

Cybersecurity Autumn 2023

Exercises Compendium

Magnus Christian Larsen

November 28, 2023

GitHub Username: Autowinto
Student Mail: magla21@student.sdu.dk
Project: <https://github.com/Autowinto/JHotDraw>
Date: mm/dd/yyyy

Contents

Info	3
Exercise 02: Starting the Journey	4
Thinking About Threats	4
Pentesting Intro	4
Exercise 03: General Assessment	7
Finding information with whois	7
Question: nmap	13
Comparing the Tools	13
Collecting the Assessment Information	14
Completing the Assessment	16
Exercise 04: SQL Injection	17
Preparation	17
Spying with SQL Injections	17
Elevation of Privilege	18
Using our Foot in the Door for Access to Other Services	19
Fully Explore Local Accounts	20
Post-Exploitation	21
Exercise 05: Drupal	22
Background	22
Post-Exploitation	22
Reflection	22
Exercise 06: Social Engineering	23
Defense	23
Experiment: Attack and Defend	23
Exercise 07: Brute Forcing Glassfish	25

Info

Questions marked in bold are the important questions for report.
Currently in doubt about format of final report. Layout will change.

Exercise 02: Starting the Journey

Thinking About Threats

Answers based on the following relevant articles:

- [Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email](#)
- [Mitigation for China-based threat actor activity](#)
- [Results of Major Technical Investigations for Storm-0558 Key Acquisition](#)

How did they separate access and infrastructure according to data relevance and impact?

They perform background checks, have dedicated identifiable accounts, secure access workstations and MFA using hardware token devices. They prevent the use of email and other communication tools which can compromise machines with malware or keylogs. They use Just in Time and Just Enough Access policies. They added the helper APIs, but failed to update relevant endpoint validation. Developers in other teams assumed that this validation was always performed and thus the disconnect happened.

How do roles and personnel fit into this, and which role could policies and training play?

Lack of evidence because of log retention policies. Because of a disconnect between team roles and personnel, validation was not performed.

Pentesting Intro

**Which advantages for penetration testing would you see in the different approaches?
What is the best option?**

- NAT
- NAT Networks
- Bridged Networking
- Host Only

**How does inspecting the ip configuration of a system help you with penetration testing?
What is the security relevant aspect?**

It does so by giving you info about all internet adapters, their protocols, their addresses, metrics, etc. etc.

How do you get the targeted user to execute our malicious payload?

Social Engineering, Disguising the file, exploiting vulnerabilities that allow for automatic code execution.

Is Metasploitable3 vulnerable to this exploit?

Testing the vulnerability is simple as connecting to the metasploitable vm and accessing sysinfo, verifying if it's correct. The vulnerability in this case, is an open nginx 8080 port, allowing us to connect. Metasploitable3 is very vulnerable to this exploit as it's designed to be so. It should close unused open ports, regularly update kernel and application versions, shut down unnecessary services and require validation before connection. It's quite easy to trick someone to download malicious files through torrenting, limewire, linkin-park-in-the-end.exe etc.

What is the practical use of this exercise? And why is the payload working in the way it is? How does this exercise relate to remote and reverse shells?

The practical use of this exercise is to see how easy it is to gain access to a vulnerable systems shell. The payload works how it does because

Which folder are you in when you get the meterpreter prompt? And what is the system-information?

I am in the folder that the payload.elf was run at

As user and the owner of this system – how would you mitigate this attack?

By not chmodding and running payloads which I don't know what are smh.

How does knowing usernames help an attacker/penetration tester?

It's a significant advantage as it allows you to brute-force passwords much faster and ensuring that you are actually on a user with specific permissions.

Now that you have access to the Metasploitable machine what else can we do? Get the list of users on this server, using a shell prompt by typing "shell" into the Meterpreter shell.

TODO

How does knowing usernames help an attacker/penetration tester?

It's a significant advantage as it allows you to brute-force passwords much faster and ensuring that you are actually on a user with specific permissions.

Using the meterpreter shell, check the output of the "arp" command. What do you find? Why could this information be relevant?

It displays internet-to-adaptor address tables and when you're connected to a target machine, it shows the tables for that machine, which is very useful information when trying to penetrate.

Now lets be on the other side of the fence and investigate suspicious connections to our metasploitable server. Which command can you use to see network status and connections? Is there an anomaly or suspicious connection to our server? What makes it suspicious?

Unexpected source ip addresses, data transfers when you aren't expecting any, HTTP traffic on an unexpected port etc.

Exercise 03: General Assessment

Finding information with whois

Listing 1: Output of whois for sdu.dk

```
1 # Hello 185.136.116.160. Your session has been logged.
2 #
3 # Copyright (c) 2002 – 2023 by DK Hostmaster A/S
4 #
5 # Version: 5.1.0
6 #
7 # The data in the DK Whois database is provided by DK Hostmaster A/S
8 # for information purposes only, and to assist persons in obtaining
9 # information about or related to a domain name registration record.
10 # We do not guarantee its accuracy. We will reserve the right to remove
11 # access for entities abusing the data, without notice.
12 #
13 # Any use of this material to target advertising or similar activities
14 # are explicitly forbidden and will be prosecuted. DK Hostmaster A/S
15 # requests to be notified of any such activities or suspicions thereof.
16
17 Domain:                sdu.dk
18 DNS:                   sdu.dk
19 Registered:            1997–10–09
20 Expires:                2023–12–31
21 Registration period:   5 years
22 VID:                   no
23 DNSSEC:                Signed delegation
24 Status:                Active
25
26 Registrant
27 Handle:                ***N/A***
28 Name:                  Syddansk Universitet (University of Southern
    Denmark)
29 Address:               Campusvej 55
30 Postalcode:            5230
31 City:                  Odense M
32 Country:               DK
33
34 Nameservers
35 Hostname:              ns1.sdu.dk
36 Hostname:              ns2.sdu.dk
37 Hostname:              ns3.sdu.dk
```

What do you learn about SDU's network? In the protocol, note the IP range.

We learn a whole lot about the network such as the date registered, the expiration date, address of registrant and hostnames.

Listing 2: Output of whois for the ip of sdu.dk

```

1
2 #
3 # ARIN WHOIS data and services are subject to the Terms of Use
4 # available at: https://www.arin.net/resources/registry/whois/tou/
5 #
6 # If you see inaccuracies in the results , please report at
7 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
8 #
9 # Copyright 1997–2023, American Registry for Internet Numbers, Ltd.
10 #
11
12
13 NetRange:      20.33.0.0 – 20.128.255.255
14 CIDR:          20.48.0.0/12 , 20.40.0.0/13 , 20.36.0.0/14 , 20.33.0.0/16 ,
15               20.34.0.0/15 , 20.128.0.0/16 , 20.64.0.0/10
16 NetName:       MSFT
17 NetHandle:     NET-20-33-0-0-1
18 Parent:       NET20 (NET-20-0-0-0-0)
19 NetType:       Direct Allocation
20 OriginAS:
21 Organization:  Microsoft Corporation (MSFT)
22 RegDate:       2017-10-18
23 Updated:       2021-12-14
24 Ref:          https://rdap.arin.net/registry/ip/20.33.0.0
25
26
27 OrgName:       Microsoft Corporation
28 OrgId:         MSFT
29 Address:       One Microsoft Way
30 City:          Redmond
31 StateProv:     WA
32 PostalCode:    98052
33 Country:       US
34 RegDate:       1998-07-10
35 Updated:       2023-06-13
36 Comment:       To report suspected security issues specific to traffic
                 emanating from Microsoft online services , including the distribution
                 of malicious content or other illicit or illegal material through a
                 Microsoft online service , please submit reports to:
37 Comment:       * https://cert.microsoft.com.
38 Comment:
39 Comment:       For SPAM and other abuse issues , such as Microsoft
                 Accounts , please contact :
40 Comment:       * abuse@microsoft.com.
41 Comment:

```


42 Comment: To report security vulnerabilities in Microsoft products
 and services , please contact :
 43 Comment: * secure@microsoft.com.
 44 Comment:
 45 Comment: For legal and law enforcement-related requests , please
 contact :
 46 Comment: * msndcc@microsoft.com
 47 Comment:
 48 Comment: For routing , peering or DNS issues , please
 49 Comment: contact :
 50 Comment: * IOC@microsoft.com
 51 Ref: https://rdap.arin.net/registry/entity/MSFT
 52
 53
 54 OrgAbuseHandle: MAC74-ARIN
 55 OrgAbuseName: Microsoft Abuse Contact
 56 OrgAbusePhone: +1-425-882-8080
 57 OrgAbuseEmail: abuse@microsoft.com
 58 OrgAbuseRef: https://rdap.arin.net/registry/entity/MAC74-ARIN
 59
 60 OrgTechHandle: SINGH683-ARIN
 61 OrgTechName: Singh , Prachi
 62 OrgTechPhone: +1-425-707-5601
 63 OrgTechEmail: pracsin@microsoft.com
 64 OrgTechRef: https://rdap.arin.net/registry/entity/SINGH683-ARIN
 65
 66 OrgTechHandle: BEDAR6-ARIN
 67 OrgTechName: Bedard , Dawn
 68 OrgTechPhone: +1-425-538-6637
 69 OrgTechEmail: dabedard@microsoft.com
 70 OrgTechRef: https://rdap.arin.net/registry/entity/BEDAR6-ARIN
 71
 72 OrgTechHandle: IPHOS5-ARIN
 73 OrgTechName: IPHostmaster , IPHostmaster
 74 OrgTechPhone: +1-425-538-6637
 75 OrgTechEmail: iphostmaster@microsoft.com
 76 OrgTechRef: https://rdap.arin.net/registry/entity/IPHOS5-ARIN
 77
 78 OrgRoutingHandle: CHATU3-ARIN
 79 OrgRoutingName: Chaturmohta , Somesh
 80 OrgRoutingPhone: +1-425-882-8080
 81 OrgRoutingEmail: someshch@microsoft.com
 82 OrgRoutingRef: https://rdap.arin.net/registry/entity/CHATU3-ARIN
 83
 84 OrgTechHandle: MRPD-ARIN
 85 OrgTechName: Microsoft Routing , Peering , and DNS
 86 OrgTechPhone: +1-425-882-8080
 87 OrgTechEmail: IOC@microsoft.com

```

88 OrgTechRef:      https://rdap.arin.net/registry/entity/MRPD-ARIN
89
90
91 #
92 # ARIN WHOIS data and services are subject to the Terms of Use
93 # available at: https://www.arin.net/resources/registry/whois/tou/
94 #
95 # If you see inaccuracies in the results , please report at
96 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
97 #
98 # Copyright 1997–2023, American Registry for Internet Numbers, Ltd.
99 #

```

The IP range is 20.33.0.0 - 20.128.255.255

What is the whois information for nextcloud.sdu.dk? What do you observe in comparison to the whois-information you gathered for www.sdu.dk

Listing 3: Output of whois for nextcloud.sdu.dk

```

1
2 #
3 # ARIN WHOIS data and services are subject to the Terms of Use
4 # available at: https://www.arin.net/resources/registry/whois/tou/
5 #
6 # If you see inaccuracies in the results , please report at
7 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
8 #
9 # Copyright 1997–2023, American Registry for Internet Numbers, Ltd.
10 #
11
12
13 NetRange:      130.225.0.0 – 130.244.255.255
14 CIDR:         130.225.0.0/16 , 130.226.0.0/15 , 130.228.0.0/14 ,
15              130.244.0.0/16 , 130.240.0.0/14 , 130.232.0.0/13
16 NetName:      RIPE-ERX-130-225-0-0
17 NetHandle:    NET-130-225-0-0-1
18 Parent:      NET130 (NET-130-0-0-0-0)
19 NetType:      Early Registrations , Transferred to RIPE NCC
20 OriginAS:
21 Organization: RIPE Network Coordination Centre (RIPE)
22 RegDate:     2003-11-12
23 Updated:     2003-11-12
24 Comment:     These addresses have been further assigned to users in
25              the RIPE NCC region. Contact information can be found
26              in
27 Comment:     the RIPE database at http://www.ripe.net/whois
28 Ref:         https://rdap.arin.net/registry/ip/130.225.0.0

```

```

28 ResourceLink:  https://apps.db.ripe.net/search/query.html
29 ResourceLink:  whois.ripe.net
30
31
32 OrgName:       RIPE Network Coordination Centre
33 OrgId:         RIPE
34 Address:       P.O. Box 10096
35 City:          Amsterdam
36 StateProv:
37 PostalCode:    1001EB
38 Country:       NL
39 RegDate:
40 Updated:       2013-07-29
41 Ref:           https://rdap.arin.net/registry/entity/RIPE
42
43 ReferralServer: whois://whois.ripe.net
44 ResourceLink:  https://apps.db.ripe.net/search/query.html
45
46 OrgAbuseHandle: ABUSE3850-ARIN
47 OrgAbuseName:   Abuse Contact
48 OrgAbusePhone:  +31205354444
49 OrgAbuseEmail:  abuse@ripe.net
50 OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE3850-ARIN
51
52 OrgTechHandle:  RNO29-ARIN
53 OrgTechName:    RIPE NCC Operations
54 OrgTechPhone:   +31 20 535 4444
55 OrgTechEmail:   hostmaster@ripe.net
56 OrgTechRef:     https://rdap.arin.net/registry/entity/RNO29-ARIN
57
58
59 #
60 # ARIN WHOIS data and services are subject to the Terms of Use
61 # available at: https://www.arin.net/resources/registry/whois/tou/
62 #
63 # If you see inaccuracies in the results, please report at
64 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
65 #
66 # Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
67 #
68
69
70
71 Found a referral to whois.ripe.net.
72
73 % This is the RIPE Database query service.
74 % The objects are in RPSL format.
75 %

```

```

76 % The RIPE Database is subject to Terms and Conditions.
77 % See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions
78
79 % Note: this output has been filtered.
80 %       To receive output for a database update, use the "-B" flag.
81
82 % Information related to '130.225.128.0 - 130.225.159.255'
83
84 % Abuse contact for '130.225.128.0 - 130.225.159.255' is 'abuse@cert.dk'
85
86 inetnum:          130.225.128.0 - 130.225.159.255
87 netname:          SDU-v4-POOL-01
88 country:          DK
89 geofeed:          https://info.net.deic.dk/deic-geofeed.csv
90 org:              ORG-SUI1-RIPE
91 admin-c:          UN61-RIPE
92 tech-c:           UN61-RIPE
93 status:           ASSIGNED PA
94 remarks:          Generated by DeIC on 2022-07-28 for more information
95                   contact netdrift@deic.dk
96 mnt-by:           DEIC-MNT
97 mnt-by:           AS1835-MNT
98 created:          2015-12-10T10:05:14Z
99 last-modified:    2022-07-28T11:50:21Z
100 source:          RIPE
101
102 organisation:     ORG-SUI1-RIPE
103 org-name:          Syddansk Universitet, IT-service
104 org-type:          other
105 address:           Campusvej 55
106 address:           5230 Odense M
107 address:           DK
108 mnt-ref:           AS1835-MNT
109 mnt-by:            AS1835-MNT
110 mnt-by:            DEIC-MNT
111 created:           2012-05-03T10:51:17Z
112 last-modified:    2022-01-28T14:00:25Z
113 source:           RIPE # Filtered
114
115 role:             DeIC Netdrift
116 address:          DeIC
117 address:          DTU Building 304
118 address:          2800 Lyngby
119 address:          Denmark
120 phone:            +45 35 888 222
121 fax-no:           +45 35 888 201
122 admin-c:          AMD2-RIPE
123 tech-c:           AMD2-RIPE

```

```

123 tech-c:          JF6044-RIPE
124 tech-c:          HUB10-RIPE
125 nic-hdl:         UN61-RIPE
126 mnt-by:          AS1835-MNT
127 mnt-by:          DEIC-MNT
128 created:         2008-11-24T13:12:55Z
129 last-modified:   2022-01-28T14:00:26Z
130 source:          RIPE # Filtered
131 abuse-mailbox:   abuse@cert.dk
132
133 % Information related to '130.225.0.0/16 AS1835'
134
135 route:           130.225.0.0/16
136 descr:           Forskningsnettet -130.225
137 origin:          AS1835
138 mnt-by:          AS1835-MNT
139 mnt-by:          DEIC-MNT
140 created:         1970-01-01T00:00:00Z
141 last-modified:   2022-01-28T14:00:18Z
142 source:          RIPE
143
144 % This query was served by the RIPE Database Query Service version 1.108
    (BUSA)

```

The IP range is 130.225.128.0 - 130.225.159.255 for one.

In addition, the output is much more detailed without having to query the ip address instead of the website name.

Question: nmap

Nmap scans can be set up to evade firewalls. Which tags would you use for sending packets with specified ip options?

To do that you would use `-ip-options` with one of several options such as "R" to set a record route.

Nmap scans can be set up to evade firewalls. Which tags would you use for spoofing your MAC address?

In that case I would use the tag `-spoof-mac` with either a specific mac address or 0 passed to use a random one.

Comparing the Tools

Compare your results from each of the previous activities in each question (e.g., sparta vs nessus vs openvas). Take notes and discuss overlaps and differences in results, pros and cons, ease of use for each tool.

GVM, NESSUS, LEGION, METASPLOITABLE VMs

Collecting the Assessment Information

Collecting assessment information for 4 services requires us to first find an

Listing 4: \$ ip a

```
1 | 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
   | group default qlen 1000
2 |     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
3 |     inet 127.0.0.1/8 scope host lo
4 |         valid_lft forever preferred_lft forever
5 |     inet6 ::1/128 scope host noprefixroute
6 |         valid_lft forever preferred_lft forever
7 | 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
   | UP group default qlen 1000
8 |     link/ether 08:00:27:9c:dc:cd brd ff:ff:ff:ff:ff:ff
9 |     inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute
   |         eth0
10 |         valid_lft 496sec preferred_lft 496sec
11 |     inet6 fe80::f5eb:f6c5:4289:b43a/64 scope link noprefixroute
12 |         valid_lft forever preferred_lft forever
```

Under the second internet adapter listing eth0, we can see that the inet range is 10.0.2.4/24

Service, port number and version number, e.g., FTP 21 vxxxxx

Listing 5: \$ nmap -sn 10.0.2.4

```
1 | Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-08 06:38 EST
2 | Nmap scan report for 10.0.2.1
3 | Host is up (0.00074s latency).
4 | Nmap scan report for 10.0.2.4
5 | Host is up (0.00059s latency).
6 | Nmap scan report for 10.0.2.15
7 | Host is up (0.00054s latency).
8 | Nmap done: 256 IP addresses (3 hosts up) scanned in 2.98 seconds
```

Running nmap finding ports we find that 10.0.2.15 has a lot of vulnerabilities

Listing 6: \$ nmap -sV -p- 10.0.2.15

```
1 | Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-08 06:47 EST
2 | Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Connect
   | Scan
3 | Connect Scan Timing: About 41.49% done; ETC: 06:50 (0:01:15 remaining)
4 | Nmap scan report for 10.0.2.15
5 | Host is up (0.00073s latency).
6 | Not shown: 65524 filtered tcp ports (no-response)
7 | PORT      STATE SERVICE      VERSION
8 | 21/tcp    open  ftp          ProFTPD 1.3.5
9 | 22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu
   | Linux; protocol 2.0)
```

```

10 | 80/tcp    open    http      Apache httpd 2.4.7
11 | 445/tcp   open    netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
12 | 631/tcp   open    ipp       CUPS 1.7
13 | 3000/tcp  closed  ppp
14 | 3306/tcp  open    mysql     MySQL (unauthorized)
15 | 3500/tcp  open    http      WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
16 | 6697/tcp  open    irc       UnrealIRCd
17 | 8080/tcp  open    http      Jetty 8.1.7.v20120910
18 | 8181/tcp  closed  intermapper
19 | Service Info: Hosts: 127.0.1.1, UBUNTU, irc.TestIRC.net; OSs: Unix,
    | Linux; CPE: cpe:/o:linux:linux_kernel
20 |
21 | Service detection performed. Please report any incorrect results at
    | https://nmap.org/submit/ .
22 | Nmap done: 1 IP address (1 host up) scanned in 112.01 seconds

```

We select the four vulnerabilities:

- FTP, 21 ProFTPD 1.3.5
- SSH, 22, OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
- HTTP, 80, Apache httpd 2.4.7
- IPP, 631, CUPS 1.7

Describe or explain at least one vulnerability that you found for that service, i.e., what is the underlying issue and what can be achieved? How severe is that issue? (You do not have to state how to exploit the vulnerability or go into technical details. We will look into this later btw. The intricate technicalities are mostly outside the scope of the course.) But make sure you describe what possible outcomes of the exploit are, what the impact for a real system were and how critical you would assess the issue due to the effects, i.e., argue for your assessment

TODO

For each of the vulnerabilities in the previous point, note the CVE and/or Source of information about the vulnerability for that version. Using metasploit's info command might help you here, if you want to go to the command line.

TODO

Completing the Assessment

Create a final report, extending the collected information with an overall review of the security concerns in both the Metasploitable-3 Windows and Ubuntu systems, e.g., different criticality levels of the services (an overview of how bad the situation is) and which ones to be prioritized when addressing security issues (a selection of the most relevant issues for prioritisation). For this use a combination of the results from the tools that you used or one of the tools. Note, that you shouldn't just copy and paste the severity of the tools you use, but read through the CVE you selected and try to determine how critical it is. I.e., what is the possible impact? Is the service inoperable, or is intellectual property at risk?

TODO

Exercise 04: SQL Injection

Preparation

try command `mysql -h <METAPLOITABLE IP> -P 3306`

Nessus does say it was unable to get version number for the MySQL server because it is restricted.

Does it mean the MySQL server is protected against cyber attacks?

It doesn't necessarily mean that the server is protected against attacks. Restricting the version number is one security measure, but it doesn't mean that the entire server is secure from any and all exploits.

How could that protection look like?

Protection against cyberattacks could be things like using strong passwords, restricting access to only certain users or groups, using TLS encryption, disabling unnecessary features in the MySQL server, logging access to the server, updating to the latest versions and security patches frequently, setting up a firewall etc.

And what exactly would it protect against?

Hiding the version-number protects against exploits that are available for certain versions of the MySQL server, while making use of general best-practices when it comes to security configuration, ensures that the amount of available exploits are minimized.

Spying with SQL Injections

Please shortly discuss your opinion of this web server's configuration concerning directory listings

Directory listings should always be disabled for public websites, as it gives potential bad actors access to information about potential vulnerabilities and files that no user would need access to.

What type of SQLi attack works? Can you explain why?

Out of the four options presented, the SQL injection attack that will work, is 'OR 1=1#. The reason for this, is because the beginning single quote terminates any string, meaning that SQL will now interpret anything after the single quote, as proper SQL statements. After the single quote, the statement OR 1=1, which is of course always a statement and makes the SQL statement always true, giving us the ability to fetch all data in a table for example.

What is the # sign for? Can we generally assume it to do the trick?

A # symbol denotes the beginning of a comment, which in the context of an SQL injection attack, effectively has the purpose of ignoring any other SQL that might come after our injection, as we don't really care about that and it reduces the risk of some check being run.

Include four relevant username/password combinations in your report. What is the issue with the passwords in the database and what could be done to secure them?

Relevant username and password combinations extracted would be:

ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:(
jarjar_binks	mesah_p@ssw0rd

Which other problem allows you to get into the machine using ssh? How could this be prevented?

The fact that I can access the SSH server without having setup a valid SSH key is alarming and should be addressed. You shouldn't be able to access an SSH server with a username and password combination only.

Elevation of Privilege

Which are the individual issues that allowed us to go from a web interface to root access, and how would you address them as a server's operator to prevent them being exploited? Describe the issues you identified and try to come up with suggestions on how to fix them

There were several issues. Below I'll list the issues and explain how I would go about fixing these issues.

- The directory listing should never be available publicly. In fact, there is very little reason why it should ever be available. Therefore, this should be made unavailable.
- Backend is prone to SQL injection attacks. The backend server should validate the incoming requests, especially when raw SQL is involved, so it isn't as prone to SQL injection attacks as what it clearly is.
- SSH server accepts plain username and passwords to connect. SSH server should require a valid SSH key to access. Additionally, the SSH server should only be allowed to connect to from specific IP addresses to limit the potential bad actors.

Can SQL Injection expose an otherwise inaccessible database server?

So long as there is a way to perform input towards an SQL server, it's possible to expose a database to potentially being attacked. It's all a matter of how well protected the backend accessing the database server is.

How likely do you think an attack scenario as presented here is?

This specific scenario is extremely unlikely today. For us to have this easy of access to an SSH server with root privileges even, a perfect storm of security vulnerabilities would need to be available to us. The only reason we have access to all of these vulnerabilities, are because of the metasploitable3

VM, made specifically to have these vulnerabilities available. In the real world, it wouldn't be so easy.

Using our Foot in the Door for Access to Other Services

Is sudo necessary? What do we gain by using it?

Using sudo specifies the command to be run with root privileges, allowing us to view the location of all files containing the payroll name that we are searching for, no matter what folder it's in. We can find files in other users' owned folders as well as folders in root owned directories like this. While not strictly necessary, it does make for a more complete search, and in this case, allows us to find the file we're looking for.

Are there other ways to search for a file? Which do you know?

There exist several commands to search for files.

- find: The command we used previously.
- grep: Used to search for text within files primarily.
- ls | grep: ls used together with piping the result to grep allows for searches.
- Fuzzy finders: Fuzzy finders allow for searching in both file contents and searching for file names.

Can you find anything interesting?

Performing the cat command shows us the contents of payroll.php. The file especially contains something interesting, in that the connection details aren't contained in some environment variables or something other. They are fully exposed, allowing us a full backdoor to the mysql database.

Listing 7: The payroll.php file

```
1 | $conn = new mysqli('127.0.0.1', 'root', 'sploitme', 'payroll');
2 | if ($conn->connect_error) {
3 |     die("Connection failed: " . $conn->connect_error);
4 | }
```

Interesting information that we can obtain from this are the username, password, hostname as well as the database name.

What's the username, password and database name?

- Hostname: 127.0.0.1 / localhost
- Username: root
- Password: sploitme
- Database Name: payroll

What was the problem with the web application?

The problem with the web application is that it's accepting user input as string concatenation, which makes it very easy to perform SQL injection.

Which ports and services were the problem associated with?

We were able to access the directory listing through the exposed port 80 nginx service, which had directory listing enabled.

How did you exploit the vulnerability?

The exposed directory listing allowed us to access the payroll.php application and exploit the SQL injectable web application.

And what were you able to do?

Through use of said exploit, I was able to gain access to SSH usernames and passwords and be able to gain access to not only the SSH server, but root access, allowing us to see the entire payroll.php file and gain information on how to gain direct database access.

How would you suggest to fix the problem? (Do some online research about SQL injections solutions.)

Based on my research, the correct way to fix an SQL injection vulnerability, is to separate the SQL from the data itself and "prepare" the data before being used in the query. In the context of the existing payroll.php application, which uses MySQLi to perform its queries, it should make use of the `execute_query()` function, which allows you to define a SQL statement and insert the user input as variables. This way, the variables are prepared properly.

Draft a shortly and crisply, the relevant parts of a policy trying to prevent these issues.

The policy to prevent these issues will sound as follows:

All database queries must be performed using prepared statements of parameters, so as to protect against SQL injections. Additionally, user input should be validated on the frontend, as well as validated and sanitized on the backend. Database connection details should be fetched from some encrypted environment variables or something similar, to not expose these variables to the eyes of potential bad actors. Systems should regularly be updated and patched to avoid some of the most serious vulnerabilities. Finally, staff should undergo periodic training to ensure that these standards are upheld.

Fully Explore Local Accounts

What are benefits of performing this scan after already having full access?

The benefits of performing the scan with full access can be, just that. Having full access and potentially discovering new passwords and usernames to crack. By having root access, we already have access to a potential multitude increase in directories that we can scan for vulnerable passwords, which allows the scan to be potentially much more effective.

Post-Exploitation

Thinking as an attacker, what would your next steps be?

First, I would seek to gain some sort of persistence, meaning that even if I was discovered and the system restarted, I could still have access to the machine. This would be in the form of some sort of backdoor.

Since I already have root access, I don't need to work towards gaining increased access, however, I would install tools which allow me to gain increased information.

Having access to one machine on a network, I would try to discover additional machines that I could access, which could potentially gain me access to even more information. I would do all of this while making sure to leave as few logs as possible, so I wasn't discovered.

As an operator, what would you do to counteract?

After discovering that an attack is underway, my first

Exercise 05: Drupal

Background

Which vulnerabilities do you think can be used? Pick two potential vulnerabilities and describe them in terms of why you picked them, i.e., date and exploit effect.

For the rest of the tutorial, we will use the vulnerability *dubbed drupageddon*. What is the underlying vulnerability?

What is so severe about the issue?

Post-Exploitation

What are possible activities/aims for the post-exploitation phase?

Write out the list in the file that has the “User Accounts”?

How does having a list of user names help?

What do the excellent post exploitation scripts for linux offer?

Reflection

What is the main issue with the web server? How did it help selecting potential exploits?

When opening the drupal web page, you are greeted by a warning. Do you think this is good practice? Why or why not?

Given a more restrictive web server configuration, finding the relevant information wouldn't have been that easy. Please check dirbuster, to be found in the “Web Application Analysis” menu. How could this tool help you finding information? Try it out on the Ubuntu metasploitable VM. Use `/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt` as dictionary.

How can effective spying with tools like dirbuster prevented?

This attack didn't get us all the way to root. How would you continue the pentest? What would be your next actions?

Do you have any specific things in mind you would try to get root access?

What makes getting a remote shell so powerful?

Exercise 06: Social Engineering

Defense

Which technical tools can be used to defend against social engineering attacks and against which?

- Email filtering software
 - **Functionality:** The software scans incoming emails for potential phishing attempts or malicious contents, resulting in many obvious attempts at malicious activity being filtered.
 - **Protects against:** Protects the user against phishing and email scams such as impersonation attempts.
- MFA systems
 - **Functionality:** Adds an additional layer of security by forcing the user to input a dynamically generated code as well as their password when signing in.
 - **Protects against:** Protects the user against password leaks, insecure passwords etc.
- Antivirus software
 - **Functionality:** Scans systems and programs for known malicious code and quarantines files before they can gain access to or change a system.
 - **Protects against:** Protects against viruses, malware, spyware and trojans.
- User roles and PAM
 - **Functionality:** User roles allow an organization to specify that a user only has access to very specific things in the organization portals and the entire PAM system monitors access to resources and logs attempts at unauthorized access.
 - **Protects against:** Helps mitigate damage of social engineering attacks by limiting access to resources if access to a user account is obtained.

Give examples on how you, as IT-experts, can either stop or mitigate Social Engineering.

Some ways of stopping or mitigating damage from Social Engineering attacks are as follows:

- Implementing strong organizational security policies and ensuring that every employee within the organization is trained to follow these policies and procedures.
- Controlling access to the physical organization by unauthorized personnel by implementing security badges, key cards, biometric systems etc.
- Implementing phishing detection tools and ensuring regular employee phishing tests, allowing them to fail without catastrophic failure ensuing.

Experiment: Attack and Defend

The experiment was performed in a small group.

DAN is a quiet reserved loner. He's trusting, good-natured and lenient. He's conscientious, hard-working, well-organized and punctual. He's calm, even-tempered, comfortable and unemotional. He's down to earth, uncreative, conventional and uncurious.

Attacker's Perspective

Based off the information provided about DAN, we believe that the proper course of action to socially engineer him would be an email phishing scam, making use of his trusting and well-organized traits by impersonating the danish tax ministry asking him to update his advance statement to ensure correct tax calculations.

Impersonating an authority figure will let us make use of his calm, unemotional and curious nature as well, as these traits make him unlikely to seek out a second opinion, especially considering tax season beginning around november.

Defender's Perspective

The course designed to train DAN on how to avoid being socially engineered needs to cater specifically to his weaknesses. Therefore, the curriculum is as follows:

- How to efficiently make use of firewalls, anti-phishing tools and spam filters.
- Instilling several rules of thumb in DAN and his way of navigating the workspace:
 - Official government communication will never include asking for personal information or direct links to signup pages.
 - Make use of multi-factor-authentication wherever available.
 - Involve coworkers or supervisors whenever there's any doubt about the validity of emails.

Comparing the strategies, improve on attack and defence

Exercise 07: Brute Forcing Glassfish

What does HTTPS actually provide protection for?

HTTPS is primarily used for ensuring a secure connection between client and server, by implementing TLS and that way protecting from man-in-the-middle attacks.

Which username/password combination did you find?

After running the glassfish_login exploit, the username and password combinations that works is admin and sploit respectively. Of course, the passwords would realistically be much stronger than simply admin and sploit.

Discuss which security relevant problems are we testing with a brute force attack?

With a brute force attack, we are testing for weak passwords, lack of multi-factor-authentication within the organization, as well as external ip addresses being allowed to sign in.

Discuss what would be your suggestions to the admin in order to address and mitigate this issue?

One thing that the admin could do is use stronger passwords, this however, doesn't help in the case of a password leak to some database. Therefore, another thing that the admin could do, is introduce multi-factor-authentication when signing in to relevant organization accounts. Additionally, restricting access to specific IP addresses localized where the organization is physically located or allowing access through a specific VPN would go a long way to mitigate this issue.

How is this attack type related to the internet of things, internet routers, and, e.g., virtual machines?

Brute force attacks relate to the three mentioned platforms in the following ways:

- **Internet of Things (IoT)** Many IoT devices, such as cameras, smart devices and more, often come with default credentials set, which are usually readily available online. This makes these the perfect target for brute force attacks, as most users don't bother changing the default credentials.
- **Internet Routers** Internet routers suffer the same issue as IoT devices, as again, routers come with default passwords, which many people don't bother setting. If an intruder is even able to gain physical access to the router, an ethernet cable can be used to open ports without the need of Wi-Fi passwords.
- **Virtual Machines** Just like with the previous two, many virtual machines come with default passwords, (for example the Kali Linux image that we're using for this course), which allows for potential easy access via brute force attacks. Especially if said virtual machines allow for remote access.

Do you know a way in which HTTPS could make the connection more secure against this kind of attack?

While HTTPS doesn't protect against brute force attacks in and of itself, it does so indirectly, by encrypting all data access, securing login pages and ensuring that the server that the user is

communicating with is actually the server that it says it is. This makes it much harder for a malicious entity to perform man-in-the middle attacks and makes it harder for passwords to leak onto potential databases which can be used to brute force.

Threat Modelling

A Simple Data Flow Diagram

Formulate STRIDE

Discuss your Data Flow Diagram & STRIDE

- *Create a data flow diagram*
Please do not worry too much about the exact way the data flow diagram is created, you can find a lot of information online which is adding more detail than we need. Focus on where the data travels and use the literature provided as inspiration.
- *Formulate STRIDE*
For each of the categories, describe at least 2 threats based on your data flow diagram, putting them down in a list or table.

Update Flow Diagram & STRIDE

Discuss your Updated Data Flow Diagram & STRIDE

- *Create a data flow diagram*
Please do not worry too much about the exact way the data flow diagram is created, you can find a lot of information online which is adding more detail than we need. Focus on where the data travels and use the literature provided as inspiration.
- *Formulate STRIDE*
For each of the categories, describe at least 2 threats based on your data flow diagram, putting them down in a list or table.