Blue Team Level 1 Certification (Standard)

Introduction to BTL1
- Welcome to Blue Team Level 1! — 4 Topics
- Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN
- Introduction to Security Fundamentals — 1 Topic
- Soft Skills — 7 Topics
- Security Controls — 5 Topics | 1 Quiz
- Networking 101 — 6 Topics | 1 Quiz
- Management Principles — 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN
- PA1) Introduction to Emails and Phishing — 7 Topics | 1 Quiz
- PA2) Types of Phishing Emails — 10 Topics | 2 Quizzes
- PA3) Tactics and Techniques Used — 12 Topics | 2 Quizzes
- PA4) Investigating a Phishing Email — 8 Topics | 2 Quizzes
- PA5) Analysing URLs, Attachments, and Artifacts — 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions — 12 Topics | 1 Quiz
- PA7) Report Writing — 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge — 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN
- TI1) Introduction to Threat Intelligence — 7 Topics
- TI2) Threat Actors & APTs — 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence — 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence — 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence — 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns — 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN
- DF1) Introduction to Digital Forensics — 5 Topics
- DF2) Forensics Fundamentals — 10 Topics | 5 Quizzes
- DF3) Digital Evidence Collection — 8 Topics | 1 Quiz
- DF4) Windows Investigations — 3 Topics | 3 Quizzes
- DF5) Linux Investigations — 4 Topics | 2 Quizzes
- DF6) Volatility — 3 Topics | 1 Quiz

Discovery

This lesson is going to cover the fourth stage in the MITRE ATT&CK framework, Discovery. These techniques are used to describe ways that adversaries will collect more information about the network they're in and other systems that are present. Adversaries should spend a good deal of time at this stage, quietly watching what is happening around them so they can take further actions and ensure that they remain stealthy, attempting to blend in to 'normal' network activity. At the time of writing currently includes 24 top-level techniques. **We will be looking at the following:**

- Account Discovery
- Network Service Scanning
- File and Directory Discovery

MITRE Technique T1087

One an attacker has a foothold in a system the next logical step is to identify existing accounts so they can plan privilege escalation and lateral movement activities. The immediate choice is to look what accounts are found within the operating system, but additional accounts could include any logged-in email accounts and web services, from Outlook to Facebook. All of these could provide valuable information but also allow follow-up attacks such as internal spear phishing and social engineering.

This technique includes 4 sub-technique which we'll go into more detail below.

Sub-techniques (4)

ID	Name
T1087.001	Local Account
T1087.002	Domain Account
T1087.003	Email Account
T1087.004	Cloud Account

- Local Accounts – Attackers may attempt to get a listing of local accounts using commands such as `net user` and `net localgroup` of the Net utility and `id` and `groups`on macOS and Linux can list local users and groups. On Linux, local users can also be enumerated through reading the `/etc/passwd` file using commands such as `cat`, `strings`, and `head`.
- Domain Accounts – Attackers may attempt to get a listing of domain accounts using commands such as `net user /domain` and `net group /domain` of the Net utility, `dscacheutil -q group`on macOS, and `ldapsearch` on Linux can list domain users and groups.
- Email Accounts – Attackers may attempt to get a listing of email addresses and accounts using techniques such as dumping Exchange address lists. It's worth mentioning that this is what Emotet does when it infects a system, using this technique to scrape email addresses so it can send malicious emails from the compromised email account to any contacts or recent recipients.

Emotet	Emotet has been observed leveraging a module that can scrape email addresses from Outlook.[7]

- Cloud Accounts – Attackers may attempt to get a listing of cloud accounts that are configured by an organisation for use by users, remote support, services, or for administration of resources within a cloud environment. This can be achieved by navigating to popular console windows for AWS or Azure through the browser of the user to identify any cached credentials to log in to these services.

Moving down to the Mitigations table on the main technique there is only one suggestion listed, which is to disable the registry key shown below to prevent administrator accounts being enumerated, disclosing information such as their usernames. To disable this key across a large environment we can use Group Policy Objects to enforce the change across all domain users.

DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
Section Introduction, ATT&CK
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Activity) ATT&CK Navigator
Activity) End of Section Review, ATT&CK
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam

Mitigations

Mitigation	Description
Operating System Configuration	Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators`. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation. [1]

MITRE suggests that we attempt to identify enumeration techniques by monitoring PowerShell and command-line arguments for commands that are related to discovery such as **`net user`** and **`net localgroup`**.

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

MITRE Technique T1046

Attackers that have a foothold in the network may attempt to discover other systems that are alive on the network, and then work to identify what ports are open and the corresponding services that are operating on those ports. This is typically done using tools that allow for port scanning or vulnerability scanning (active scanning) but can also be achieved using quieter methods such as listening on the network to see how other systems are communicating using a tool like Wireshark (passive scanning).

In the Procedure Examples table we can see that APT32 conducting network scans once they are on a system to identify other systems, open ports, the operating systems used, and identify vulnerabilities they can exploit to perform lateral movement, also known as pivoting.

Procedure Examples

Name	Description
APT32	APT32 performed network scanning on the network to search for open ports, services, OS finger-printing, and other vulnerabilities.[23]
APT39	APT39 has used CrackMapExec and a custom port scanner known as BLUETORCH for network scanning.[27][28]
APT41	APT41 used a malware variant called WIDETONE to conduct port scans on the specified subnets.[13]
BlackEnergy	BlackEnergy has conducted port scans on a host.[7]

In the Mitigations table the first entry is straight to the point, if a service and port aren't being used, they should be disabled to prevent fingerprinting by a malicious actor. Out-of-date services can also provide an appealing target for attackers and could allow them to gain access to that system. Network Intrusion Detection and Prevention Systems (NIDS/NIPS) should be used to detect suspicious network traffic such as port scans and exploitation activity. Popular examples include Snort and Bro/Zeek. Proper segmentation and use of VLANs can limit which systems are able to communicate which each other and can result in an attacker being 'trapped' in one system, not able to attack any others.

Mitigations

Mitigation	Description
Disable or Remove Feature or Program	Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
Network Intrusion Prevention	Use network intrusion detection/prevention systems to detect and prevent remote service scans.
Network Segmentation	Ensure proper network segmentation is followed to protect critical servers and devices.

As mentioned in the Detection section of this technique a system randomly performing network or vulnerability scans is, unsurprisingly, not normal activity and should be investigated. Network Intrusion Detection Systems (NIDS) can be used to generate alerts on suspicious or malicious traffic which can be investigated by security analysts, while Network Intrusion Prevention Systems (NIPS) can take automated actions to block or reset connections, preventing scans from returning results to the compromised system.

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events from legitimate remote service scanning may be uncommon, depending on the environment and how they are used. Legitimate open port and vulnerability scanning may be conducted within the environment and will need to be deconflicted with any detection capabilities developed. Network intrusion detection systems can also be used to identify scanning activity. Monitor for process use of the networks and inspect intra-network flows to detect port scans.

MITRE Technique T1083

Attackers may decide to see if there are any interesting files on the system they have compromised, a process known as file and directory enumeration. This could include looking for important files using an extension list such as .xlsx for spreadsheets which could include financial information. There are a wide range of commands that adversaries could use to locate specific files and folders, including; `dir`, `tree`, `ls`, `find`, and `locate`.

The Procedure Examples table for this technique is incredibly long (seriously, it's freaking long), but that makes sense because almost every threat actor is going to want to identify confidential or valuable files and download them back to their attacking system for further analysis. Below you can see a number of examples where threat actors or malware have been observed performing file and directory enumeration to discover interesting files.

Procedure Examples

Name	Description
3PARA RAT	3PARA RAT has a command to retrieve metadata for files on disk as well as a command to list the current working directory.[78]
4H RAT	4H RAT has the capability to obtain file and directory listings.[78]
admin@338	admin@338 actors used the following commands after exploiting a machine with LOWBALL malware to obtain information about files and directories: `dir c:\ >> %temp%\download dir "c:\Documents and Settings" >> %temp%\download dir "c:\Program Files\" >> %temp%\download dir d:\ >> %temp%\download`[159]
ADVSTORESHELL	ADVSTORESHELL can list files and directories.[98][67]
APT18	APT18 can list files information for specific directories.[153]

It's pretty much impossible to Mitigate a user looking through files and directories, because we all do it everyday. One method that should be used across all counts is principle of least privilege, ensuring that users can't access, delete, or modify files that they should not have access to. Access to network shares and file transfer servers should use strong passwords and should timeout after a certain period of time to prevent unauthorised access.

Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

To detect this kind of activity we should monitor WMI, PowerShell, and CMD usage for any commands that could be used maliciously to locate specific files or browse the file structure of a system. This includes but isn't limited to **`locate`**, **`find`**, **`dir`**, and **`tree`**. Remember that these commands will be used legitimately, so alerting on this would generate a lot of false positives, making it hard to properly identify malicious usage.

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Collection and Exfiltration, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Privacy & Cookies Policy