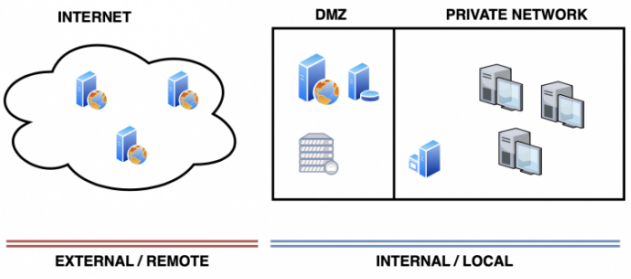
Common Events & Incidents

This lesson will cover the common security events observed by security operations teams, giving you an insight into the typical day-to-day investigations that take place. We will also cover how some common events can progress into incidents and the actions that are taken by defenders to properly analyze the situation. The events we will cover are:

- Remote to Local Scanning
- Remote to Local DoS/DDoS
- Local to Local Scanning
- Login Failures

Before we jump into these security events, we want to explain what is meant by "remote to local", "local to remote" and "local to local". When considering an organizations private network, we use the term internal, as it is inside the organization. Anything outside of the organization, such as websites not hosted by the company and public IP addresses, this is referred to as external, or remote.

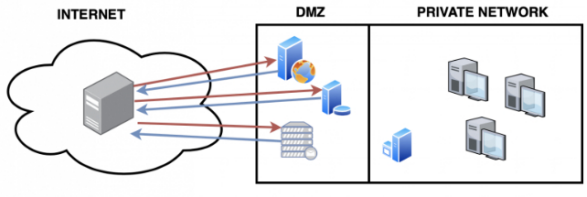


So activity that occurs between two systems within a private network is **local to local**, while activity from an external IP address towards a public IP address owned by the organization would be **remote to local**. Throughout the rest of this lesson we will be using the abbreviations:

- R2L – Remote to Local
- L2R – Local to Remote
- L2L – Local to Local

R2L PORT SCANNING

With this activity, an external public IP address is scanning the public IP addresses owned by the organization. This is typically conducted to see what IP addresses are used by the organization, which of them are in use, and what ports are open. This type of activity is likely to happen all day, every day, and is arguably the most common alert analysts will see, depending on how the specific organization monitors this activity.



In the simplified diagram above, we have shown how a system present on the internet is able to perform a port scan against systems in the DMZ by going through a list of public IPs that are owned by the organization. The red lines represent the system sending a request to an IP address on a specific port, and the blue lines represent a response from the system (provided there is an active system on that IP).

Detection

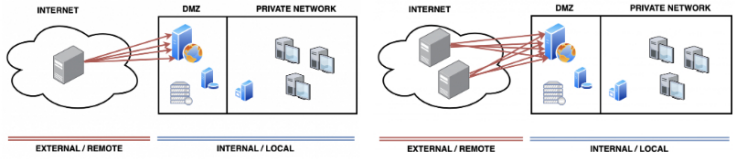
For this, we would want to collect logs from perimeter firewalls and web application firewalls. The rule would look for multiple connections within a small timeframe to a number of different ports on the system. Typically, web servers should only ever be contacted on ports 80 (http) and 443 (https). A remote system that starts connecting on 93, 1195, 1959, and other random non-standard ports is most likely scanning or fingerprinting the system.

Potential Impact

Scanning happens all the time, and there is rarely an immediate impact. Older systems could be affecting by scanning if there is no scalability, and the actor is performing an intense scan. This could potentially use up a lot of bandwidth and lead to other systems not being able to connect to it, causing a denial-of-service (DoS).

R2L DOS/DDOS

With this activity, one (DoS) or more (DDoS) external IP addresses are sending a high volume of requests or malformed packets to a target system in an attempt to crash it.



The diagram on the left shows an R2L denial of service attack, where one IP is attempting to send more packets to the target system than it can process, causing it to crash, preventing legitimate traffic reaching it, resulting in a denial of service.

The diagram on the right shows an R2L distributed denial of service attack, where multiple IPs are attempting to crash or consume the target system's resources so that it can't process legitimate requests, resulting in a denial of service.

Detection

We can use rules that monitor the number of requests the systems in the DMZ receive. Establish a baseline for the levels of "normal" traffic that is expected to be received by these systems, and create a rule that will generate an alert when a threshold higher than the baseline is observed.

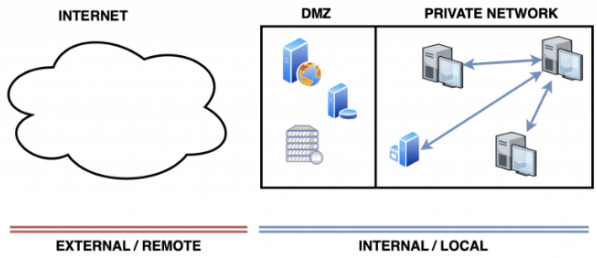
Potential Impact

Denial of service attacks, while dependent on a number of factors, have the potential to take systems offline. This can result in loss of customer trust, a decline in sales, and potentially even damage to the affected system. Let's go through an example; if Organisation A is an online retailer and their website is hit by a DDoS attack and it goes offline, customers will be unable to place orders, resulting in lost sales. Customers who hear how the site has been "attacked", without proper context and knowledge of cybersecurity may believe the site has been hacked, and take their business elsewhere. In 2016 a DDoS attack was launched against Dyn, a DNS provider. This led to organizations that used Dyn to also go offline, as users that attempted to visit the sites were unable to resolve the IP address from the domain name. This attack affected companies such as Amazon, BBC, PayPal, Reddit, and Twitter. You can read more about this high-profile DDoS attack here.

L2L SCANNING

L2L SCANNING

With this activity, an internal private IP address is scanning another, or multiple, private IP addresses.



In the simplified diagram above, we have shown how a system within the private network is scanning other systems on the same network, sending out requests and receiving replies, using these to determine what systems are active and perform fingerprinting activities to identify the operating system and any running services on other hosts.

Detection

SIEM rules can be configured to generate alerts when one private IP is making rapid connections to other internal private IPs. Thresholds or patterns should be used to prevent false positives, as internal systems will make legitimate connections to each other, but it is highly unlikely internal systems should be port scanning or fingerprinting each other! Internal vulnerability scanners should be whitelisted from any L2L scanning rules, as if the security team starts an internal vulnerability scan, the SIEM will generate an alert as the scanner begins scanning other internal systems.

Potential Impact

If an internal system has been compromised, the likely next step for an attacker once persistence has been achieved would be to identify other systems in the same network so they can perform lateral movement – the process of moving from one system to another. They will identify other systems by conducting scans using ARP, UDP, TCP, or ICMP to see what other IPs are in use, and what ports and services are running on them, looking for a way into the machine.

LOGIN FAILURES

There are three typical reasons this activity occurs;

1. A user has had their password reset routinely and has forgotten their new password.
2. A user has simply forgotten their current password and entered it in wrong multiple times.
3. A malicious actor is attempting to gain unauthorized access to a user account, and has incorrectly guessed the password.

Luckily in Windows Active Directory domains we can get useful information from the domain controller, giving us context to the login failures. Within the login failure event, Windows Security Log Event ID 4625, there is a field for "failure information" which will contain one of the following codes:

Status and Sub Status Codes	Description (not checked against "Failure Reason:")
0xC0000064	user name does not exist
0xC000006A	user name is correct but the password is wrong
0xC0000234	user is currently locked out
0xC0000072	account is currently disabled
0xC000006F	user tried to logon outside his day of week or time of day restrictions
0xC0000070	workstation restriction, or Authentication Policy Silo violation (look for event ID 4820 on domain controller)
0xC0000193	account expiration
0xC0000071	expired password
0xC0000133	clocks between DC and other computer too far out of sync
0xC0000224	user is required to change password at next logon
0xC0000225	evidently a bug in Windows and not a risk
0xc000015b	The user has not been granted the requested logon type (aka logon right) at this machine

These codes give us tons of useful information, so we can recognize why the login actually failed. For example, if we had an alert for multiple login failures, and we saw the status code 0xC0000071, we know that the login has failed because the password has expired and needs to be reset. If we had another SIEM alert with the status code 0xC0000064 then we know that someone is trying to login with a username that doesn't actually exist.

Detection

In a Windows environment we can monitor Windows Security Log Event ID 4625, and set thresholds to detect multiple login failures against the domain controller for the same username. Analysts will then be able to investigate by looking at the status code from the security log and take actions based on the alerting activity. Password spraying attacks can also be detected by monitoring for a small number of login failures (2/3) for a large number of users within a short period of time.

Potential Impact

Users that are locked out can't work, resulting in a decline of productivity. Typically users will call up or visit their IT service desk to get the account unlocked, so it isn't a major issue and is typically resolved very quickly. However, login failures where the username is not recognized (0xC0000064) or the account is locked out because of too many failed logins (0xC00000234) could be signs of an attacker that is trying to gain access to internal accounts using a username and password wordlist, employing a dictionary attack, acting as an indicator that an internal system has been compromised.

Previous Topic

Mark Complete

Next Topic

Back to Lesson