**JD Haynes**

**Week 16 HW – Open Source Intelligence**

**HW Part One: DNS and Domain Discovery**

**DNS and Domain Discovery**

1. Steps to navigate to centralops.net through osintframework.com

* Go to <https://osintframework.com/>
* Click on “Domain Name”
* Click on “Whois Records”
* Click on “Domain Dossier” which will take you to “<https://centralops.net/co/DomainDossier.aspx>”

1. Enter website of choice in Domain Dossier and view DNS records

* Enter the website URL (Dell.com) in the “domain or IP address” field
* DNS Records
  + Displays the IP address 105.135.166.143 associated with the domain name Dell.com
  + Displays several nameservers and some additional IP addresses associated with some name servers.
  + Displays the MX servers
  + Displays the PTR

1. Network Whois Record

* NetRange: 143.166.0.0 – 143.166.255.255
* CIDR Range: 143.166.0.0/16
* Attacker user:
  + Netrange and CIDR range can be used to identify IP addresses used by the target.
  + Info in Whois Record includes addresses, phone numbers, contact names, emails, and URLs that can be used for social engineering
  + Registered owner and registered address can be used to search for other IP ranges belonging to same organization.
  + Use IP addresses for vulnerability scanning starting with network enumeration (nmap) including port scanning and ping sweeping, service discovery, OS discovery, and application discovery – this information can be used to identify exploitable ports, services, operating systems, and apps. The Nmap Scripting Engine (NSE) and Zenmap can be used to customize scanning, exploits, and attacks.
  + IP addresses can be used by other vulnerability scanners such as Nessus to help build an inventory of connected services and their vulnerabilities.

1. DNS Records

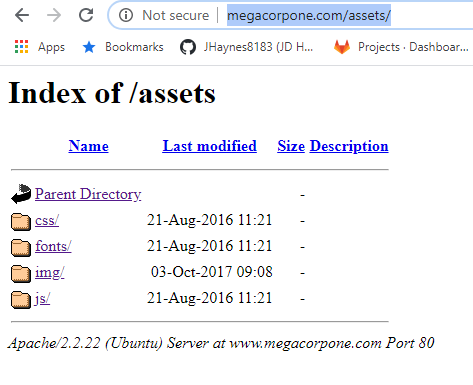
* Displays the nameservers and some of the associated IP addresses for these names servers
* Displays the nameserver usage such as MX (mail exchange), PTR (printer), TXT (apps and services such as adobe site verification, smartsheet site verification, etc – which can provide information on some of the applications used by the organization. This information can be used to research vulnerabilities.)
* Attacker use - Knowledge of the IP addresses and domain name servers can be used for DNS attacks including:
  + - DNS hijacking/redirecting
    - DNS flood attack such as distributed denial of service (DDoS), including NXDOMAIN attacks, as well as distributed reflection denial of service (DRDoS)
    - DNS tunneling
    - DNS spoofing
    - Random subdomain attacks
    - Phantom domain attacks

1. Service Scan – was not included in homework, but I looked at it for fun. It provides info on different services such as FTP, SMTP, HTTP, POP3, IMAP, and HTTPS and their status. In this instance it included the signature algorithm (sha256RSA), public key size (2048 bits), certificate issuer, and the name of the server (BigIP). Some of this info could be valuable for researching attack vectors.

**Google Dorking**

Find an index of MegaCorpOne’s server:

* From google, searched on “site:megacorpone.com intitle:/”
* Search returned several URLs such as <http://www.megacorpone.com/assets/js/> and <http://www.megacorpone.com/assets/img/>
* Clicked on the “Parent Directory” of one of these URLs to go to <http://www.megacorpone.com/assets/> to get to top level of assets. This list can then be used to drill down into each set of assets



**Shodan**

* IP address 93.184.216.34 for example.com identified on OSINT Framework tool. IP address entered into Shodan. This returned information on services available including:
  + Port 80, tcp, http
  + Port 443, tcp, https
* Alternative DNS names were provided: example.com, example.org, example.edu, example.net, [www.example.com](http://www.example.com), [www.example.edu](http://www.example.edu), [www.example.net](http://www.example.net), [www.example.org](http://www.example.org)
* Additional information provided in Shodan included:
  + Latitude 42.1596 and Longitude -70.8217, org Verizon Business
  + SSL versions
  + SSL certificate information including public key type and public key
  + WAF application – Edgecast/Verizon Digital Media

**HW Part Two: OSINT Recon**

MegaCorpOne

* Using Google Cheat Sheet found these links that included multiple contact names, titles, email, phone numbers, addresses, and social media info at the following URLs. The twitter handles are especially useful for gathering more info for individual social engineering such as targeted phishing emails, etc. Photos of some contacts also available – these can be used for demographics social engineering (gender, age, etc.). Also found links that included code used on their website
  + <https://www.megacorpone.com/contact.html>
  + <https://www.megacorpone.com/about.html>
  + <http://www.megacorpone.com/assets/img/team/orig/> (photos of additional team members?)
  + <http://www.megacorpone.com/assets/js/> (code used on website)

|  |  |
| --- | --- |
| CONTACT | INFO |
| Joe Sheer | * CEO * Email: [joe@megacorpone.com](mailto:joe@megacorpone.com) * Twitter: <https://twitter.com/joe_sheer/> * Twitter: @Joe\_Sheer * **Photo available** |
| Mike Carlow | * VP of Legal * Email: [mcarlow@megacorpone.com](mailto:mcarlow@megacorpone.com) |
| Alan Grofield | * IT and Security Director * Email: [agrofield@megacorpone.com](mailto:agrofield@megacorpone.com) |
| Tom Hudson | * Web Designer * Email: [thudson@megacorpone.com](mailto:thudson@megacorpone.com) * Twitter: @TomHudsonMCO * **Photo available** |
| Tanya Rivera | * Senior Developer * Email: [trivera@megacorpone.com](mailto:trivera@megacorpone.com) * Twitter: @TanyaRieraMCO * On github in megacorpone repo/xampp.users: trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0 (perhaps username and hashed password?) * **Photo available** |
| Matt Smith | * Marketing Director * Email: [msmith@megacorpone.com](mailto:msmith@megacorpone.com) * Twitter: @MattSmithMCO |
| William Adler | * Intern * Twitter page: <https://twitter.com/realwilladler?lang=en> |
| Human Resources | * Email: hr@megacorpone.com |
| Sales | * sales@megacorpone.com |
| Shipping | * [shipping@megacorpone.com](mailto:shipping@megacorpone.com) |
| MegaCorpOne | * Email: [sales@megacorpone.com](mailto:sales@megacorpone.com) * Tel: (903) 883 – MEGA * Web: <http://www.megacorpone.com> * Location: 2 Old Mill St., Rachel, NV 89001 (U.S.) * Facebook: <https://www.facebook.com/MegaCorp-One-393570024393695/> * LinkedIn: <https://www.linkedin.com/company/megacorp-one> (currently not active, but could be hijacked and used since it’s listed on their website), The “About” tab reveals their address and a map of their location. * GitHub: <https://github.com/megacorpone> (source code for several of the web pages) * (In megacorpone repo/index.html: source code website) * Using *Apache/2.2.22 (Ubuntu) Server at www.megacorpone.com Port 80* |
| Potential Vulnerabilities – based on bug reports from users. (found info on linked pages using “link:” in the google search criteria)  I think I could spend days going down this rabbit hole – there is so much info out there – these are just a few examples. | * User reprting Windows XP crashes at <https://answers.microsoft.com/en-us/protect/forum/all/windows-xp-keeps-randomly-crashing/a4c1ffd1-898f-4012-a540-f53dfdc12024> provides info such megacorpone’s use of McAfee AV, IE8, control software on an old XP computer, a file name found on PWNED.SYS, etc. – could be leveraged for an attack. * Penetration Test reports at <https://www.offensive-security.com/reports/penetration-testing-sample-report-2013.pdf> and <http://sda.pu.go.id/tkpsda/saddang/uploads/buletin/buletin_201606091844.pdf> Although dated 2013 & 2014, if vulnerabilities are not patched, this could be leveraged. * Additional employee names such as Fred Ducasse (Investments), Stan Denvers (Collections), Handy McKay (Recruiter) on this page <https://rocketreach.co/megacorp-one-email-format_b5e8edb3f42e8177> that also provides the email format for megacorpone being used 100% of the time – makes it easy to impersonate anyone’s email there. * This link provides hosting location, list of internal links, list of javascripts, etc. It includes latitude/longitude of host location which resolved to China. I could not reach the IP address of the host 38.100.193.76. But a page with this kind of information could be very useful for launching an attack on the hosting site. * Just for fun – found this link that just happen to use megacorpone.com in some of their pentesting examples – like using cewl for password profiling and how to mutate password lists using JTR. |

Used OSINT Framework 🡪 centralops.ent 🡪 DomainDossier to get info for domain “megacorpone.com”:

* IP: 74.194.137.8
* Nameservers, name of registrant/admin/tech (Alan Grofield)
* Mail.megacorpone.com, mail2.megacorpone.com, spool.mail.gandi.net
* Support.gandi.net and contact.gandi.net

Using Shodan:

* Support.gandi.net is in Paris, France, IP 217.70.182.71
* Spool.mail.gandi.net has multiple IP subdomains:
  + 217.70.178.211 spool2.mail.gandi.net - port 25 and 53
  + 217.70.178.210 spool1.mail.gandi.net – port 25 and 53
  + 217.70.178.213 spool4.mail.gandi.net – port 25
  + 217.70.187.212 spool3.mail.gandi.net – port 53
  + 217.70.178.1 spool.mail.gandi.net – port 25
  + 217.70.178.214 spool5.mail.gandi.net – port 25 and 53
  + 220.134.173.208 HINET-IP.hinet.net (Taipei Taiwan) Hello [24.102.73.236] – ports 21, 80, 81, 443, 445, 587, 995, 3306, 7010, 7777, 33060 and their associated services (tcp, ftp, http, https, http-simple-new, smb, smtp, pop3-ssl, mysql). Lots of vulnerabilities including sql injection. Per Shodan, appears to be a database and further info includes:
    - Uses Webtechnologies jQuery and NivCMS
    - Marked with vulnerability CVE-2020-0796 for remote code execution on SMBv3
    - Contains list of commands that are recognized by database.

Using crt.sh - searched on site sans.org

Interesting subdomains for sans.org

* Several lab and development subdomains – may not be as secured as production and some include reference to “admin” so could allow easier privilege escalation. Also email subdomains could help identify email addresses for phishing campaigns. VPN sub-domains could provide information that would help attacker gain access across the organization’s VPN. The “files” subdomain might allow access to files with confidential information.
* \*.labs.sans.org
* gitlab.tbt570.sans.org
* \*.devlabs.sans.org
* devlabs.sans.org
* dev-dwgoogleads.sans.org
* admin.labs.sans.org
* pre-odadmin.sans.org
* adselfservice.animal.platform.sans.org
* dev-dwgoogleads.sans.org
* admin.labs.sans.org
* pre-odadmin.sans.org
* \*.vpn.sans.org
* vpn.sans.org
* zeus.vpn.sans.org
* view.email.sans.org
* click.email.sans.org
* image.email.sans.org
* files.tbt570.sans.org
* How attacker might use certificate information
  + Since CT logs contain all certificates issued by a participating CA for any given domain, the attacker can find information such as domain names, sub-domain names, and email addresses – this information can be used for domain based attacks and phishing attacks.
  + Attacker can also create a rogue certificate (a valid cert issued for a domain without the domain owner’s knowledge) that is accepted by clients as genuine, then the attacker can user the rogue cert to create illegitimate websites that are indistinguishable from real websites.
  + Many content management systems such as Wordpress will not have any form of authentication when initially set up. Many web hosting providers support https by default so the domain name will appear on a CT log – attackers can search the CT logs and find the web apps not yet set up with authentication then take over the server.
  + PKI vulnerabilities in the hashing algorithms (especially MD5) used by digital certificates can be leveraged to create man-in-the-middle attacks.
* Methods to mitigate threats posed by certificate transparency
  + Organizations should monitor the public CT logs for certificates issued against the domain/s they manage and identify any rogue certificates so they an be revoked. There are multiple search engines available for viewing certificates such as the ones listed above and automation could be implemented to run daily checks for new certificates that are then verified. There are already vulnerability scanning tools, config mgmt. tools and other dedicated tools available to check for insecure certificates and new certificates. This is the easiest and lowest cost prevention.
  + Use a certificate and key management system such as Venafi, Entrust Discovery, Trustwave, Symantec) to keep track of and manage certificates. There will be added cost for the service but it is one of the most practical ways to manage certs and therefore help mitigate threats. Some orgs will instead store private keys in separate networks and/or encrypted containers as an alternative.
  + Ensure that all your internet client software has the latest security updates installed to protect against security breaches that result from fraudulent certificates.
  + Never trust an expired certificate – put automation in place to prevent trusting expired certs. Train users to follow this policy as well.
  + Organizations can implement their own PKI but this can be costly, requires a lot of effort, and may have to be outsourced. This solution is not reasonable for most orgs.
* Note that there are multiple search engines that can be used by organizations and attackers to monitor and gather certificate information including:
  + - crt.sh
    - censys.io
    - developers.facebook.com/tools/ct
    - google.com/transparentcyreport/https/ct

**HW Part Three: Recon-ng**

Using Recon-ng:

* Used Recon-ng to discover 90 hosts on Rapid-7.com

