OSINT Assignment

Jacob Krupa

ITMS 543

9/25/18

University of Illinois at Chicago OSINT Report

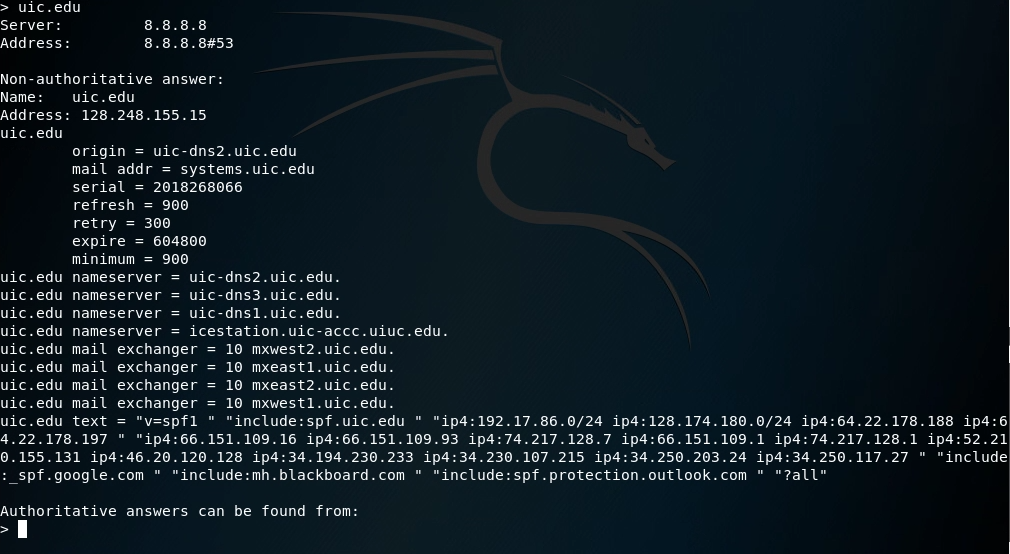
For my OSINT assignment, I have chosen the University of Illinois at Chicago for my passive recon. I chose uic.edu because through my initial recon of small businesses and schools, I saw that my initial DNS search for uic.edu brought valuable information and showed me that they most likely host their own servers.

Whois



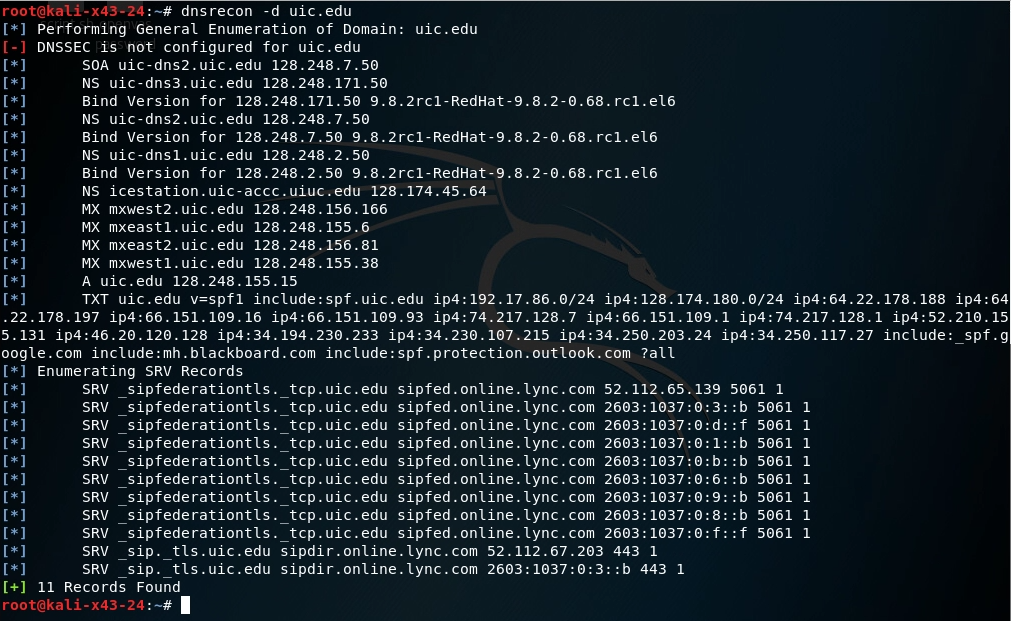
With the whois command, I was able to spot that UIC hosts their own DNS name servers, which will possibly lead to being able to recon more information with more tools and it means they most likely host more servers as well. Also, under administrative and technical contact, it gives me a name of Edward Zawacki and his email “edz@uic.edu”. Now I know a certain person named Edward Zawacki that I know must work at UIC because his name is on their DNS records and now I know UIC’s username/email patterns for logging into their system and I could possibly use Edward’s email for a possible attack.

Nslookup



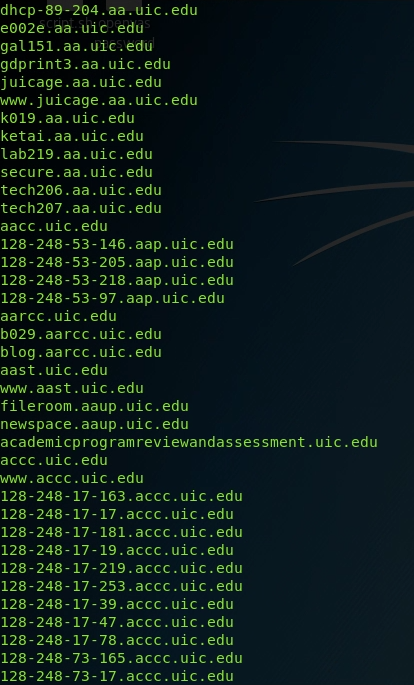
Here, the nslookup command allows me to search for further detail about UIC’s servers and DNS information. Here I am able to see that UIC has a 4th name server that I didn’t pick up with whois called icestation.uic-accc.uiuc.edu. I am also, now, able to see UIC’s mail servers, which they have four. They also host their own mail servers, which are probably easier to break into than mail servers hosted by someone like Google. From their internal IP addresses from which they query the DNS servers, I can see that they use google and blackboard in some way.

Dnsrecon



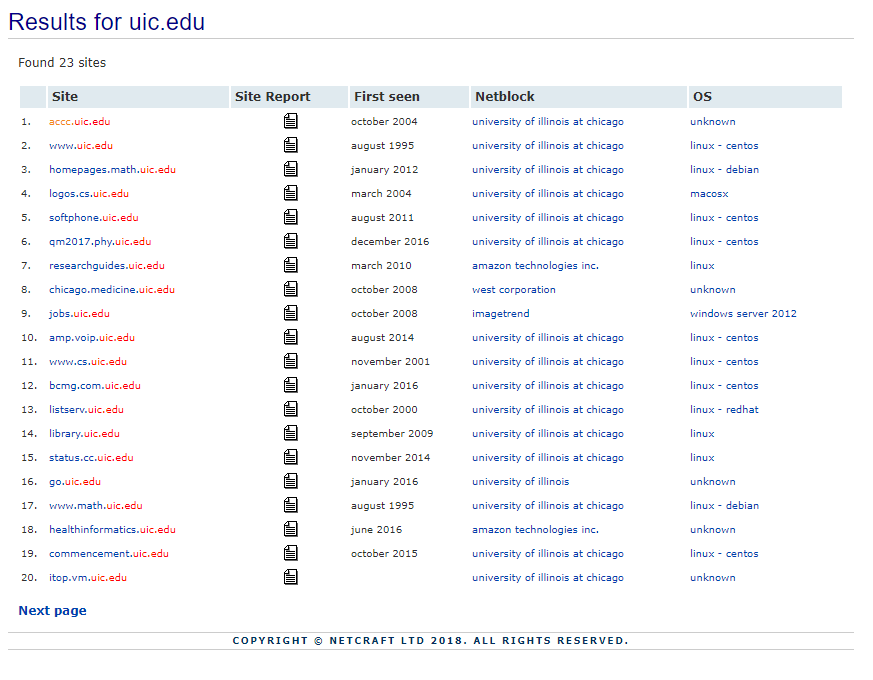
With dnsrecon, I am able to pull some very valuable information for which I can use later to attack UIC. First off, I am able to see that almost all of their DNS name servers run on some form of the RedHat Linux distribution, which allows me to know that their name servers run on a Linux box. Secondly, I was able to pull 11 SRV records off of uic.edu. These records show that UIC uses the Microsoft Lync service, which can be described as Skype in a way. I believe Skype is now Microsoft Lync and I believe Office 365 has also been integrated into this. Here I can host names of these servers, their services like sipfederationtls or sip.\_tls, what protocol they use like TCP, the ports theses services use like port 5061, and what I believe to be either target IPs or host IPs. This gives me a lot of insight into what UIC is doing in their network.

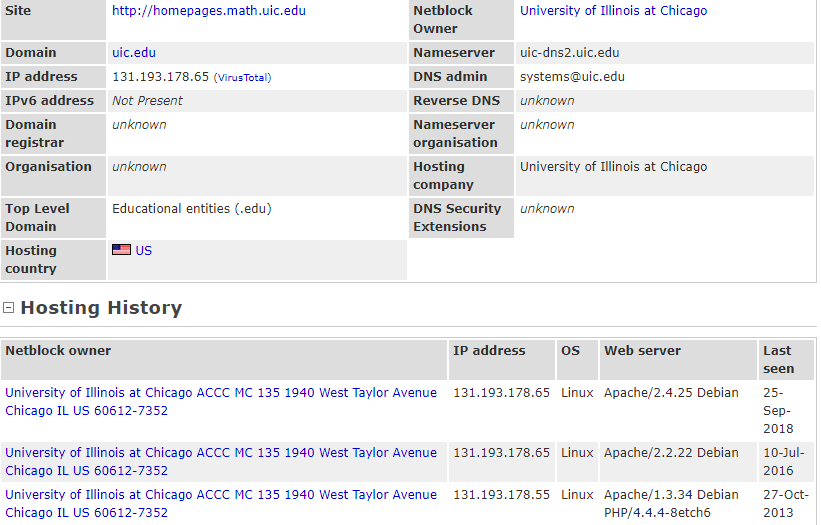
Sublist3r



Next, I used sublist3r, which gave me hundreds and hundreds of sub-domains of uic.edu. This gives me a whole list of potential attacks targets I can use to try to breach in UIC. All in all, this tool gives me more information to work with and tells me what I could potentially target.

Netcraft





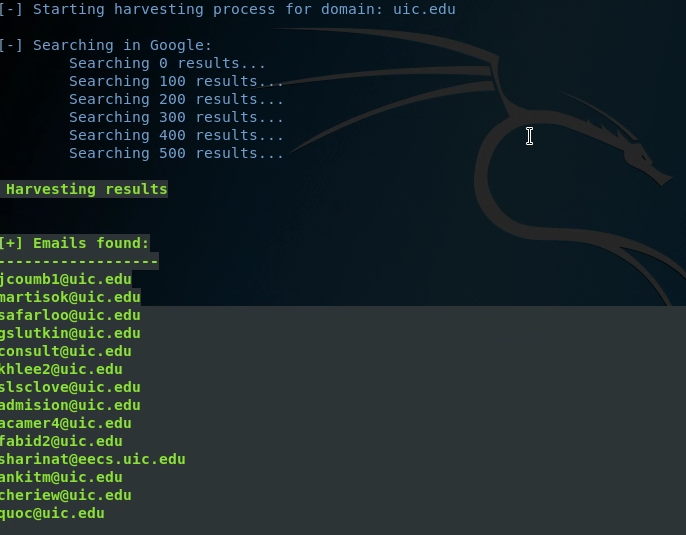
With the Netcraft website, I was able to search and find 23 domains and sub-domains of UIC. From the general look of it, they seem to mainly run on Linux boxes of several different distributions including Centos, Redhat, and Debian. They also seem to occasionally use Windows Server 2012 and Macosx. The servers that are run by amazon also run Linux distributions. Through Netcraft, I was able to see what type of webserver each domain and sub-domain runs and what type of OS they run. Almost every Linux box was found on Netcraft ran some version of Apache. The Amazon servers ran a Linux distribution that also ran nginx 1.4.0 and the Windows server 2012 box ran Microsoft-IIS/8.5. The Linux boxes that ran Apache were not consistent across the board in terms of what version they ran. I saw Apache versions 2.4.10, 2.2.15, 2.4.16, 2.4.6, and 2.4.25.

CVE Details



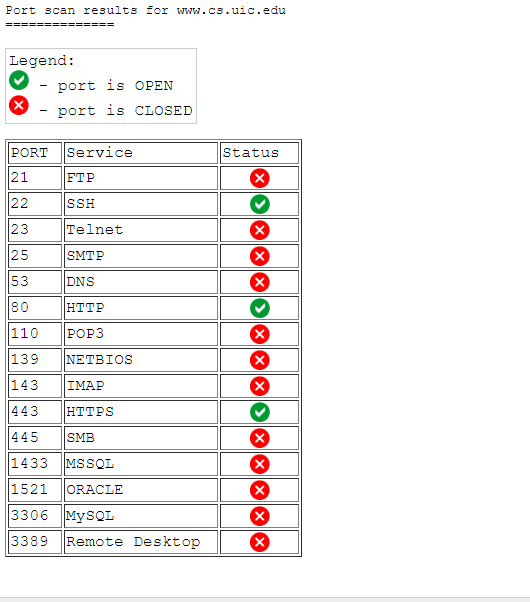
Using information learned from Netcraft like webserver types and versions, I looked through a site called CVE Details. This site gives me the known vulnerabilities of certain webserver versions. This gives me a lot of information as now I know how I can potentially exploit their domains through webserver exploits. For example, Apache 2.4.6 is pretty vulnerable to DOS attacks and Apache 2.2.15 is vulnerable to DOS attacks as well but it can also be exploited through overflow and bypass exploits.

TheHarvester

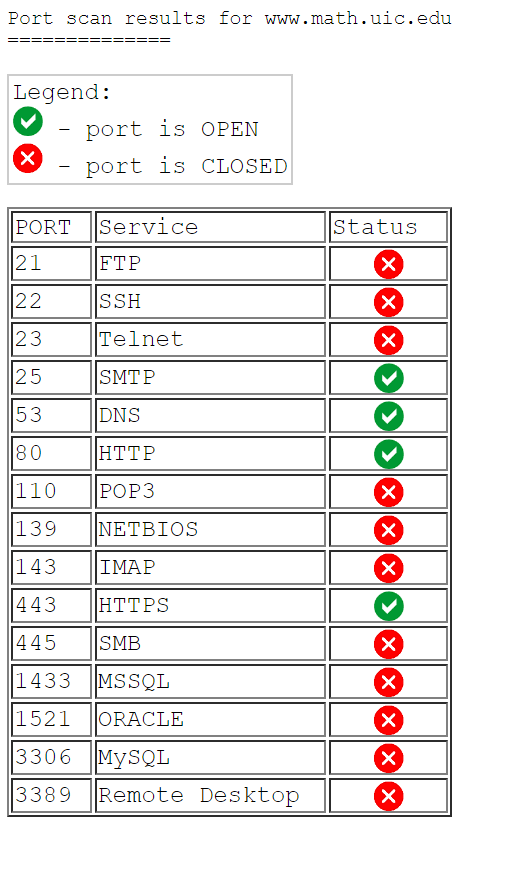


Using theharvester tool, I was able to pull about 14 UIC emails using google’s search engine. I can use these emails for possible targets to attack and use their email to gain access or I can use their email and try to use gain access to their accounts through social engineering/phishing techniques.

Passive Port Scan



Finally, I used passive port scans from OSINT Intel Techniques website to see what ports are open on UIC’s domains and sub-domains. Here I scanned www.cs.uic.edu, which is most likely their computer science department website. As you can see, they have 3 ports open, 22, 80, and 443.



Here, I also did a passive port scan of the UIC math department and they have more ports open, which are 25, 53, 80, and 443. Using this tool, I am able to look at every sub-domain if I wanted and try to see what ports open and what ports are closed, which gives me more and more info about the target and what I could do to break in.

Conclusion

Each of these tools provide small bits of information about a specific company or a specific target. You will get small pieces of information, but the more recon you do and the more tools you use, the more information you get. That information builds and builds and then you get a pretty good picture of what the target is and what you could do to exploit that target. All this information gathered could be used as vectors of attacks or as exploits that can be used to facilitate an attack. Through my recon and use of passive tools, I was able to find out how many DNS servers and mail servers UIC is running and what OS’s they are most likely using. I was able to find a lot of emails that used uic.edu and that gave me a pattern of what a username looks like in a UIC system and I can also use those emails to launch social engineering attacks to be able to gain access or exploit those emails. I was able to find a decent number of sub-domains of UIC and was able to find out what type of OS they were running and what type and version of webserver they are running. With this information, I can search for the many vulnerabilities of those operating systems and those webservers, which gives me a lot of vectors of attacks on those sub-domains. Finally, I scanned some of the sub-domains and found out which of their ports are open, which could also be used as a vector of attack.

Basically, all this information builds up a profile on my target and I get a pretty good idea of what my target is and what I can maybe do to break in and research and explore further exploits based on this initial research. This information allows me to explore into further exploits and brings me closer to actually getting into a target’s network.

UIC itself is not the most secure place in terms of what information I’ve gathered from my recon. I was able to get a lot of emails, enumerate their SRV records and see what they are using them for, I was able to see their name servers and their email servers, and finally I was able to see what most of their main subdomains were running on and what their vulnerabilities are. I can use information learned to further my research into my target of UIC and see what I can do to get closer to breaking in.