

Forum:[Hack Forums](#)

Thread: [ssh/22 script python domains attack](#)

barbel - November 2, 2025, 11:13 am

hello,

i want to briefly explain if someone is available and able to make a simple functional python script that tries to connect via ssh/22 to domains.

i need a python script that can connect to a list of domains: domains.txt which are one under the other on ssh/22 with user which is formed by the first 7 characters of the domain it is trying and the password to be the full name of the domain without .net .com .org etc

do you think it is possible?

i leave a jabber here if you can make such a script i am really interested in collaborating.

barbel@xmpp.jp

thanks.

ayoua - November 2, 2025, 11:43 am

man just use paramiko library and with the help of chatgpt or any llm would be super easy

Code import paramiko

```
def ssh_command(ip, port, user, passwd, cmd):
    client = paramiko.SSHClient()
    client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    client.connect(ip, port=port, username=user, password=passwd)
    _, stdout, stderr = client.exec_command(cmd)
    output = stdout.readlines() + stderr.readlines()
    if output:
        print('--- Output ---')
        for line in output:
            print(line.strip())
```

```
if __name__ == '__main__':
    import getpass
    user = getpass.getuser()
    user = input('Username: ')
    password = getpass.getpass()
    ip = input('Enter server IP: ') or '192.168.1.203'
    port = input('Enter port or <CR>: ') or 2222
    cmd = input('Enter command or <CR>: ') or 'id'
    ssh_command(ip, port, user, password, cmd)
```

this code is from blackhat python (a known book) it should give you foundation so you can implement yours

barbel - November 2, 2025, 11:50 am

I was thinking that we could do something together, to make it seem like we were a community, I hope I'm not wrong. Anyway, thank you very much for your intention.

FrostMost - November 4, 2025, 1:03 am

(Nov 2, 2025 12:50 PM)barbel Wrote: [\[CITE\]](#) I was thinking that we could do something together, to make it seem like we were a community, I hope I'm not wrong. Anyway, thank you very much for your intention.

No ur completely right. I guess the other guy just mistook u for just a seller or sm who just wants a quick script. If u r open to collaborative learning and effort the whole community is open to help u bro ???

Namz - November 4, 2025, 1:38 am

(Nov 2, 2025 12:13 PM)barbel Wrote: [\[CITE\]](#) hello,
i want to briefly explain if someone is available and able to make a simple functional python script that tries to connect via ssh/22 to domains.

i need a python script that can connect to a list of domains: domains.txt which are one under the other on ssh/22 with user which is formed by the first 7 characters of the domain it is trying and the password to be the full name of the domain without .net .com .org etc

do you think it is possible?

i leave a jabber here if you can make such a script i am really interested in collaborating.

barbel@xmpp.jp

thanks.

You can check my FREE SSH BRUTER here : [FREE SSH BRUTER IN GO](#)

barbel - November 4, 2025, 4:44 am

I looked over the script and I really appreciate the help, it wasn't about ips, it was about domains

I'm interested if you can help me even in go with a script for bruteforce ssh that extracts the first 7 characters from the domain and uses them as a username and as a password you will use the entire domain without .com .net .org and so on, do you think that this can be done?

so I can buy the whole list of dopmen .es as an example and at the username you will use %domain7firstletter% and at the password you will use %domain% without .es and try the whole list on the port set by me either 22 or 2222 or which port are now open, do you think it can be done? even in go I understood that it is much faster

barbel - November 5, 2025, 12:06 pm

hello, I saw the brutele, it's excellent, my question is if it can be done for domains, I have a list of domains that I'm posting here as an example:

aboisserie.ovh
abominable.ovh
abondar.ovh
abonneau.ovh
abonnementiptv.ovh
abonnin.ovh
abouar.ovh
aboubacar-ali.ovh
aboudaya.ovh
aboulala.ovh
abouque.ovh
abousir-el-meleq.ovh
aboutastro.ovh
aboutblank.ovh

what I want the go script to do is take the first 7 characters of the domain name and use them as the username and the domain name as the password, can you make this change to your go script?

I managed to make a script in go that checks on port 22 if the domains have the port open and I tested it, it works perfectly, now I need help for what I'm trying to do. I hope to find some help here

```
// check_ssh_ports.go
package main

import (
    "bufio"
    "context"
    "fmt"
    "net"
    "os"
    "sync"
    "time"
)

const (
    port      = "22"
    timeoutSec = 3           // timeout per connection
    concurrency = 200        // numarul de goroutines simultane (ajusteaza dupa nevoie)
    inputFile  = "domains.txt" // intrare: un domeniu per linie
    outputFile = "open_ssh.txt" // iesire: domenii cu port 22 deschis
)

func worker(ctx context.Context, jobs <-chan string, results chan<- string, wg sync.WaitGroup) {
    defer wg.Done()
    for {
        select {
        case <-ctx.Done():
            return
        case domain, ok := <-jobs:
            if !ok {
                return
            }
            address := net.JoinHostPort(domain, port)
            d := net.Dialer{Timeout: time.Second * timeoutSec}
            conn, err := d.DialContext(ctx, "tcp", address)
            if err == nil {
                // port deschis
                conn.Close()
                results <- domain
            }
            // daca e închis sau timeout, nu trimitem nimic
        }
    }
}

func main() {
    // deschide fisier intrare
    in, err := os.Open(inputFile)
    if err != nil {
        fmt.Fprintf(os.Stderr, "Eroare la deschiderea fisierului %s: %v\n", inputFile, err)
        os.Exit(1)
    }
}
```

```

}
defer in.Close()

// pregatim canale si worker pool
jobs := make(chan string)
results := make(chan string)
ctx, cancel := context.WithCancel(context.Background())
defer cancel()

var wg sync.WaitGroup
for i := 0; i < concurrency; i++ {
    wg.Add(1)
    go worker(ctx, jobs, results, &wg)
}

// writer goroutine: scrie rezultatele într-un fisier
out, err := os.Create(outputFile)
if err != nil {
    fmt.Fprintf(os.Stderr, "Eroare la crearea fisierului %s: %v\n", outputFile, err)
    os.Exit(1)
}
defer out.Close()
writerDone := make(chan struct{})
go func() {
    w := bufio.NewWriter(out)
    for d := range results {
        fmt.Fprintln(w, d)
    }
    w.Flush()
    close(writerDone)
}()

// citim domeniile si le trimitem la joburi
scanner := bufio.NewScanner(in)
count := 0
for scanner.Scan() {
    line := scanner.Text()
    if line == "" {
        continue
    }
    count++
    jobs <- line
}
close(jobs)
if err := scanner.Err(); err != nil {
    fmt.Fprintf(os.Stderr, "Eroare la citirea fisierului: %v\n", err)
}

// asteptam workerii sa termine
wg.Wait()
// închidem canalul de results si asteptam writer-ul
close(results)
<-writerDone

```

```
        fmt.Printf("Gata — am procesat ~%d domenii. Domeniile cu port 22 deschis au  
fost scrise în %s\n", count, outputFile)  
    }
```

```
go build -o check_ssh_ports check_ssh_ports.go  
./check_ssh_ports
```

put domains in domains.txt

Does anyone have an idea? Does anyone have a pertinent suggestion? I await your answers.

Does anyone have an idea? Does anyone have a pertinent suggestion? I await your answers.

psickophant - November 10, 2025, 12:33 am

As previously stated, The code posted is in Blackhat Python version2. It would be a great help for you to look over it and ask questions of anything you don't understand. I would be happy to assist with augmenting the code to achieve your goal. PM me if you would like.

Chornaya Magiya - November 10, 2025, 1:29 am

Peace of garbage idea, do not even waste your time u will not get any hosts.

barbel - November 13, 2025, 12:22 am

there are hundreds of millions of hosts, you get them for 9 usd targeted by countries and domains, please support the idea, don't throw mud if you don't know.

thanks for all the positive ideas.

here is the link for what I'm saying.

domains-monitor.com

Download a list of 311 980 138 domains in 1 570 zones!

Last update: 13.11.2025 00:10 (CET), next update in 15 hours

25 30% have ssh open!

@psickophant

I can't send messages, I'm not a user with over 25 posts, please make an effort and send a private email, you're the first one, I'll tell you more there. Thank you very much for your support, I'm waiting for your message.