems have been identified as moderate risk level and contain as high data which, if accessed inappropriately, could cause material harm to Vantage Credit Union. In an effort to test Vantages ability to defend against direct and indirect attack, KNewman compiled an intel on the client’s systems and employees. KNewman also ran a vulnerability assessment. The purpose of this assessment was to verify the effectiveness of the security controls put in place by Vantage Credit Union to secure business-critical information. This report represents the findings from the assessment and the associated remediation recommendations to help Vantage credit union strengthen its security posture.

**Risk Ranking/Profile:**

The overall risk ranking/profile/score will be identified and explained in this area.

[](http://www.pentest-standard.org/index.php/File:Reporting-risk-scale.png)

The overall risk for vantage risk score for Vantage credit union is currently a four (4). This rating implies a moderate risk of security controls being compromised with the possibility of limited financial losses occurring as a result.

**Technical Report**

**Introduction:**

* Only CEO and upper management are aware of the test. The only person from the pen testing team involved is Pen tester KNewman.
* Contact information:
  + Pen testers Information: (314)-337-7114
  + Point of contact @ Vantage Credit Union
* Objectives of Test: The client indicated that their objective in performing this engagement was to improve the security of the external facing services that they provide. The testing that was conducted should focus on identifying attack vectors in addition to the vulnerabilities and risks these attack vectors may expose.
* Scope of Test: 5 weeks.
* Strength of Test: The strength of the test is medium because there wasn’t an exploration or post exploitation stage included.
* Approach: Conducted the test as Black Hat Test. Declined to receive any insider information from the client. Pen tester wanted the test to be as close to a real life scenario as possible.

**Information Gathering:**

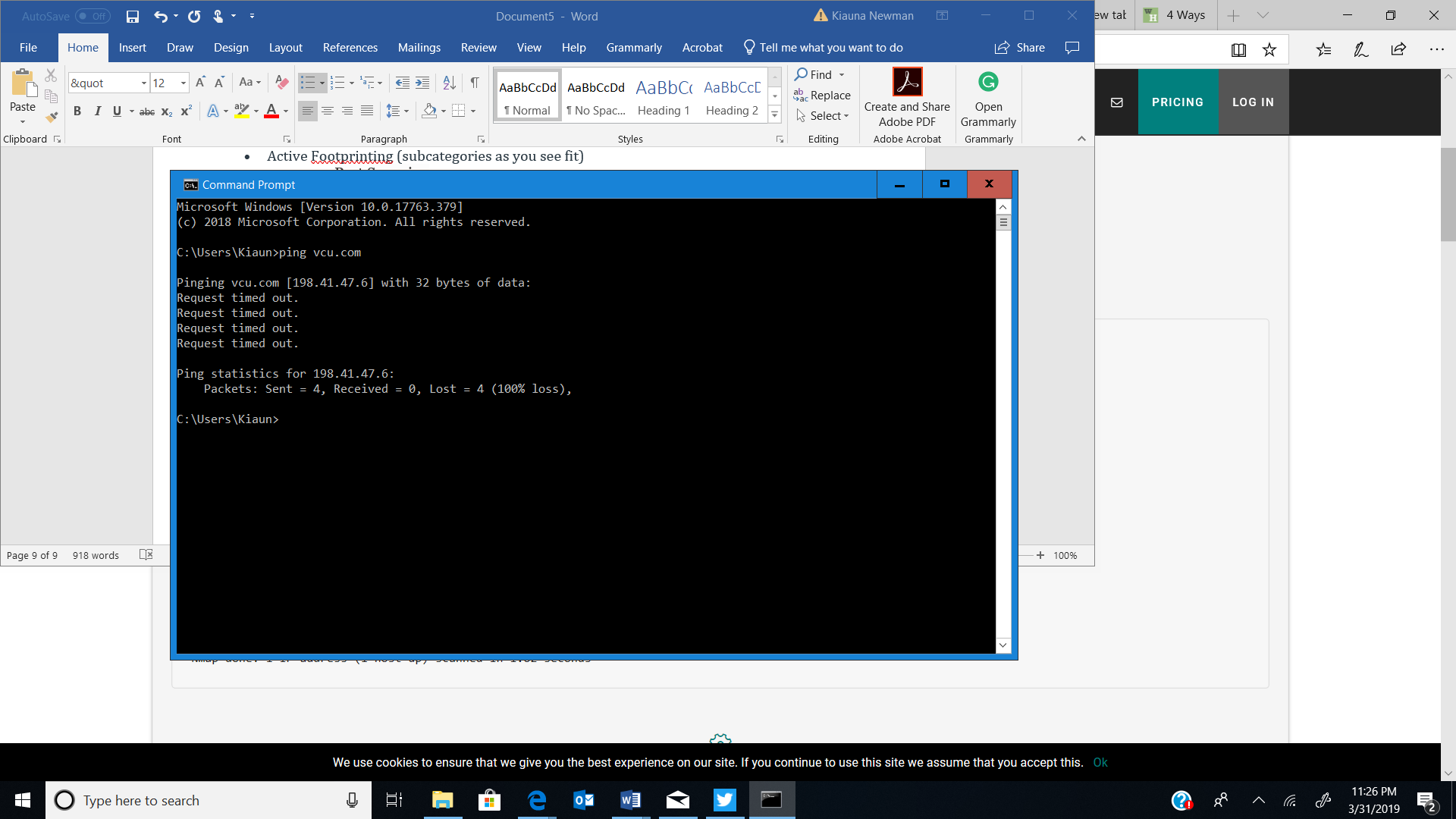
Information available to the general public.

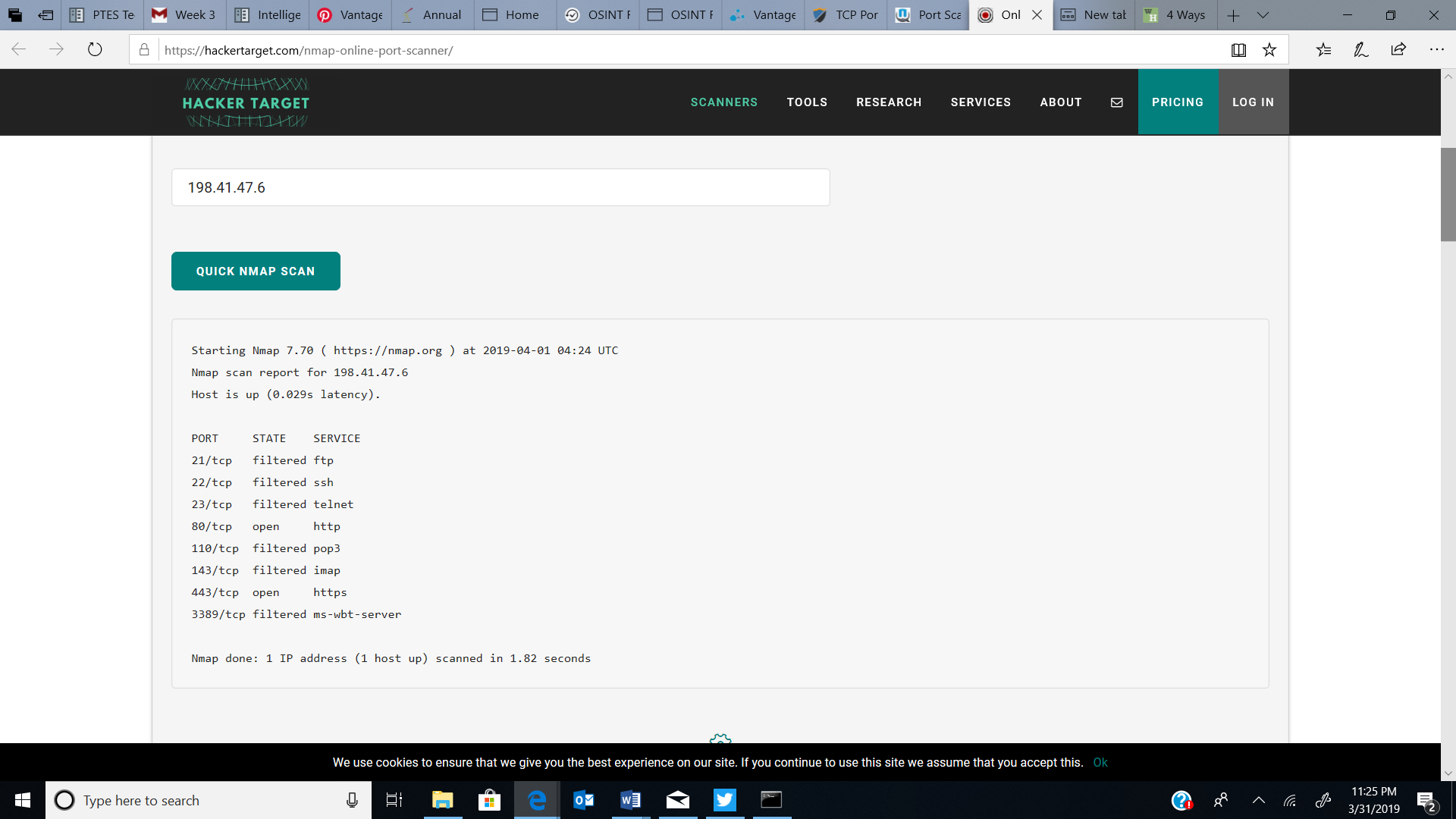
* Corporate
  + Locations
    - Headquarters: 4020 Fee Fee Road Bridgeton, MO. 63044 4
  + Branches:
    - 4020 Fee Fee Rd Bridgeton, MO 63044
    - 1330 YMCA Dr Festus, MO 63028
    - PO Box 4433 Bridgeton, MO 63044
    - 332 Festus Centre Dr Festus, MO 63028
    - 13 Collinsville Ave East Saint Louis, IL 62201
    - 16260 Truman Rd Ballwin, MO 63011
    - 1077 Cave Springs Blvd Saint Peters, MO 63376
    - 11654 W Florissant Ave Florissant, MO 63033
  + Businesses near Vantage Headquarters:
    - Certified Power Solutions
    - Extended Stay America
    - Embassy Suites
    - Ergonomic Partners
    - Certified Power Solutions
    - Credit Union Insurance Agency
    - Mortgage Solutions,
    - Vantage investment Services Group
  + Timezone: Central U.S. Zone
  + Hosts/NOC

**Passive Intelligence:**

* + **WHOIS Lookups**[¶](https://pentest-standard.readthedocs.io/en/latest/intelligence_gathering.html#whois-lookups)
    - Domain Name: VCU.COM
    - Registry Domain ID: 2582620\_DOMAIN\_COM-VRSN
    - Registrar WHOIS Server: whois.networksolutions.com
    - Registrar URL: http://networksolutions.com
    - Updated Date: 2018-12-14T16:29:16Z
    - Creation Date: 1998-11-30T05:00:00Z
    - Registrar Registration Expiration Date: 2020-11-29T05:00:00Z
    - Registrar: NETWORK SOLUTIONS, LLC.
    - Registrar IANA ID: 2
    - Reseller:
    - Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
    - Registry Registrant ID:
    - Registrant Name: Vantage Credit Union
    - Registrant Organization: Vantage Credit Union
    - Registrant Street: 4020 FEE FEE RD
    - Registrant City: BRIDGETON
    - Registrant State/Province: MO
    - Registrant Postal Code: 63044-2708
    - Registrant Country: US
    - Registrant Phone: +1.3142645400
    - Registrant Phone Ext:
    - Registrant Fax: +1.231231234
    - Registrant Fax Ext:
    - Registrant Email: techops@vcu.com
    - Registry Admin ID:
    - Admin Name: Support, DCIT
    - Admin Organization: VCU
    - Admin Street: 4020 Fee Fee Rd
    - Admin City: Bridgeton
    - Admin State/Province: MO
    - Admin Postal Code: 63044-2708
    - Admin Country: US
    - Admin Phone: +1.3142645400
    - Admin Phone Ext:
    - Admin Fax:
    - Admin Fax Ext:
    - Admin Email: techops@vcu.com
    - Registry Tech ID:
    - Tech Name: Support, DCIT
    - Tech Organization: VCU
    - Tech Street: 4020 Fee Fee Rd
    - Tech City: Bridgeton
    - Tech State/Province: MO
    - Tech Postal Code: 63044-2708
    - Tech Country: US
    - Tech Phone: +1.3142645400
    - Tech Phone Ext:
    - Tech Fax:
    - Tech Fax Ext:
    - Tech Email: techops@vcu.com
    - Name Server: NS4.P23.DYNECT.NET
    - Name Server: NS3.P23.DYNECT.NET
    - Name Server: NS2.P23.DYNECT.NET
    - Name Server: NS1.P23.DYNECT.NET
    - DNSSEC: unsigned
    - Registrar Abuse Contact Email: abuse@web.com
    - Registrar Abuse Contact Phone: +1.8003337680

**Active Intelligence:**





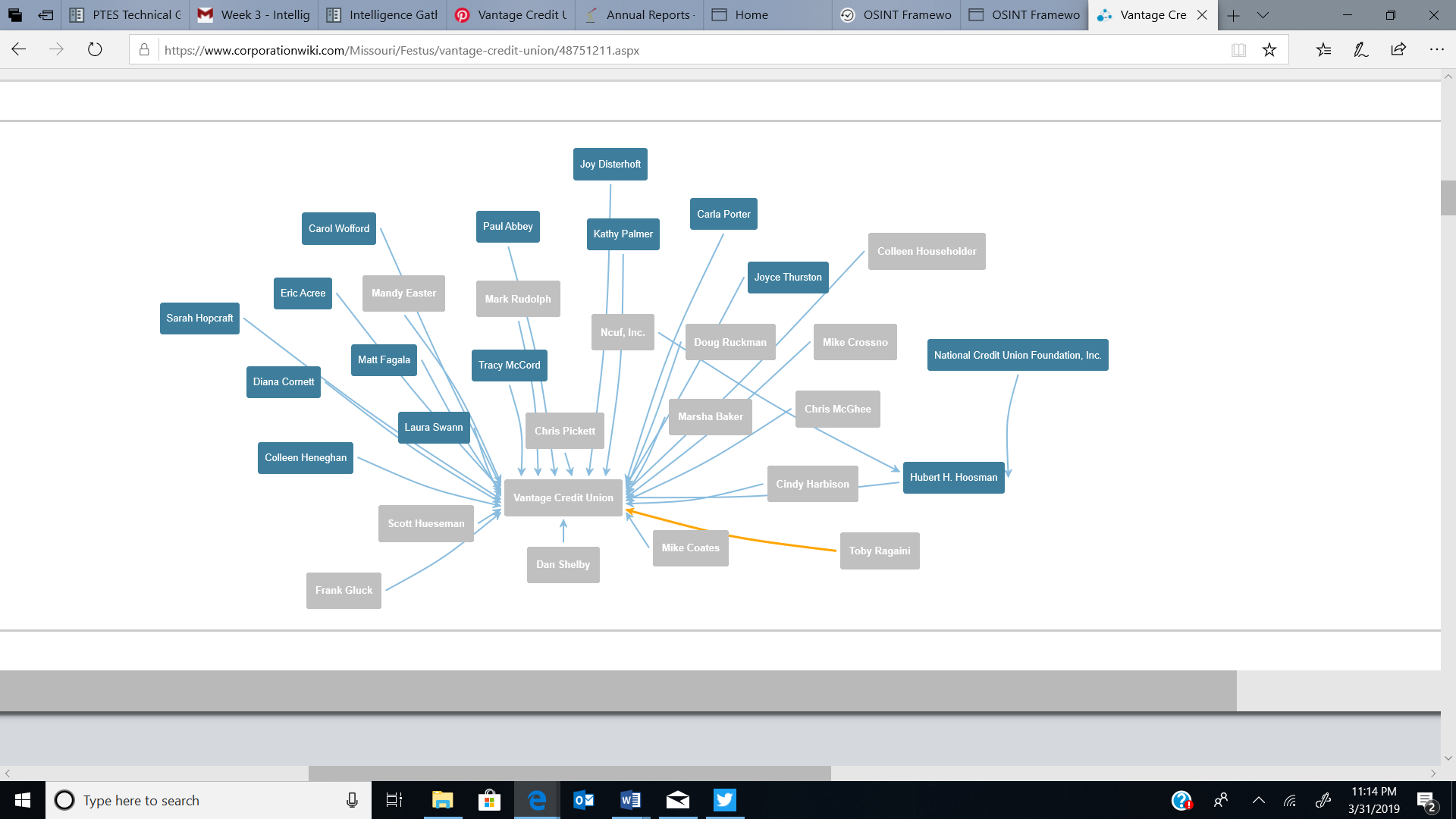
**Corporate Intelligence:**

* + Land/Tax Records:
    - Charter Number: 67804
    - Parcel Number: 12M530515
    - Locator Number 12M530515
    - Built in 1984, this property features 5.47 acres lot, and 0.97 acres lot space
    - Central Heat and Air
* Affiliations:
  + Northwest chamber of commerce
  + Chesterfield Chamber of Conference
* Business Partners:
  + Turbo Tax
  + Enterprise Rent A Car Six Flags
  + Members Resource, LLC,
  + Credit Union Insurance Agency (CUIA), LLC,
  + Mortgage Solutions, LLC,
* Competitors:
  + 1st Financial Credit Union,

**Personnel Intelligence:**

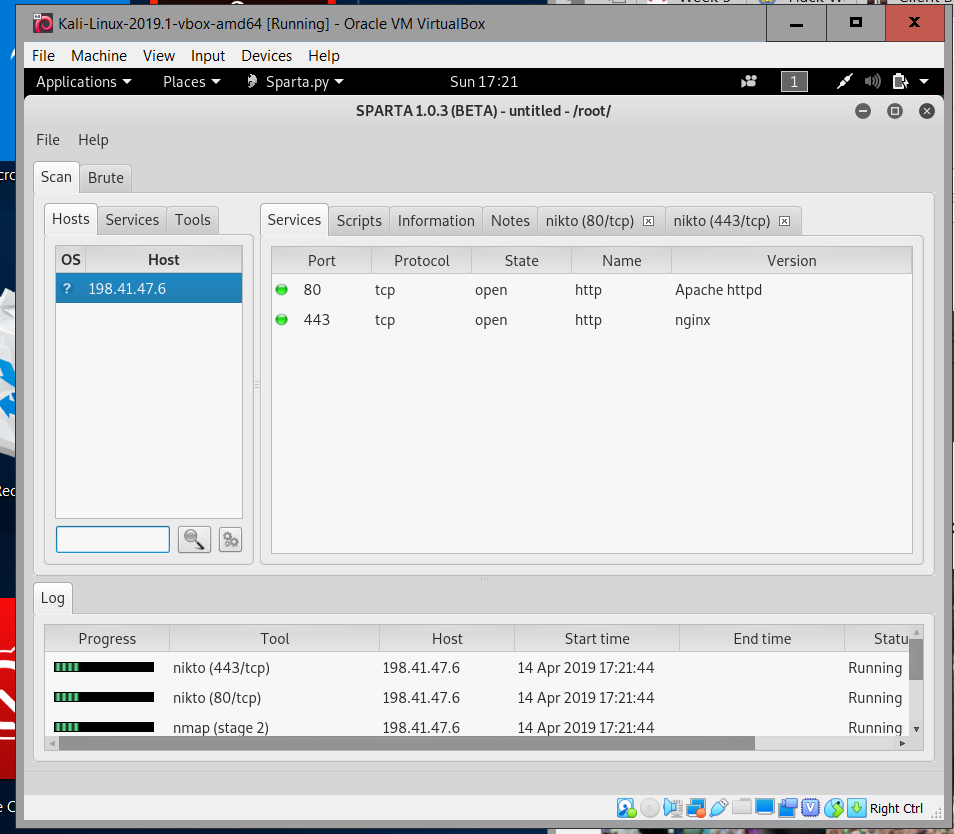
* + Owner: Hubert Hoosman
    - Executive Management
      * Eric Acre [President and CEO]
      * Rachel Parent-Director of Marking and Business Intelligence
      * Ruben Bernales -Director of Human Resources
      * Beckley Bradley-Assistant Branch Manager
      * Jerry Beckley-Chief Technology Officer
    - Middle Management
      * Cindy Mojeske
      * Annie Toczylowski Goede
    - Technical/Team Leads
      * Debbie Meyer, Vantage Project Manager
    - Engineers/Technicians
      * Terry Raby-Systems Engineer II
    - Human Resources
    - Cathy Craom-Human resource assistant
  + Employees and Former Employees
    - Nathan Hennessey
    - Mary Kay Hogan
    - Kenny DeShields
    - Collen Heneghan-
    - Chrissy Thompson
    - Casandra Olenik
    - Daniel Shelby
    - Jenn Cloud (former employee Red Key realty)

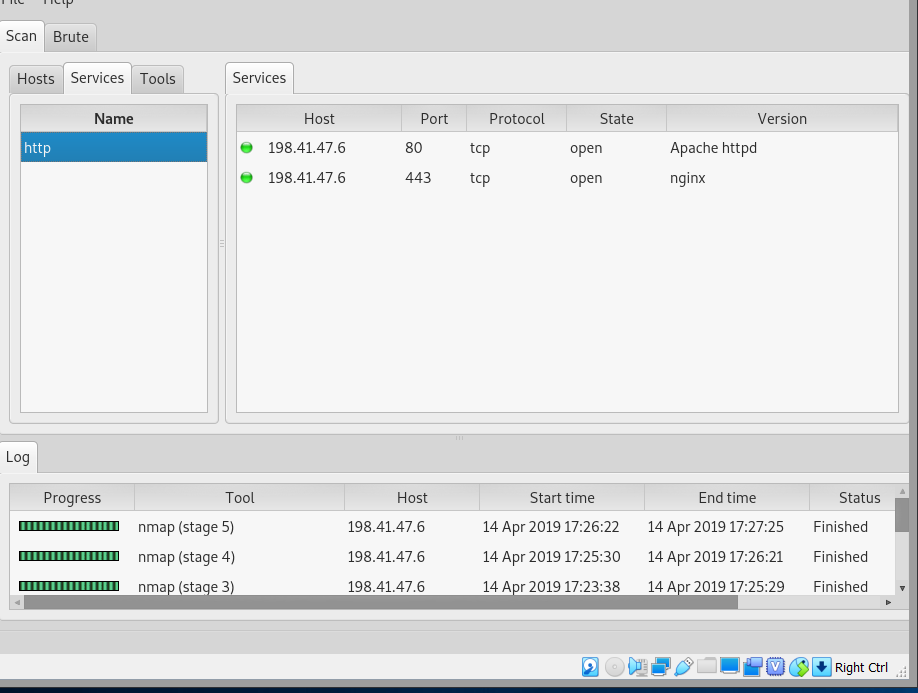
Organizational Map

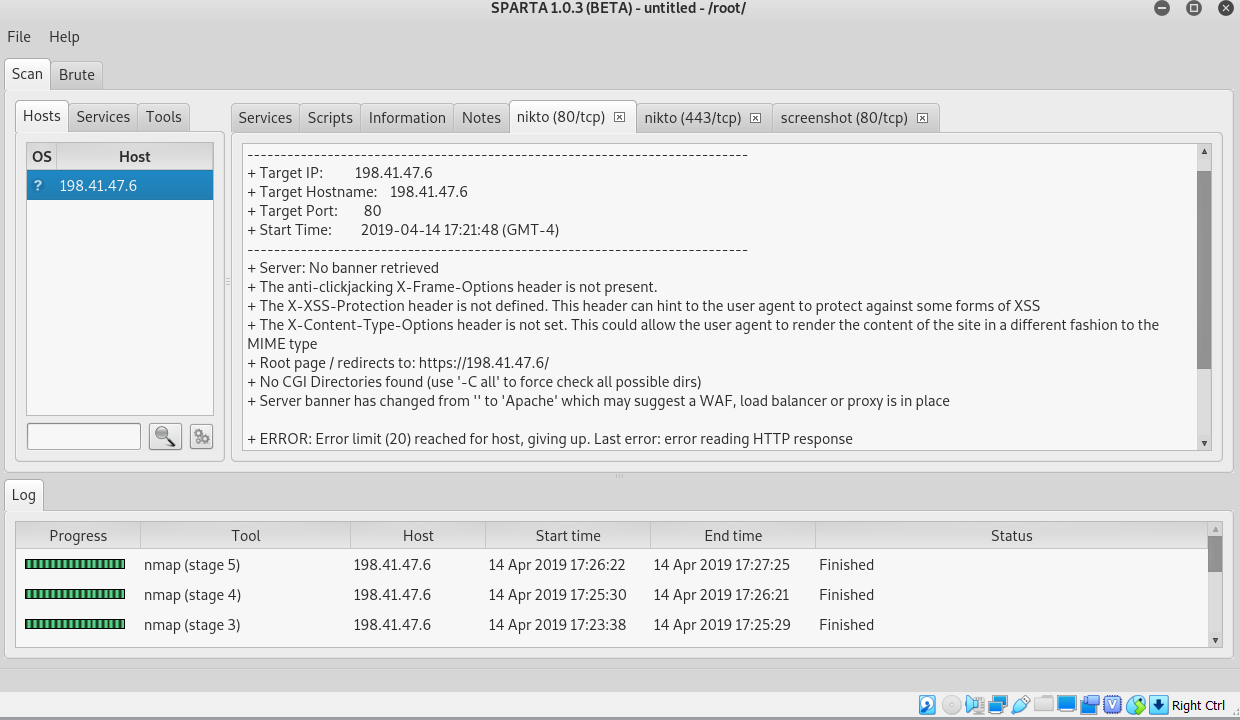


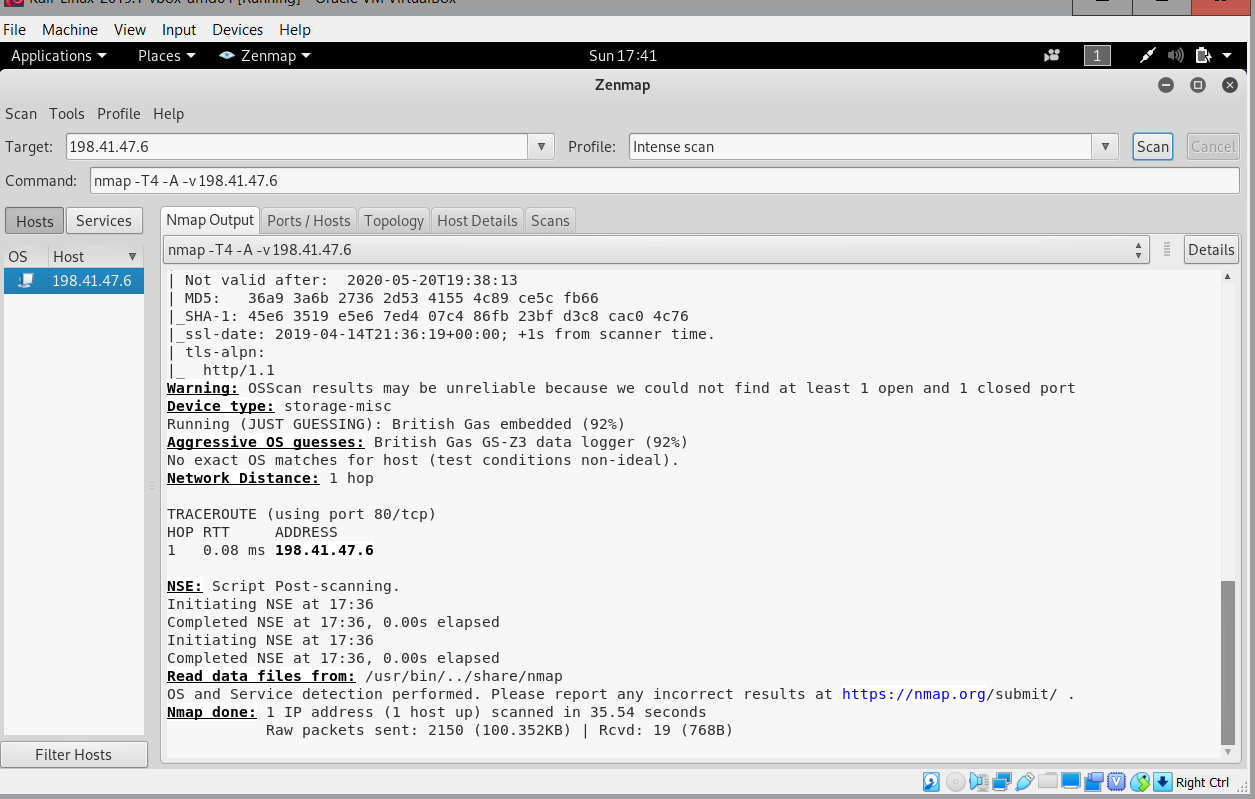
**Vulnerability Assessment:**

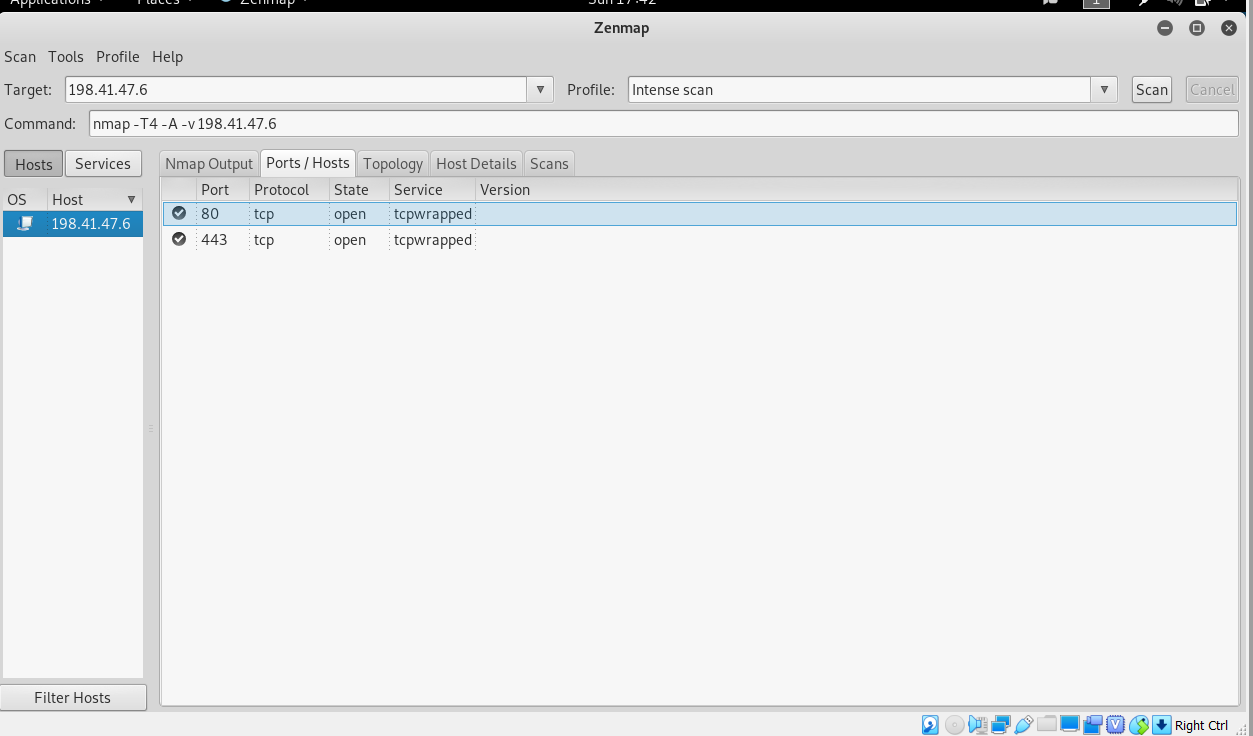
* Active
  + Port Based/Service/Banner Grabbing

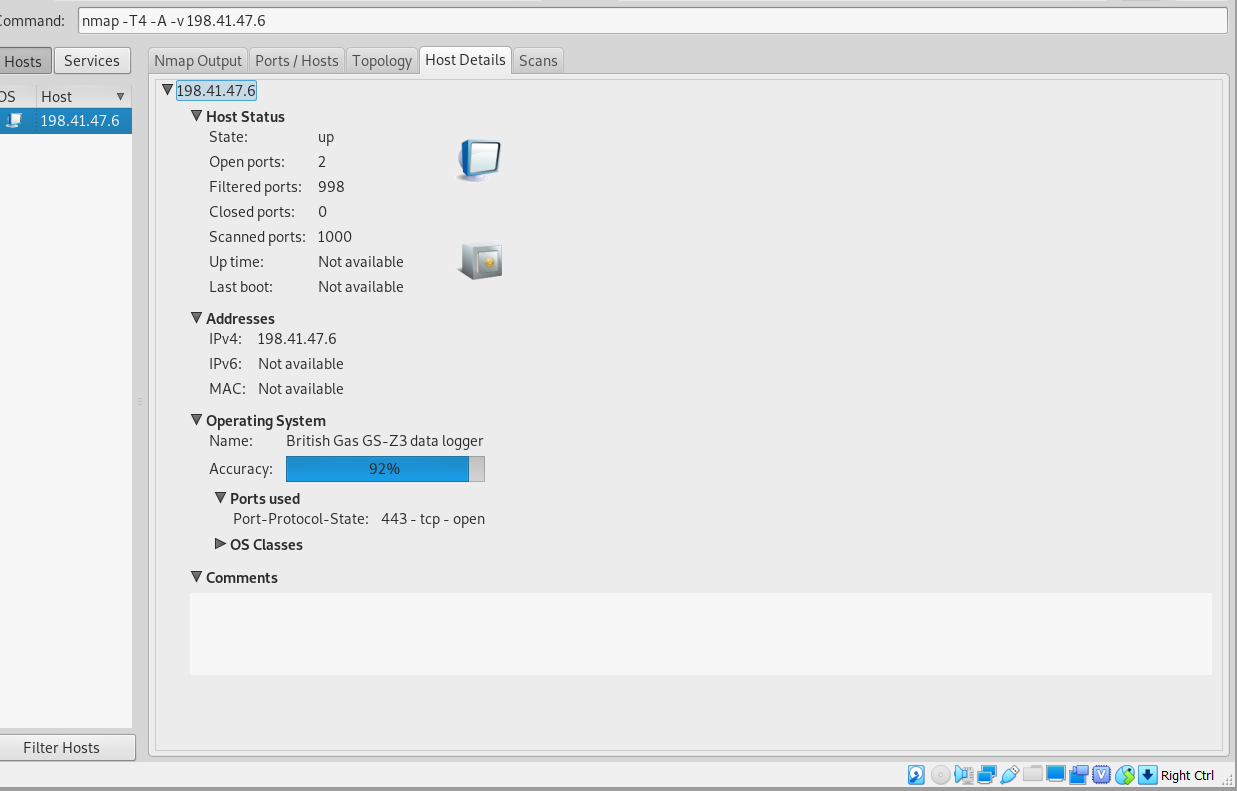


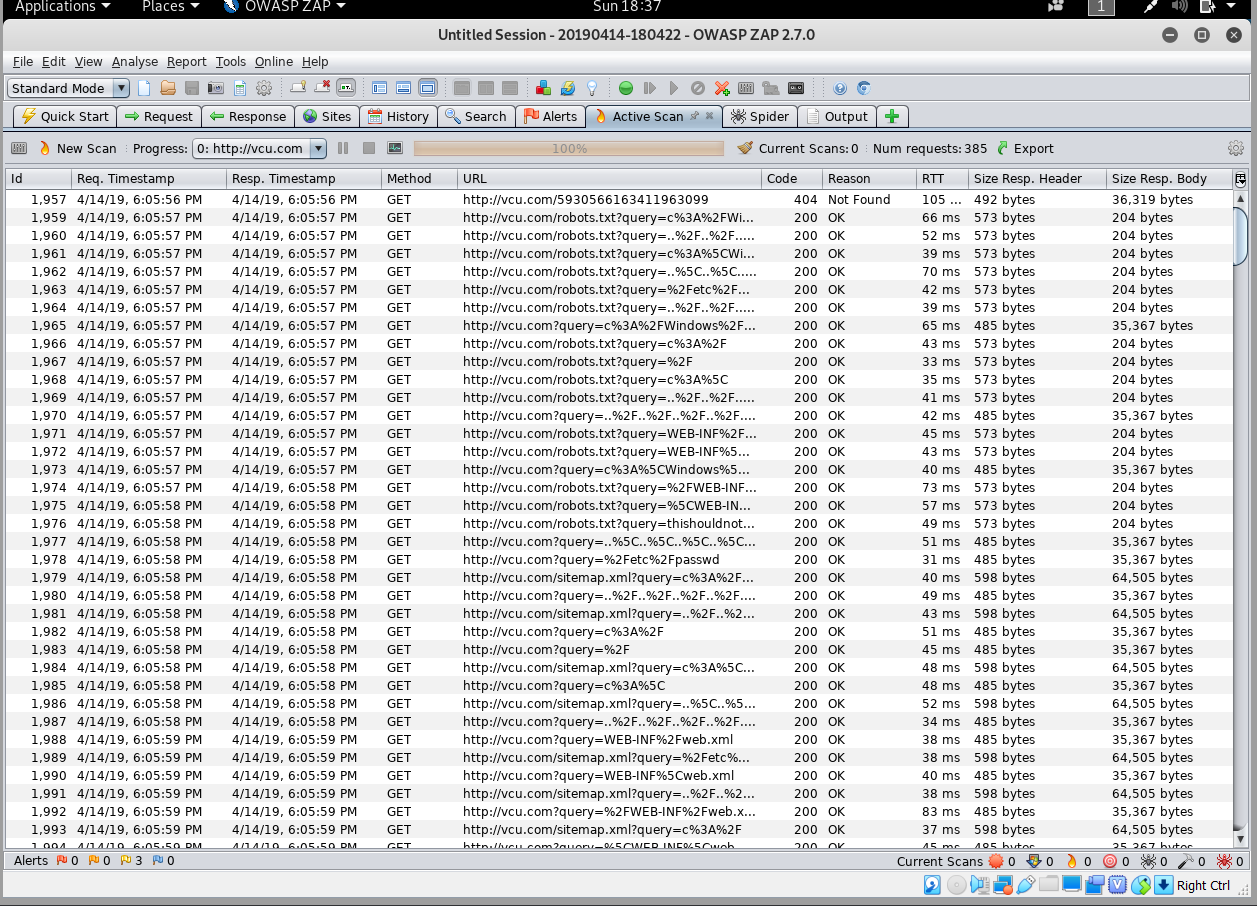


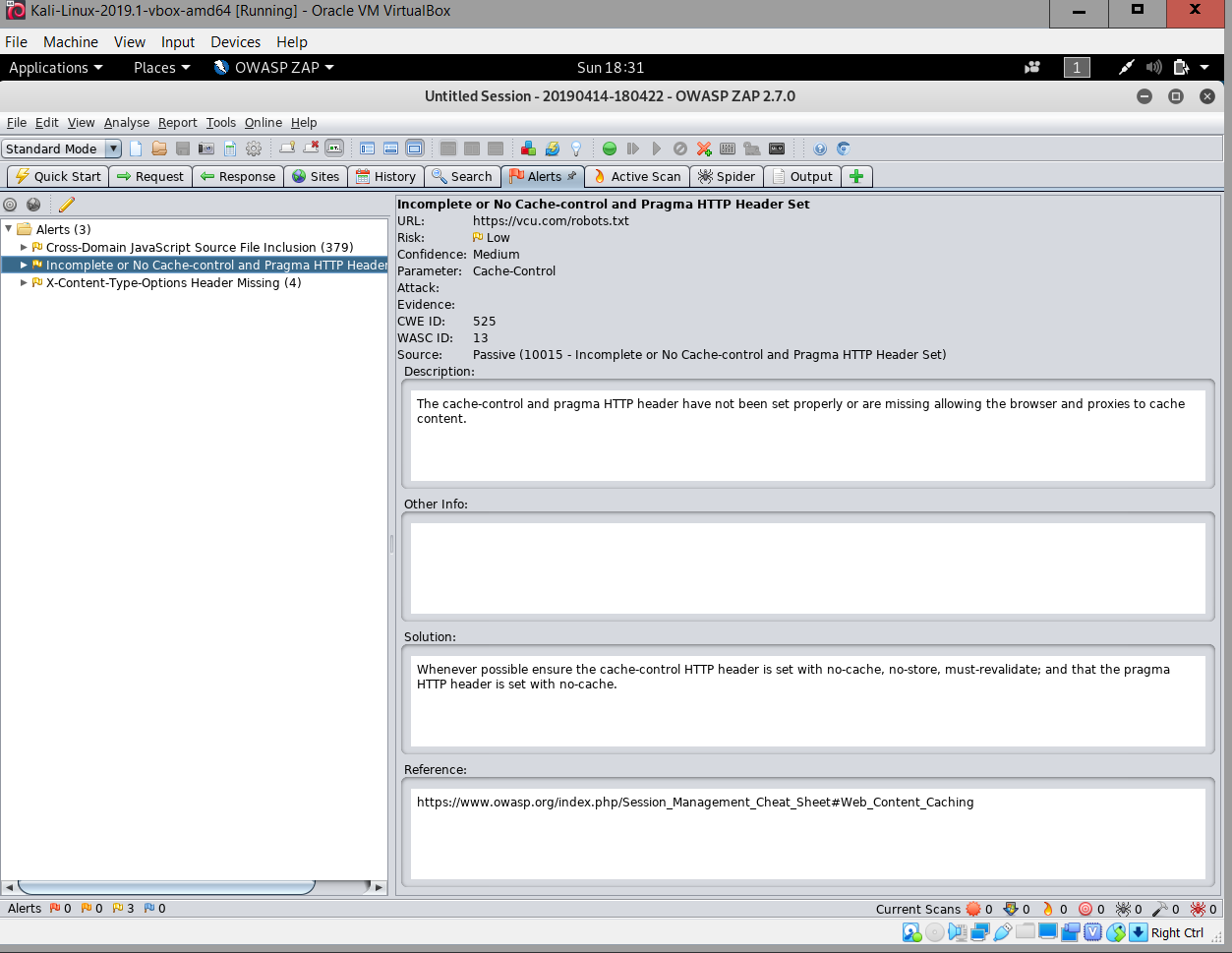


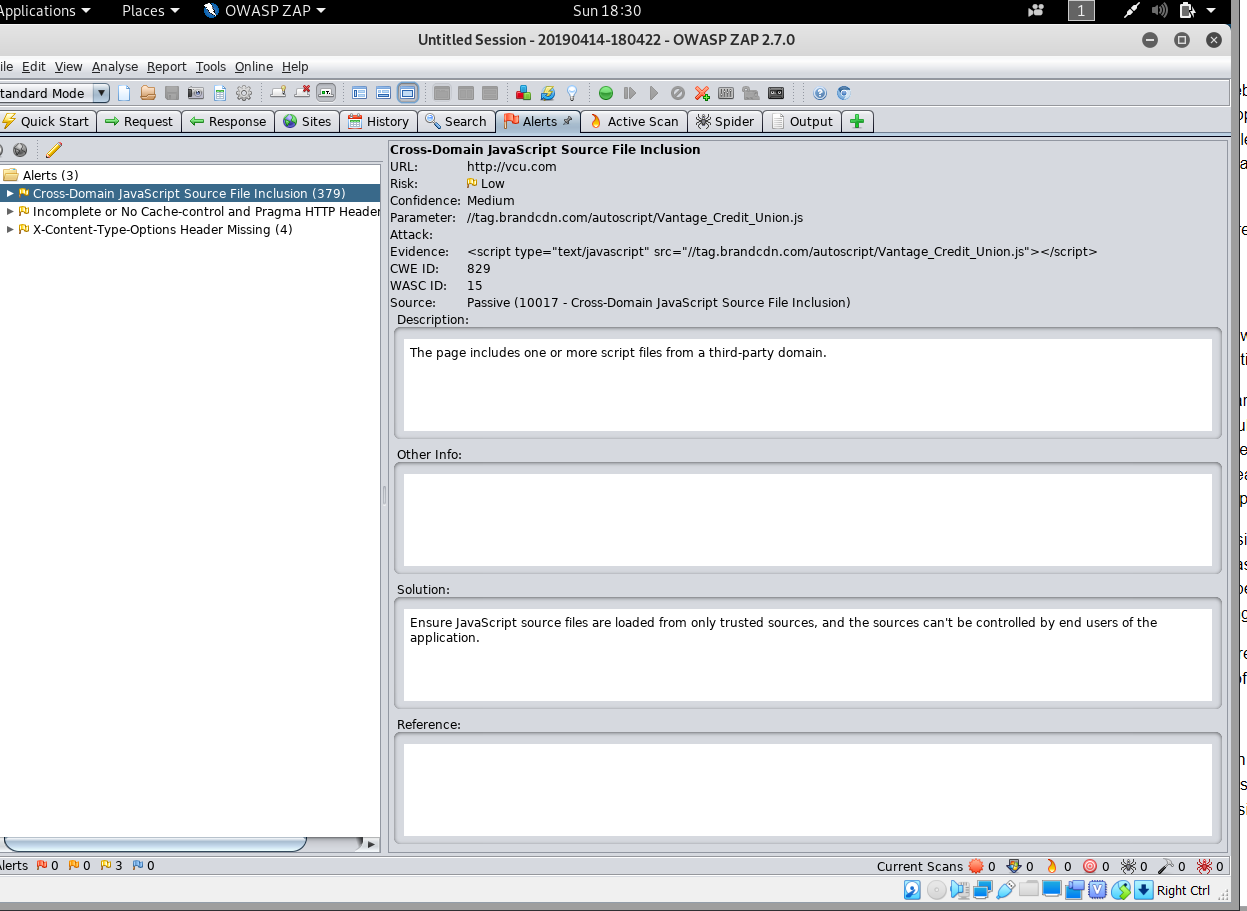


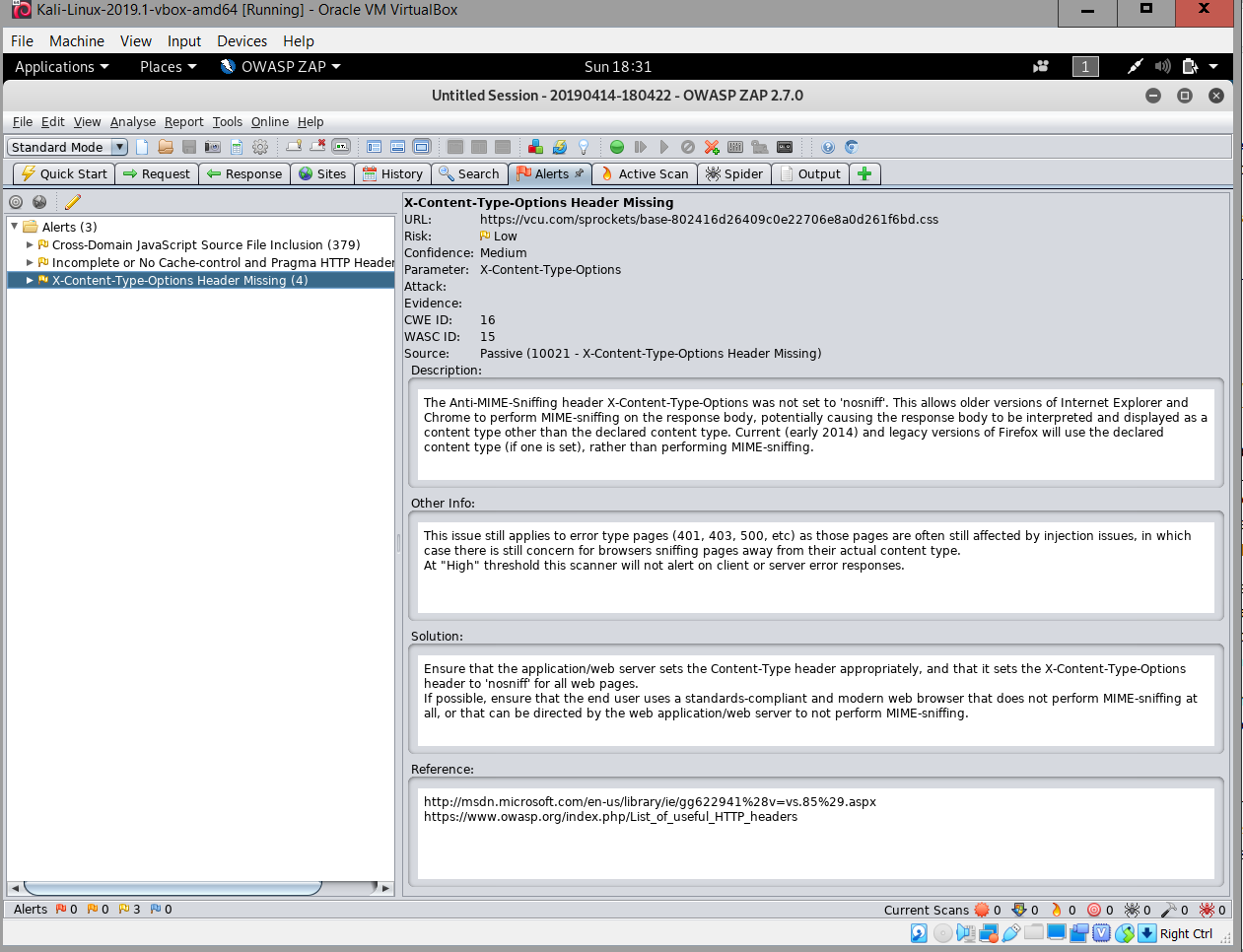


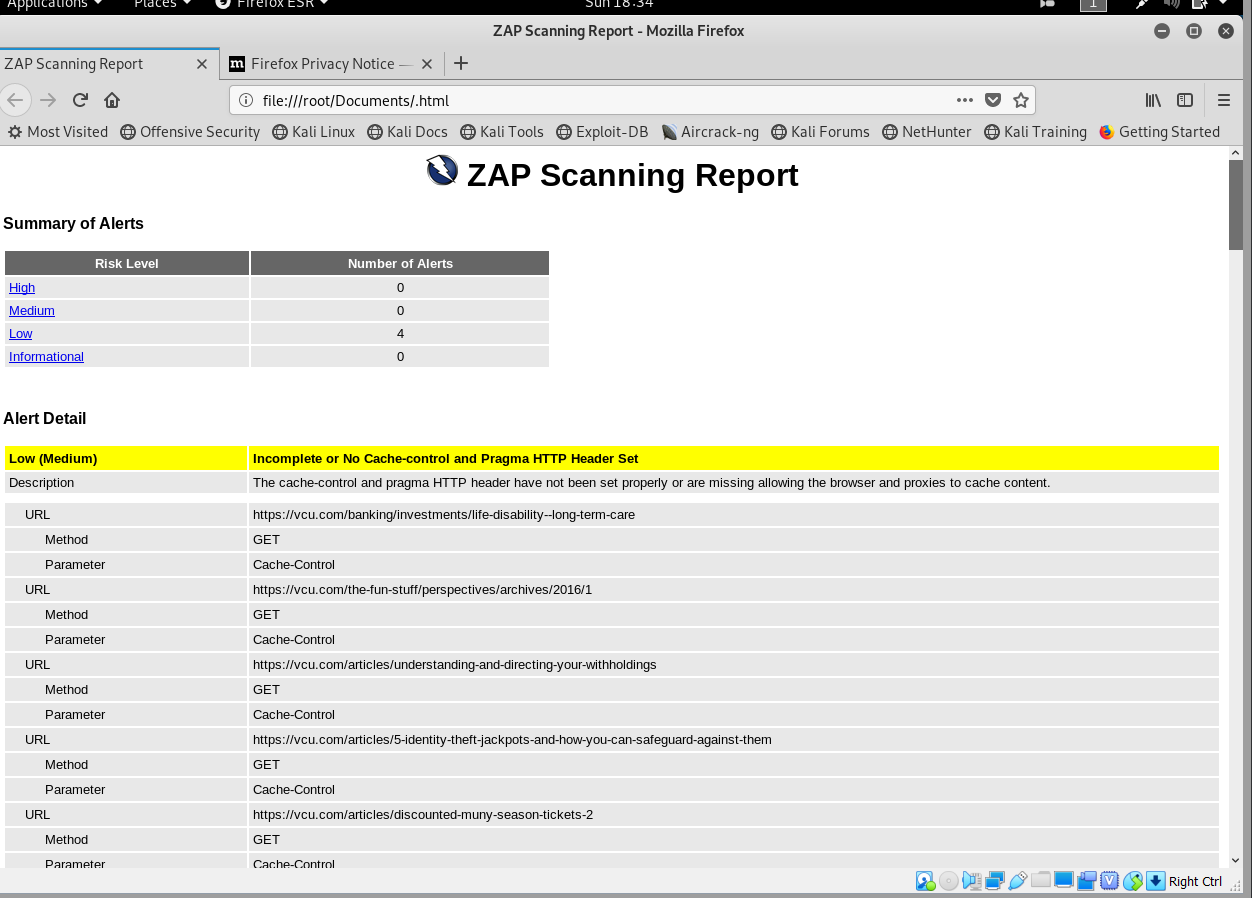


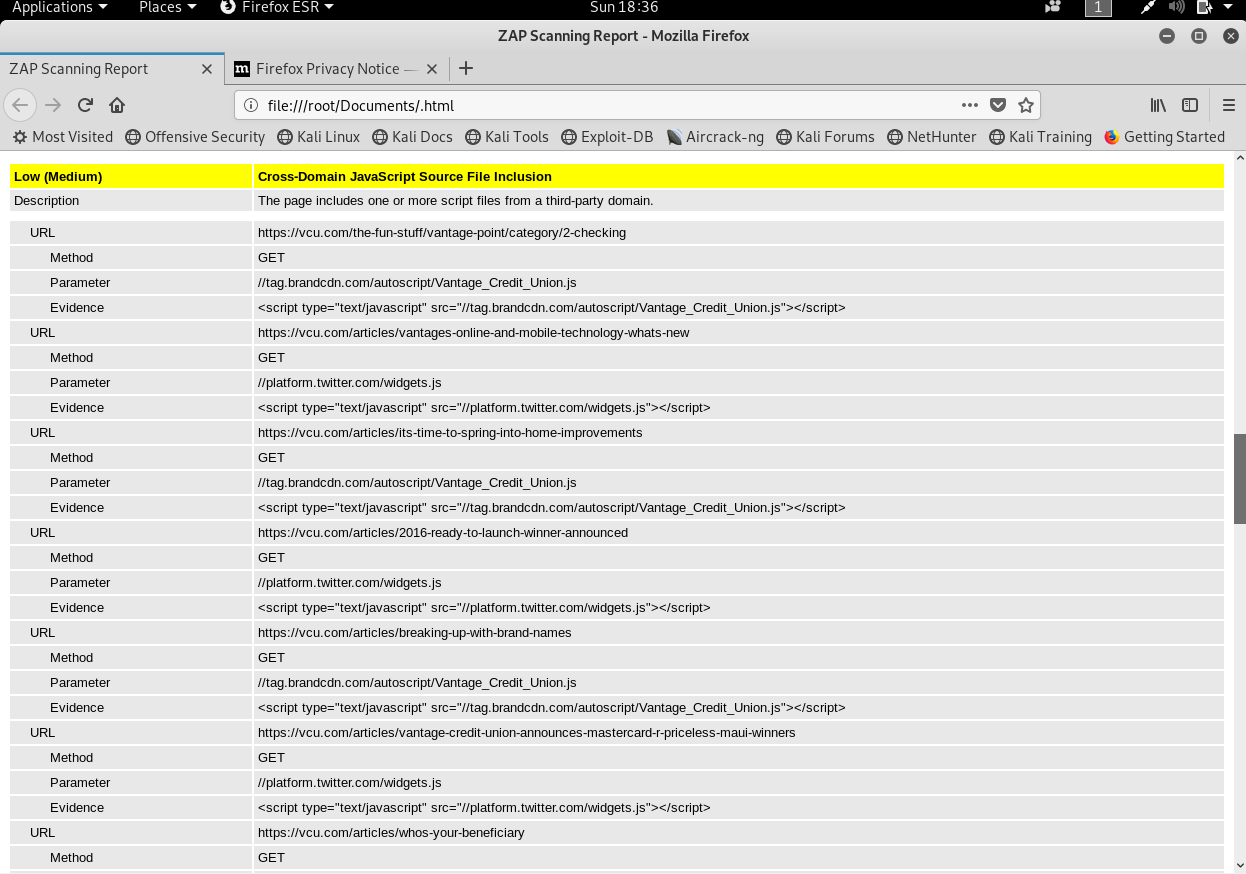
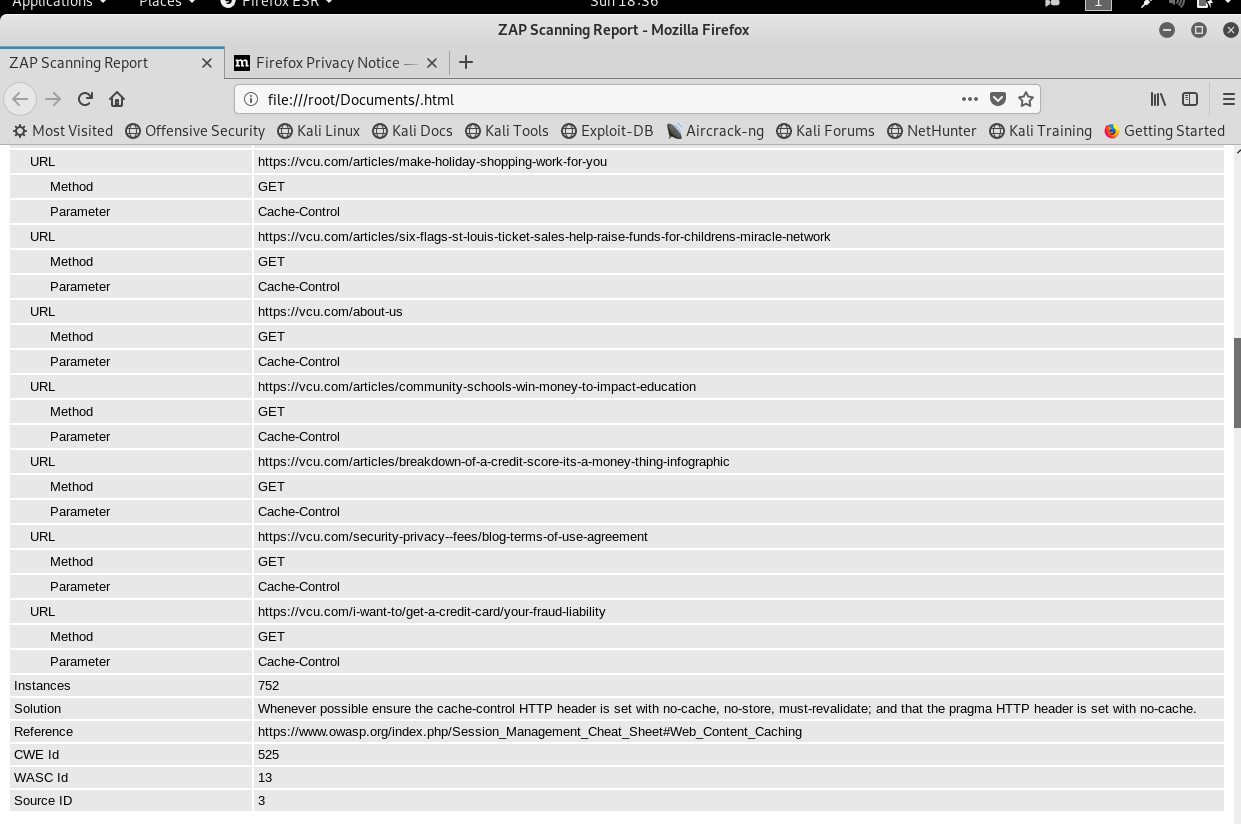
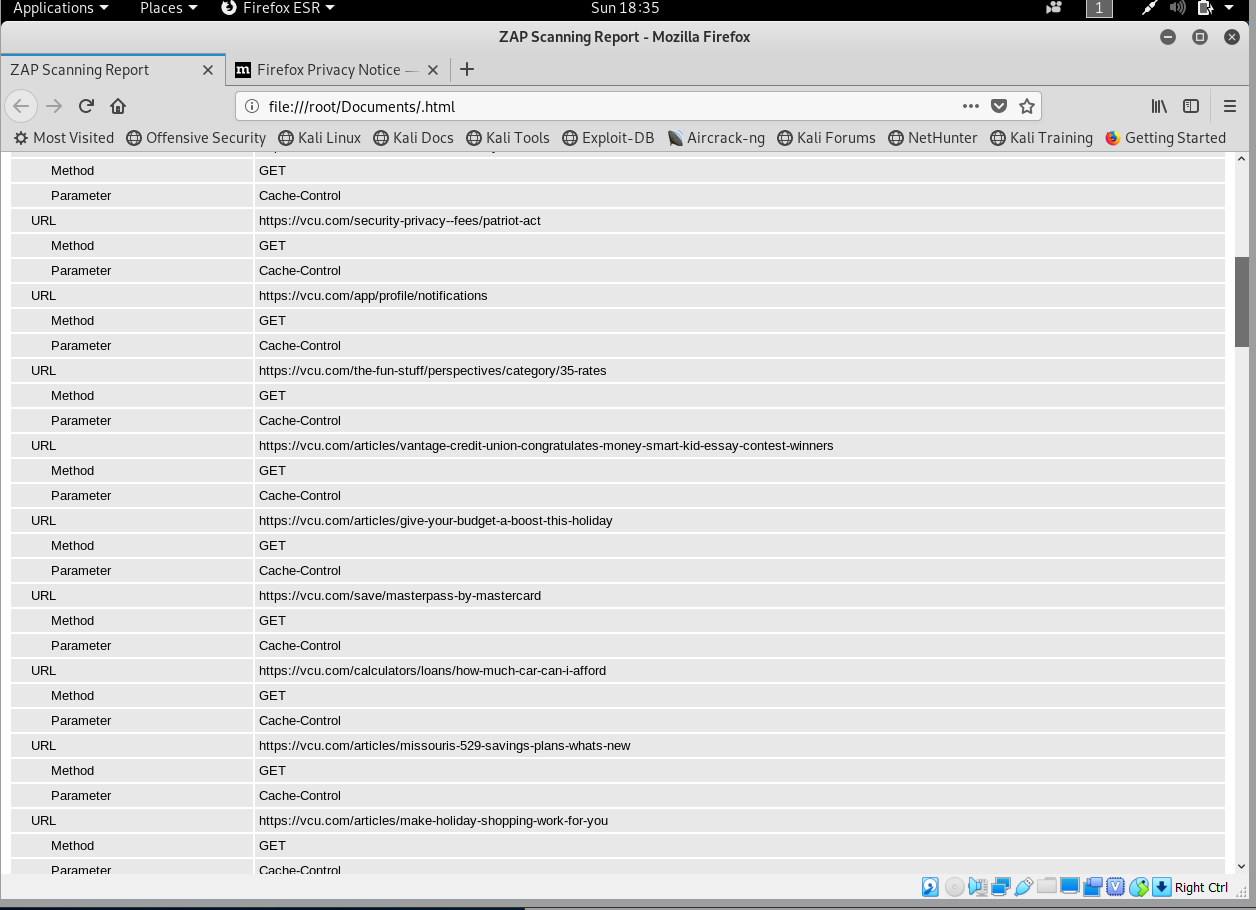
* Web Server Version
* 











* Summary of Results: For the active port scanning, vulnerability and banner grab tests, I used a variety of different programs. First, I used Sparta, and I scanned the IP address of vantage credit union. I’ve included the results in the document. The scanner scanned active ports and revealed any vulnerabilities on those ports. I also used zenmpap for a second scan and to get banner results. The same two ports 80 and 443 were showing the results. Next, I ran a web scan on the URL using owa. This web scanner ran an in-depth analysis on all of the website’s links sub links, and directories. The results alerted me to bumper abilities concerning different links. I also was able to save a report detailing the results of the scan.

**Conclusion:**

In conclusion vantage Credit union security risk is moderate. The financial company could improve their web applications as well removing public information from online data websites.