PivotPoint SECURITY

THE PENETRATION TEST TRAIL

A NETWORK'S JOURNEY

TO PROVE IT'S SECURE

When your network goes through a penetration test, it's a little like taking a journey on The Oregon Trail… Think of your network as an eager adventurer looking to prove its prowess and demonstrate to its administrators that it can "securely" traverse the treacherous terrain of today's threat landscape.

Like any traveler who has attempted to best The Oregon Trail (whether in real life or through the famous video game), peril usually awaits. Follow us on an adventure with Network 1337 and its five externally-facing IP addresses on the Penetration Test Trail.

MEET NETWORK 1337

Based on the effectiveness of your Asset, Patch, and Vulnerability (APV) management your network will have abundant, moderate, or limited resources:

THE CISO (BANKER)

ABUNDANT RESOURCES

Only networks with robust APV management can begin their journey to proving they are secure with the vast resources of The CISO. Networks that know what devices they touch and their functions, and actively track/mitigate vulnerabilities can often afford to ride in luxury on the Penetration Test Trail.

THE IT DIRECTOR (CARPENTER)

MODERATE RESOURCES

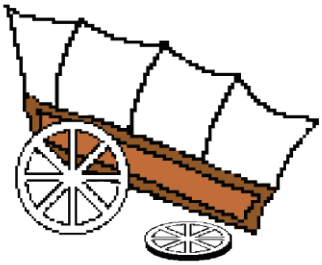
Most networks do not have robust APV management, but are well on their way. For networks that at least know their devices and can tell if they are patched, the journey to proving they are secure will be challenging but attainable.

THE TECH INTERN (FARMER)

LIMITED RESOURCES

Often we see networks with poor APV management. This is a warning sign for significant issues on the journey to prove security.

With some APV management in place but considerable room to grow, Network 1337 and its five IPs set off on their journey to prove security on the Penetration Test Trail!

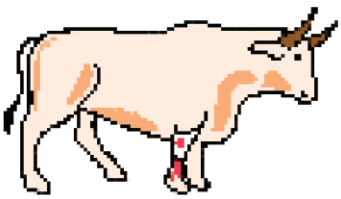


BROKEN WAGON WHEEL...

In the case of Network 1337, an initial vulnerability assessment revealed a number of hosts configured to allow Microsoft Server Message Block 1.0 (SMB v1) as a valid method of communication. The issue is that SMB v1 is very insecure. This is the vulnerability used by WannaCry and Petya ransomware viruses to spread.

YOU WERE ABLE TO REPAIR THE WAGON WHEEL...

ONE OF YOUR OXEN IS INJURED...



We utilized a tool named Empire to receive and manage reverse shell connections. Empire is a post-exploitation framework we utilize to manage compromised hosts, escalate privileges, pivot from host to host, and collect additional information that would be useful to gain deeper access, including in-memory credentials. After a few minutes, we can see that a number of hosts have been compromised.

YOUR RATE OF TRAVEL HAS DECREASED...

ONE OF YOUR IP'S DIES

We were able to harvest a number of credential sets from within the host's memory. It didn't take long to find a compromised host that a domain administrator had recently logged into. We tested these credentials to see if they truly were domain administrator level by attempting to use them to login to non-compromised servers.

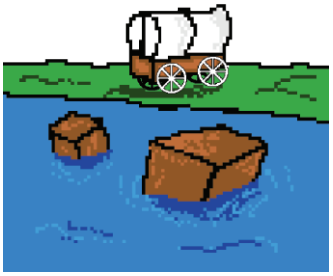
4 IPS REMAIN TO COMPLETE THE JOURNEY...

ONE IP IN YOUR PARTY BROKE THEIR LEG…

We then used a desktop PC to browse the network in order to see what domain shares were available. As it turned out, server backups were available. These could be downloaded and "restored" to a database server we controlled. Next, we utilized our captured credentials to attempt to gain access to the domain controller.

A SIGNIFICANT BLOW. BUT THE JOURNEY CONTINUES…

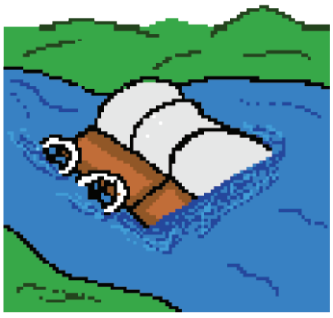
ATTEMPTED TO FORD THE KANSAS RIVER - YOUR SUPPLIES GOT WET AND YOU LOST ONE DAY…



We then attempted to leverage our position to gain access to the numerous MSSQL servers on the network. We were unable to login to a sampling of MSSQL servers using our captured domain administrator credentials.

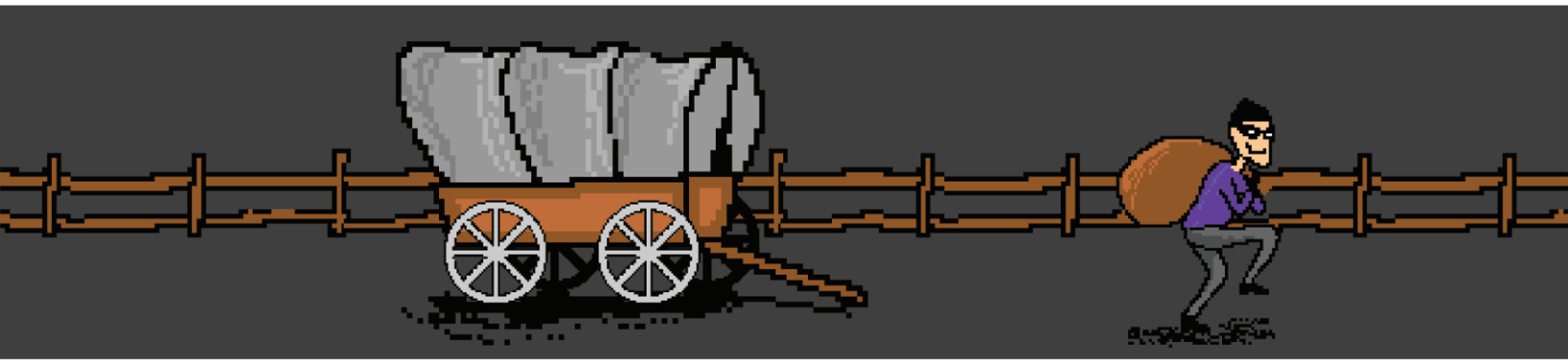
WHEW…

ATTEMPTED TO FORD BIG BLUE RIVER - RIVER WAS TOO DEEP -- 2 IP'S IN YOUR PARTY DROWNED…



Utilizing the domain credentials, we were able to log into a server hosting HR information. The exploitation of this vulnerability (SMB v1 permitted/SMB Signing Disabled) ultimately allowed us to gain control of Active Directory as well as the ability to collect an incalculable amount of corporate/sensitive data.

WILL NETWORK 1337 SURVIVE?



A THIEF COMES DURING THE NIGHT AND STEALS 1,000 LB.S OF FOOD...

During manual review of the network, many auxiliary device control panels were discovered (printers, server temperature monitoring devices, etc.). These control panels were exposed with either insecure, default, or in some cases, no passwords. Aside from gaining direct control over these devices, it may be possible to intercept documents, upload and serve malware, and possibly even manipulate these devices into a botnet.

RESOURCES ARE DWINDLING FAST

A FIRE IN YOUR WAGON RESULTS IN LOSS OF — 4 SETS OF CLOTHES, 2 WAGON WHEELS AND 1 IP DIES...

We were able to collect the IPMI hashes for a number of hosts, and determined that one host used a default credential set. We then used those credentials to log in to an IPMI control panel. This control panel could potentially be used to pivot onto the host machine but was not attempted as it requires crashing and rebooting the host to gain access.

ONLY ONE IP LEFT

ONE OF YOUR IP'S DRINKS BAD WATER AND DIES OF … SOMETHING UNPLEASANT…

During manual review, we located a management portal. We attacked two different ports and were able to gain access via both avenues. A malicious user in this position could reconfigure the VessRAID devices, blocking legitimate access, altering data integrity, or outright destroy data.

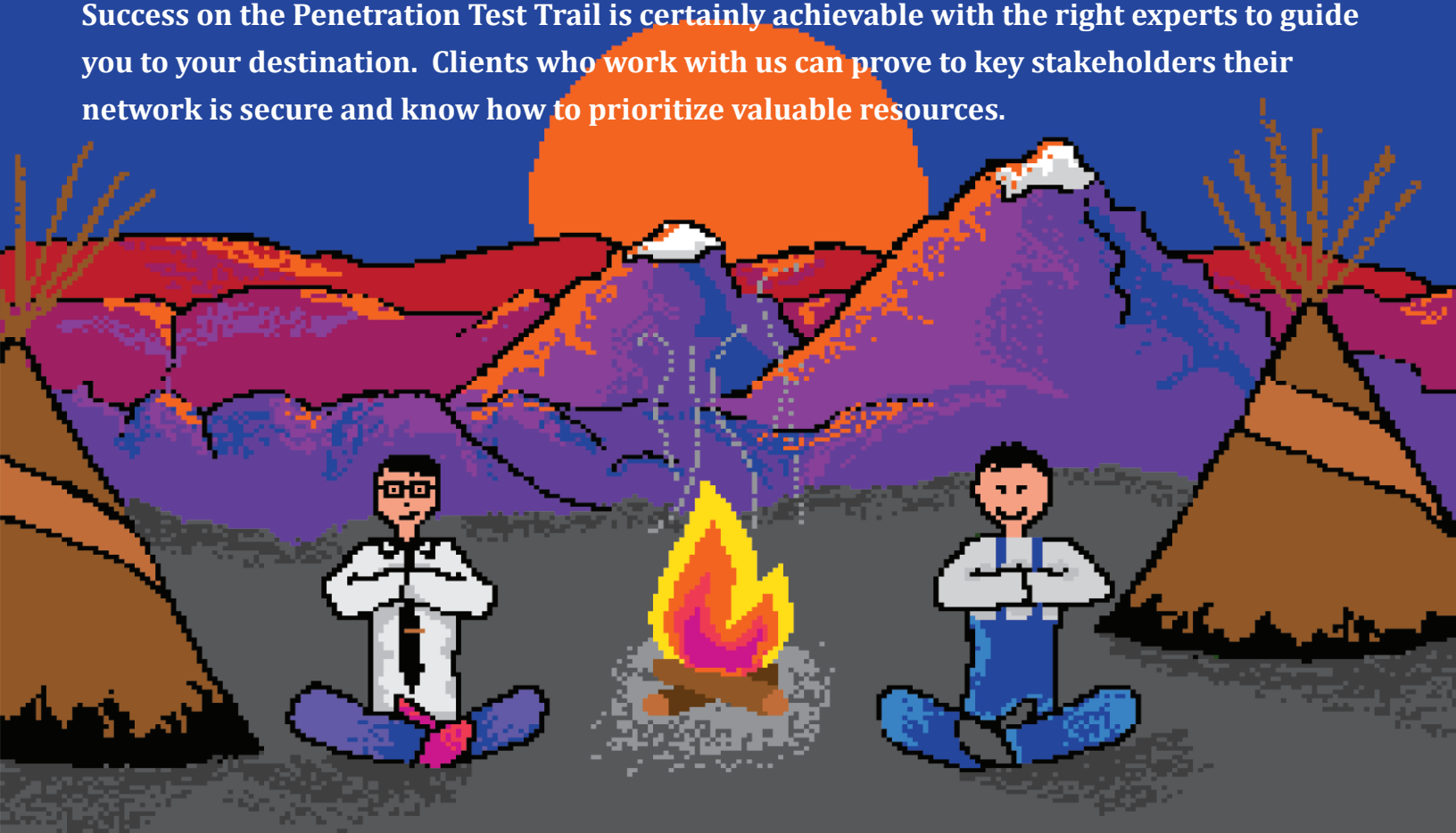
NETWORK 1337 'S JOURNEY ENDS HERE

...IS THIS THE END?

Like many adventurers that went before, Network 1337 was not able to withstand the rigors of "The Penetration Test Trail." Lack of quality APV management and deficiencies in the implementation of the password policy across all devices were significant obstacles.

YOU CAN SUCCEED WITH THE RIGHT GUIDE.

Success on the Penetration Test Trail is certainly achievable with the right experts to guide you to your destination. Clients who work with us can prove to key stakeholders their network is secure and know how to prioritize valuable resources.



For more information on Network 1337's journey, or to plan your own network's journey to prove it's secure, talk to Pivot Point Security.

Pivot Point SECURITY

info@pivotpointsecurity.com