Assignment 2

February 23, 2020

Task: Short Answers

1.) **During a penetration test, a testing team discovers a vulnerability. What will be written in the report about this vulnerability? Looking for things related to this vulnerability, not examples. Name at least 4.**

The testing team will provide the following information in their report about a vulnerability:

a. Information about the vulnerability itself.
b. Information about what it is affected by the vulnerability (systems, networks, applications, processes, people, etc.).
c. The probability that the vulnerability will be exploited.
d. The impact (technical, financial, physical, etc.) that exploitation of the vulnerability would have.
e. Whether the vulnerability has already been exploited, insofar as we can tell.
f. Information about how the vulnerability can be exploited and steps to reproduce an exploit.
g. Recommendations about how the vulnerability can be remediated or mitigated.
h. Recommendations to mitigate other risks.

2.) **In what ways could a penetration test provide different results than those from an automated vulnerability assessment? Why?**

A vulnerability analysis is similar to, and usually part of, a penetration test; however, it is less thorough. A vulnerability test includes automated reconnaissance and scanning for potential vulnerabilities, as well as generic recommendations for mitigating vulnerabilities. It is a passive reconnaissance technique.

Conversely, in a penetration test, the testers will not only scan for vulnerabilities but will also attempt to exploit them. By actively validating the vulnerabilities via exploitation, testers will gain more comprehensive insight into the nature of the vulnerabilities and can therefore offer additional information about the potential risks to the organization, as well as ways to harden the system and protect against future attacks. It is an active reconnaissance and penetration process.

Both vulnerability analyses and penetration tests identify vulnerabilities; vulnerability analyses report *potential* vulnerabilities while penetration testing confirms *actual* vulnerabilities via exploitation. Penetration testing involves human testers examining the system while vulnerability analyses are automated, which means penetration testing provides for broader, more nuanced understanding of the system.

3.) **After you finish a penetration test, you write the report. Which section(s) may contain fixes/recommendations for vulnerabilities you found? Explain.**

Because the report will be seen by many different people within the organization, there is a need to restate the concepts so that they meet the needs and priorities of each party reading it. Rephrasing items in the report will be important so that they are understandable to both technical and non-technical teams; therefore, recommendations for mitigating vulnerabilities may be made in several sections of the report:

- Executive Summary
  - This section of the report may be read by non-technical management and therefore high-level mitigation strategies—especially immediate ones—may be made here.

- Introduction
  - This section will provide an overview of the test but may also be used to provide the organization with some recommendations.
- Findings
  - This section lists details about all the findings from the test, including specific vulnerabilities and the level of risk posed to the company. For each vulnerability discovered, the team should outline recommendations for remediation.
- Recommendations
  - In this section, the team should clearly outline all recommendations based on their findings. These recommendations may be in technical in nature or may offer suggestions for improving physical security or mitigating human error within the company. The testing team should provide clear steps for how to carry out these suggestions.
- Conclusion
  - This section includes a summary of the reasons for the test, the scope and targets, the testers' methodology and findings, and an overview of recommended actions to be taken as determined by the test's findings.

4.) Why would you use a tool like masscan instead of nmap? How these tools different?

Masscan and nmap are similar port scanning tools used for reconnaissance, but there are several key differences:

The biggest difference between masscan and nmap is speed: masscan is incredibly fast, claiming to scan the entire Internet in six minutes. That makes it an invaluable tool for scanning large networks. It works asynchronously, not waiting for responses before moving on to the next host. The trade-off to speed, however, is accuracy. While masscan can fire through targets, it cannot detect dropped packets and therefore does not yield refined results. Additionally, due to the rate at which masscan is scanning and causing dropped packets, it is possible to induce a Denial of Service, even against oneself.

Nmap, meanwhile, works synchronously, waiting for a response and trying again if it does not receive one for each packet. When hosts are unresponsive, Nmap waits for the request to timeout before moving on. This process yields more accurate results but at a significantly slower rate.

Another key difference is discretion. Masscan creates a "loud" presence that is easily detectable due to many dropped packets, while nmap offers options to obfuscate visibility, such as randomizing source IPs. Masscan is typically more useful in a blue-team approach, while nmap can be used more dependably in a red-team assessment when keeping a low profile is crucial.

Nmap offers many other features that are unavailable with masscan, helping to hone one's search. Unlike masscan, nmap accepts domain names as well as IP addresses. Nmap also has a helpful debug feature.

For the reasons outlined above, nmap is often used for regularly scheduled vulnerability scans, while masscan is helpful for finding anomalies within a large network.

5.) What kind of nmap scan will result in a port being listed as unfiltered? Why does it say this and how is it helpful?

A TCP ACK scan (command: **-sA**) can be used to detect ports that are unfiltered, i.e., not protected by a firewall. Ports protected by a firewall will either not reply to an ACK, or will yield an error message. Unprotected ports,

whether they are open or closed, will return a RST packet. By scanning in this way, nmap detects ports that are unfiltered by a firewall and therefore can be used to map out a network's firewall system.

6.) You are enumerating subdomains using some automated tools and ended up with about 65,000 subdomains. As if we were performing an actual test, what are the next things you should do with this list, and how could you do it?

Large raw data sets are typically not useable until they are refined. The first step in managing a list of 65,000 subdomains would be to find the most interesting results and organize them. By formulating a list of naming conventions, for example, a tester could discover patterns that lend clues about the organization's internal network topology as well as assets. Additionally, using reconnaissance tools (e.g., EyeWitness, recon-ng, nmap, etc.) a tester can determine operating systems, versions of the devices in-network, and the vulnerabilities therein. Vulnerability scanners such as Nessus or OpenVAS can scan subdomains for known vulnerabilities, such as cross-site scripting.

7.) Name some of the things you can do to protect test results during and after an on-site penetration test? Name at least three.

1.) Secure communication – between the penetration testing team and the organization is critical because sensitive information will be exchanged. Steps should be taken to ensure that all correspondence is encrypted and that only designated individuals will have access to it.
2.) Secure handling – of data and records per an established chain of custody. There should exist thorough documentation about who accessed data and when, and who modified it and how (i.e., a "paper trail"). Data should be kept in one secure location.
3.) Secure data retention – including policies about the retention of test results, correspondence, reports, and other sensitive information that, if leaked, could give malicious entities details about how to carry out an attack against the organization. These policies should be thoroughly communicated and agreed to in writing by the organization.

8.) What are all possible packets sent by nmap by default to determine if a host is alive?

The following is a list of packets that nmap can send to discover hosts:

- TCP SYN ping (command: **-PS**). If the host is closed, a RST packet will be sent back. If it's open, the target will attempt to continue the three-way handshake by sending a SYN/ACK TCP packet.
- TCP ACK ping (command: **-PA**). Active hosts will always respond with a RST packet.
- UDP ping (command: **-PU**). If the packet hits a closed port, the target will respond with an "ICMP port unreachable" packet.
- ICMP pings (commands: **-PE, -PP, -PM**). Nmap will send a packet with an echo request.
- IP protocol ping (command: **-PO**). Active hots will often send back responses using the same protocol as the nmap packet, or they will send an "ICMP port unreachable" packet.
- ARP scan (command: **-PR**). Nmap sends raw ARP requests.
- A combination of these techniques. By default, nmap will scan using ICMP, TCP SYN, and TCP ACK pings.

Task: Technical

9.) **Write a Scapy script in a language of your choice (python recommended) or command(s) to send network traffic similar to the following nmap command. *Scapy must receive the correct answers from the targets, same as if nmap was used.***

Please see attached text file (cs6573hw2-ewf215.txt) and pcap file (cs6573hw2-ewf215.pcap) for this script and the results of this scan.

10.) **You are looking for public vulnerabilities for a website which participates in a bug bounty program.**

a. **What subdomain is out of scope regarding open redirects?**

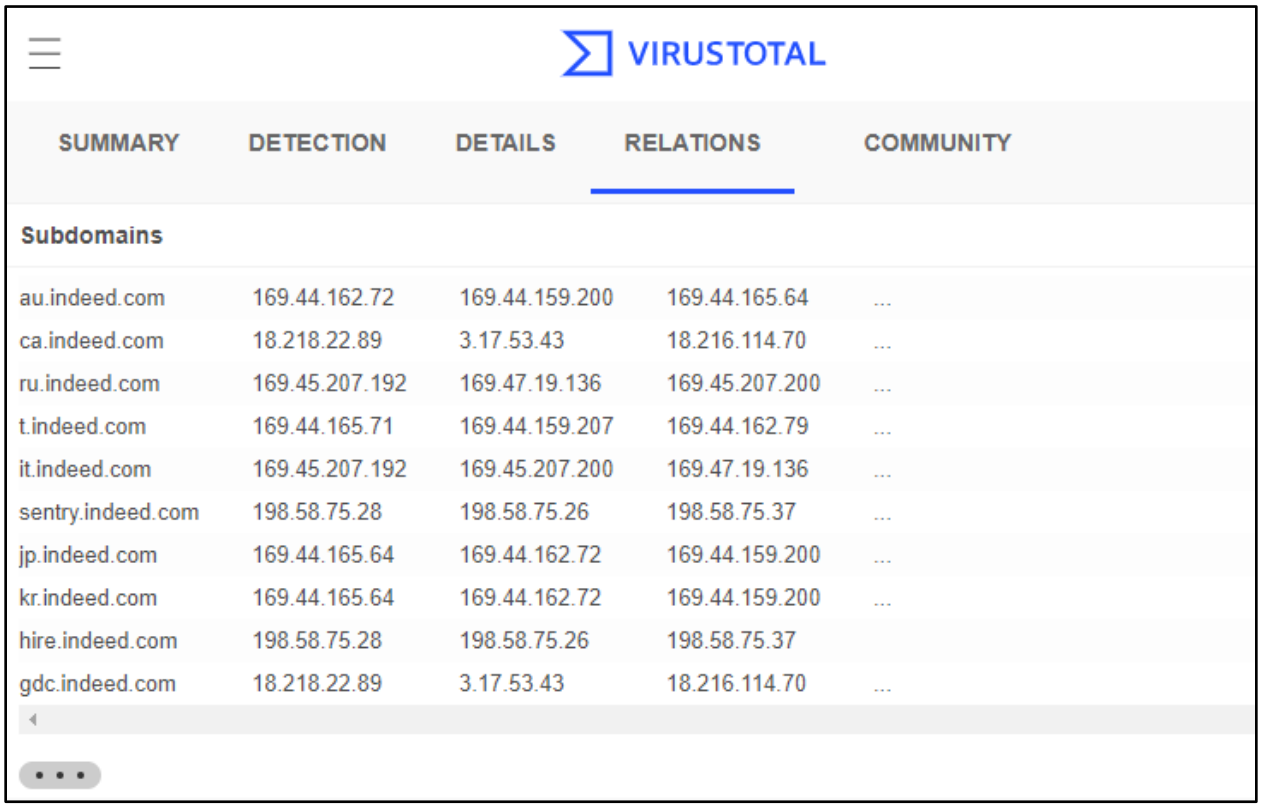
t.indeed.com is specifically cited to be out of scope.

b. **Using passive methods only, what subdomains can you find for indeed.com?**

I used several methods to find information about subdomains for indeed.com. I started by doing a Google search for "site.indeed.com" and I noticed that many Indeed subdomains included country codes (e.g., au.indeed.com).

Then I went to virustotal.com where I was able to gather a list of 100 subdomains. Please see Appendix I for results.

Screenshot 10b.1: **Virustotal.com findings.**



c. **From those subdomains, what unique IPs can you find?** ***Must have at least 25 and must be online.***

Among the results, I found numerous active, unique IPs. Highlighted items in Appendix I are active subdomains that do not timeout or resolve to an error.

d. **What netblocks are associated with the company and who owns them?**

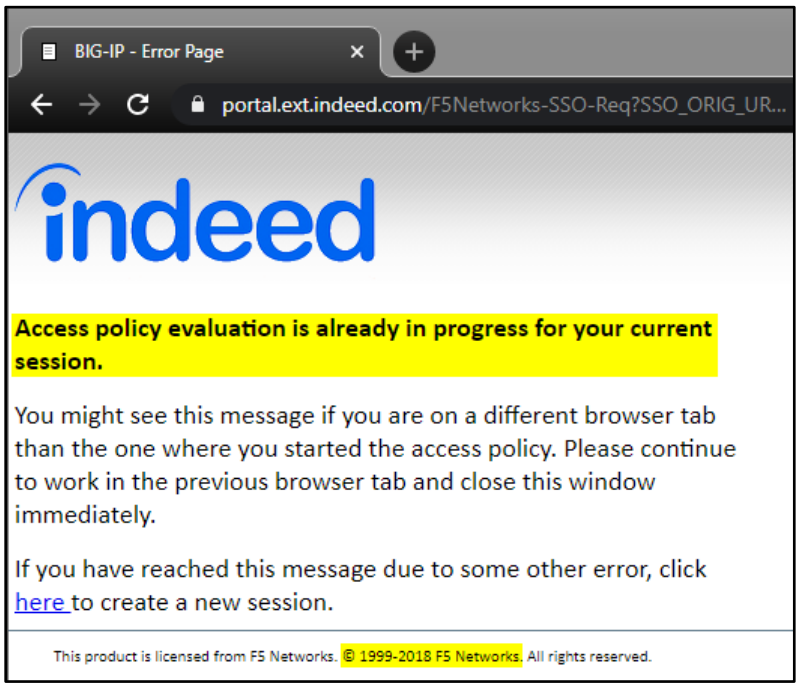
Table 10d.1: **Netblocks associated with indeed.com.**

CIDR address block	Company
18.128.0.0/9	Amazon Technologies Inc.
52.0.0.0/11	Amazon Technologies Inc.
13.52.0.0/14	Amazon Technologies Inc.
54.218.0.0/16	Amazon.com, Inc.
104.16.0.0/12	Cloudflare Inc.
198.58.75.0/25	CyrusOne Inc.
76.77.155.128/29	CyrusOne Inc.
35.208.0.0/12	Google
35.224.0.0/12	Google
35.240.0.0/13	Google
45.33.0.0/17	Linode
199.15.212.0/22	Marketo Inc.
192.28.144.0/20	Marketo Inc.
110.0.0.0/8	RackCorp
162.13.0.0/16	Rackspace Inc.
169.44.165.64/29	Softlayer Technologies, Inc. (IBM Cloud)

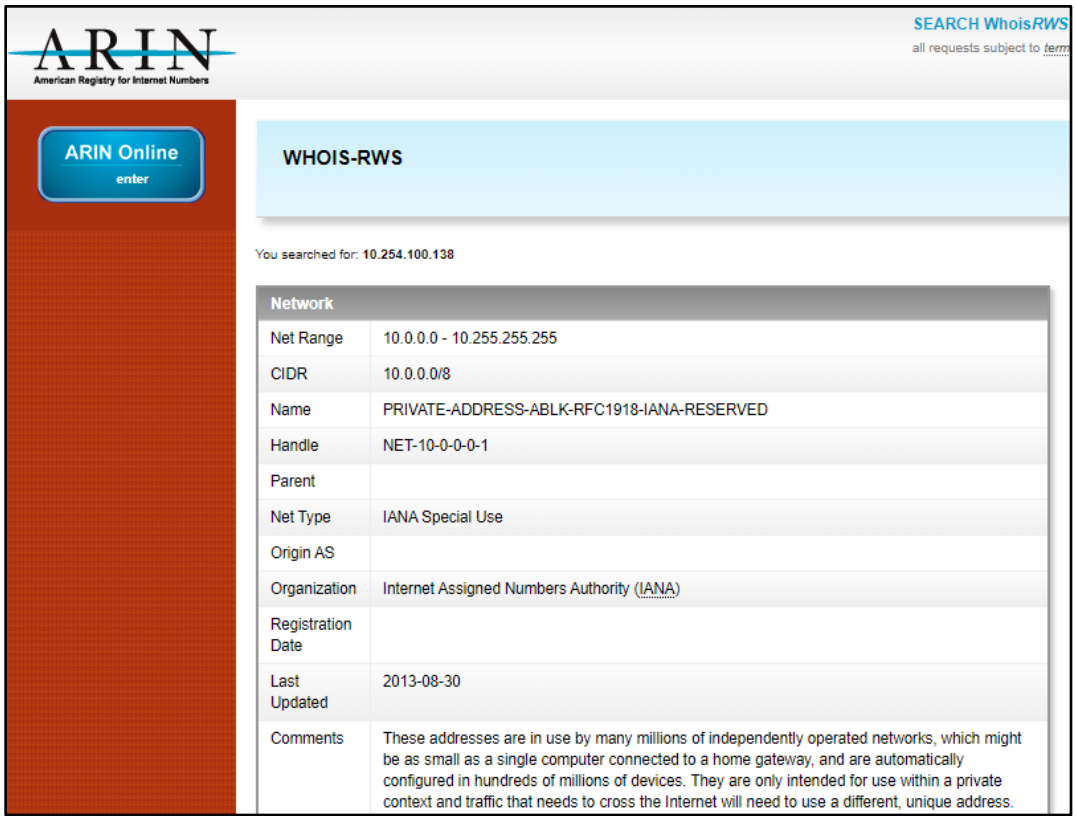
e. Using a **non-aggressive method** we covered in class, such as Google dorking, polite recon-ng modules, or Eyewitness, find at least one endpoint, service, or exposure that could be used for future research or testing. For example, an API that doesn't require a key/token, an interesting file, error page, service, etc. It does not have to be a proven vulnerability, just something that should be researched more as we enumerate the attack surface. Prove the method and findings.

Within the list of subdomains collected, I noticed two private IP addresses (marked below in red in Appendix I). Upon investigation via EyeWitness and Whois, and by navigating to one of the subdomains (mechabugs.indeed.com), I found several interesting items: The rendered page contained the title "BIG-IP Error Page" and included a copyright notice for F5 Networks from 1999-2018, indicating that this site had not been updated in several years. Via Google, I searched for "BIG-IP Error Page" and discovered that BIG-IP is a software product owned by a company called F5. I searched through the F5 site for release notes (https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/releasenotes/product/relnote-bigip-11-6-4.html#rn_link_to_supplemental) about BIG-IP, including known issues, configurations, and updates. The release notes also contain contact information for F5 regional offices, which could be potentially useful for social engineering to gather more information about the BIG-IP product. More research would be necessary to discover whether any of these vulnerabilities currently exist and whether they pose risks to indeed.com

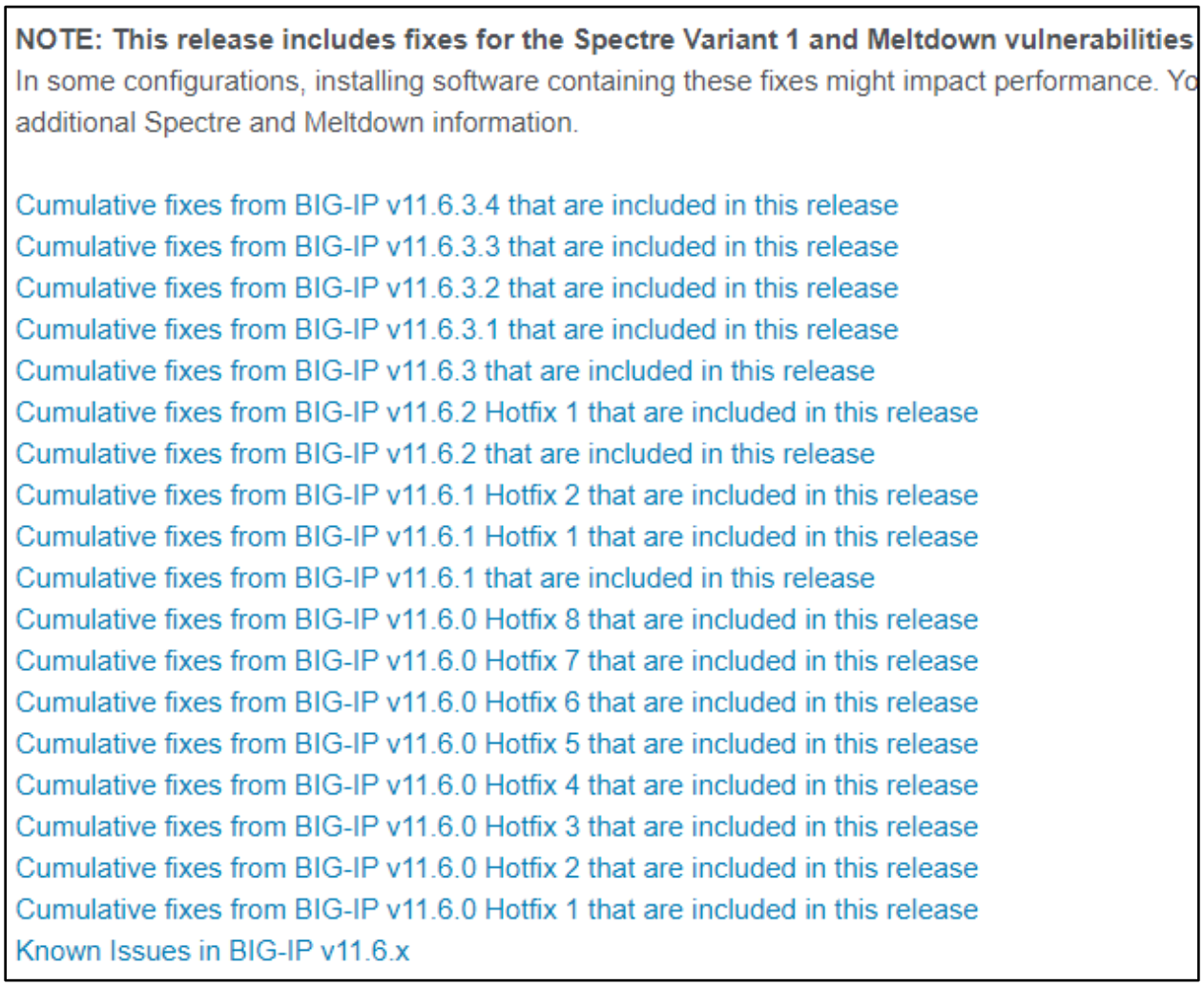
Screenshot 10e.1: Page displayed at mechabugs.indeed.com.



Screenshot 10e.2: Whois results for IP 10.254.100.138, which was found among list of subdomains.



Screenshot 10e.3: List of known fixes in BIG-IP, per release notes.



NOTE: This release includes fixes for the Spectre Variant 1 and Meltdown vulnerabilities
In some configurations, installing software containing these fixes might impact performance. Yo
additional Spectre and Meltdown information.

Cumulative fixes from BIG-IP v11.6.3.4 that are included in this release
Cumulative fixes from BIG-IP v11.6.3.3 that are included in this release
Cumulative fixes from BIG-IP v11.6.3.2 that are included in this release
Cumulative fixes from BIG-IP v11.6.3.1 that are included in this release
Cumulative fixes from BIG-IP v11.6.3 that are included in this release
Cumulative fixes from BIG-IP v11.6.2 Hotfix 1 that are included in this release
Cumulative fixes from BIG-IP v11.6.2 that are included in this release
Cumulative fixes from BIG-IP v11.6.1 Hotfix 2 that are included in this release
Cumulative fixes from BIG-IP v11.6.1 Hotfix 1 that are included in this release
Cumulative fixes from BIG-IP v11.6.1 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 8 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 7 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 6 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 5 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 4 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 3 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 2 that are included in this release
Cumulative fixes from BIG-IP v11.6.0 Hotfix 1 that are included in this release
Known Issues in BIG-IP v11.6.x

Screenshot 10e.4: List of known vulnerabilities in BIG-IP, per release notes.

Vulnerability Fixes

ID Number	CVE	Solution Article(s)	Description
757025-5	CVE-2018-5744	K00040234	BIND Update
739970-4	CVE-2018-5390	K95343321	Linux kernel vulnerability: CVE-2018-5390
757027-5	CVE-2019-6465	K01713115	BIND Update
745257-5	CVE-2018-14634	K20934447	Linux kernel vulnerability: CVE-2018-14634
643554-11	CVE-2017-3731 CVE-2017-3732 CVE-2016-7055	K37526132 K44512851 K43570545	OpenSSL vulnerabilities - OpenSSL 1.0.2k library update

References

[1] https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6?gi=72053991e318

[2] https://resources.infosecinstitute.com/masscan-scan-internet-minutes/#gref

[3] https://nmap.org/

[4] https://www.blackhat.com/docs/us-17/wednesday/us-17-McGrew-Protecting-Pentests-Recommendations-For-Performing-More-Secure-Tests-wp.pdf

[5] https://whois.arin.net/ui/

[6] https://www.virustotal.com

Appendix

I. Subdomain list for indeed.com:

secure.indeed.com	169.44.165.65	18.224.92.228	18.224.217.37
ads.indeed.com	198.58.75.63	64.9.168.152	198.58.75.52
my.indeed.com	169.44.165.67	3.18.9.149	13.59.96.6
subscriptions.indeed.com	18.218.201.2	3.16.32.78	13.58.145.233
it.indeed.com	169.45.207.192	169.45.207.200	169.47.19.136
au.indeed.com	169.44.162.72	169.44.159.200	169.44.165.64
gdc.indeed.com	18.218.22.89	3.17.53.43	18.216.114.70
sentry.indeed.com	198.58.75.28	198.58.75.26	198.58.75.37
ca.indeed.com	18.218.22.89	3.17.53.43	18.216.114.70
ie.indeed.com	169.47.19.136	169.45.207.192	169.45.207.200
de.indeed.com	169.47.19.136	169.45.207.200	169.45.207.192
jp.indeed.com	169.44.165.64	169.44.162.72	169.44.159.200
www.indeed.com	18.216.114.70	18.218.22.89	3.17.53.43
autocomplete.indeed.com	162.13.248.115	162.13.248.123	18.218.201.2
appsstatus.indeed.com	54.218.247.76	52.27.210.93	44.225.164.27
t.indeed.com (out of scope)	169.44.165.71	169.44.159.207	169.44.162.79
employers.indeed.com	198.58.75.26	198.58.75.28	198.58.75.23
hire.indeed.com	198.58.75.28	198.58.75.26	198.58.75.37
aq.indeed.com	3.17.53.43	18.218.22.89	18.216.114.70
apply.indeed.com	169.44.165.68	3.17.243.179	52.15.244.162
cpqa-employers.indeed.com	64.9.168.144	198.58.75.26	198.58.75.28
cts.indeed.com	198.58.75.26	198.58.75.28	198.58.75.37
profile-api.indeed.com	3.17.217.131		
support.indeed.com	104.16.53.111	104.16.55.111	104.16.51.111
bh.indeed.com	169.45.207.192	169.45.207.200	169.47.19.136
rss.indeed.com	169.44.165.64	18.218.22.89	3.17.53.43
conv.indeed.com	3.17.53.43	18.216.114.70	18.218.22.89
resumes.indeed.com	198.58.75.26	198.58.75.28	198.58.75.37
mail78.indeed.com	198.58.75.78		
se.indeed.com	169.45.207.192	169.47.19.136	169.45.207.200
ua.indeed.com	169.45.207.200	169.45.207.192	169.47.19.136
refer.indeed.com	52.73.62.123	34.193.246.244	34.231.88.193
idsync.indeed.com	198.58.75.26	198.58.75.28	198.58.75.37
blog.indeed.com	104.197.207.166	104.130.159.106	45.33.113.239
inbox.indeed.com	198.58.75.20	64.9.168.158	
cz.indeed.com	169.45.207.200	169.45.207.192	169.47.19.136
pa.indeed.com	18.216.114.70	3.17.53.43	18.218.22.89
pl.indeed.com	162.13.248.112	169.47.19.136	169.45.207.192
kr.indeed.com	169.44.165.64	169.44.162.72	169.44.159.200
at.indeed.com	169.45.207.200	169.45.207.192	169.47.19.136
us.dyn.indeed.com	3.17.53.43	18.216.114.70	18.218.22.89
es.indeed.com	169.45.207.192	162.13.248.120	162.13.248.104
co.indeed.com	18.218.22.89	18.216.114.70	3.17.53.43
slomo-qa.indeed.com	3.20.166.77	3.137.8.212	3.136.53.124
tw.indeed.com	169.44.162.72	169.44.165.64	169.44.159.200
employal-employers.indeed.com	64.9.168.144	198.58.75.28	198.58.75.26
api.indeed.com	18.218.22.89	3.17.53.43	18.216.114.70
resumecontacts.indeed.com	198.58.75.26	198.58.75.28	198.58.75.37
link.indeed.com	198.58.75.26	198.58.75.28	198.58.75.37
eg.indeed.com	169.47.19.136	169.45.207.192	169.45.207.200
no.indeed.com	162.13.248.112	169.47.19.136	169.45.207.192

tr.indeed.com	169.45.207.200	169.45.207.192	169.47.19.136
sydprod.indeed.com	110.232.117.116		
api-title-webapp.indeed.com	13.58.145.233	169.44.165.70	169.45.207.206
reportcontent.indeed.com	198.58.75.28	198.58.75.26	
to.indeed.com	198.58.75.28	198.58.75.26	198.58.75.37
lu.indeed.com	169.45.207.200	169.45.207.192	162.13.248.112
qa.indeed.com	169.45.207.200	169.47.19.136	169.45.207.192
be.indeed.com	169.47.19.136	169.45.207.200	169.45.207.192
sa.indeed.com	169.45.207.192	169.47.19.136	169.45.207.200
content.indeed.com	199.15.215.8	192.28.146.247	
gr.indeed.com	169.45.207.192	169.47.19.136	169.45.207.200
ru.indeed.com	169.45.207.192	169.47.19.136	169.45.207.200
interview.indeed.com	198.58.75.26	198.58.75.37	
smb-communication-employers.indeed.com	3.16.32.78	13.58.145.233	18.218.201.2
il.indeed.com	169.45.207.192	169.45.207.200	169.47.19.136
ar.indeed.com	3.17.53.43	18.218.22.89	18.216.114.70
screener-questions.indeed.com	169.44.159.206	169.44.162.78	169.44.165.70
seen.indeed.com	198.58.75.28	198.58.75.57	
tezjobs.indeed.com	198.58.75.28		
nz.indeed.com	169.44.165.64	169.44.162.72	169.44.159.200
employers-rezsearch.indeed.com	198.58.75.28	198.58.75.26	169.44.162.78
hero-employers.indeed.com	198.58.75.26	198.58.75.28	198.58.75.37
vn.indeed.com	169.44.165.64	169.44.159.200	169.44.162.72
ro.indeed.com	169.47.19.136	169.45.207.192	169.45.207.200
hu.indeed.com	169.47.19.136	169.45.207.192	169.45.207.200
redirects.indeed.com	18.189.253.57		
pet.indeed.com	13.58.145.233		
net.indeed.com	10.1.1.241		
js.indeed.com	192.28.157.112		
dyn4.indeed.com	3.17.53.43		
ng.indeed.com	169.45.207.192	169.45.207.200	169.47.19.136
adh.indeed.com	198.58.75.26		
indeedbot.indeed.com	198.58.75.46		
om.indeed.com	169.47.19.136	169.45.207.192	169.45.207.200
central.indeed.com	198.58.75.28		
dk.indeed.com	169.45.207.200	169.47.19.136	169.45.207.192
beseen.indeed.com	198.58.75.28	198.58.75.26	198.58.75.57
wiki.indeed.com	76.77.155.130	10.254.100.138	
kimoyo.indeed.com	198.58.75.28	198.58.75.26	198.58.75.37
sdp.indeed.com	198.58.75.26		
fisheye.indeed.com	10.254.100.11		
jsna.indeed.com	3.16.32.78	18.218.201.2	13.58.145.233
jsna-gw.indeed.com	35.234.144.2	35.193.123.18	
bugs.indeed.com	76.77.155.130	10.254.100.138	
mechabugs.indeed.com	76.77.155.130	10.254.100.138	
ma.indeed.com	169.45.207.200	169.47.19.136	169.45.207.192
resumejp.indeed.com	169.44.159.206	169.44.165.70	169.44.162.78
offers.indeed.com	104.17.74.206	104.17.71.206	104.17.72.206
kw.indeed.com	169.45.207.200	169.45.207.192	169.47.19.136

Bonus:


interview.indeed.com/private/poodlepants/
HTTP ERROR 404
Problem accessing /private/poodlepants/. Reason:
Not Found