Get a Quick Win in the Battle Against Ransomware by Disabling SMBv1

blog.netwrix.com/2021/11/30/what-is-smbv1-and-why-you-should-disable-it

Kevin Joyce

Server Message Block (SMB) is a Microsoft communication protocol used primarily for sharing files and printer services between computers on a network. SMBv1 dates back to the LAN Manager operating system and was deprecated in 2013 — so why should you care about it?

I can answer in one word: ransomware.

SMBv1 has a number of vulnerabilities that allow for remote code execution on the target machine. Even though most of them have a patch available and SMBv1 is no longer installed by default as of Windows Server 2016, hackers are still exploiting this protocol to launch devastating attacks. In particular, EternalBlue exploits a vulnerability in SMBv1 — and just a month after EternalBlue was published, hackers used it to launch the infamous WannaCry ransomware attack. It affected 200,000+ computers across 150 countries and some experts estimate the total damage to be billions of dollars. If your organization has older Windows operating systems, you are vulnerable to such attacks.

Handpicked related content:

[Free Guide] How to Prevent Ransomware Infections: Best Practices

In this article, I demonstrate how an attacker can exploit SMBv1 and get an elevated command prompt in just 3 quick steps — enabling them to launch ransomware, add themselves as a local admin, move laterally, escalate their privileges and more.

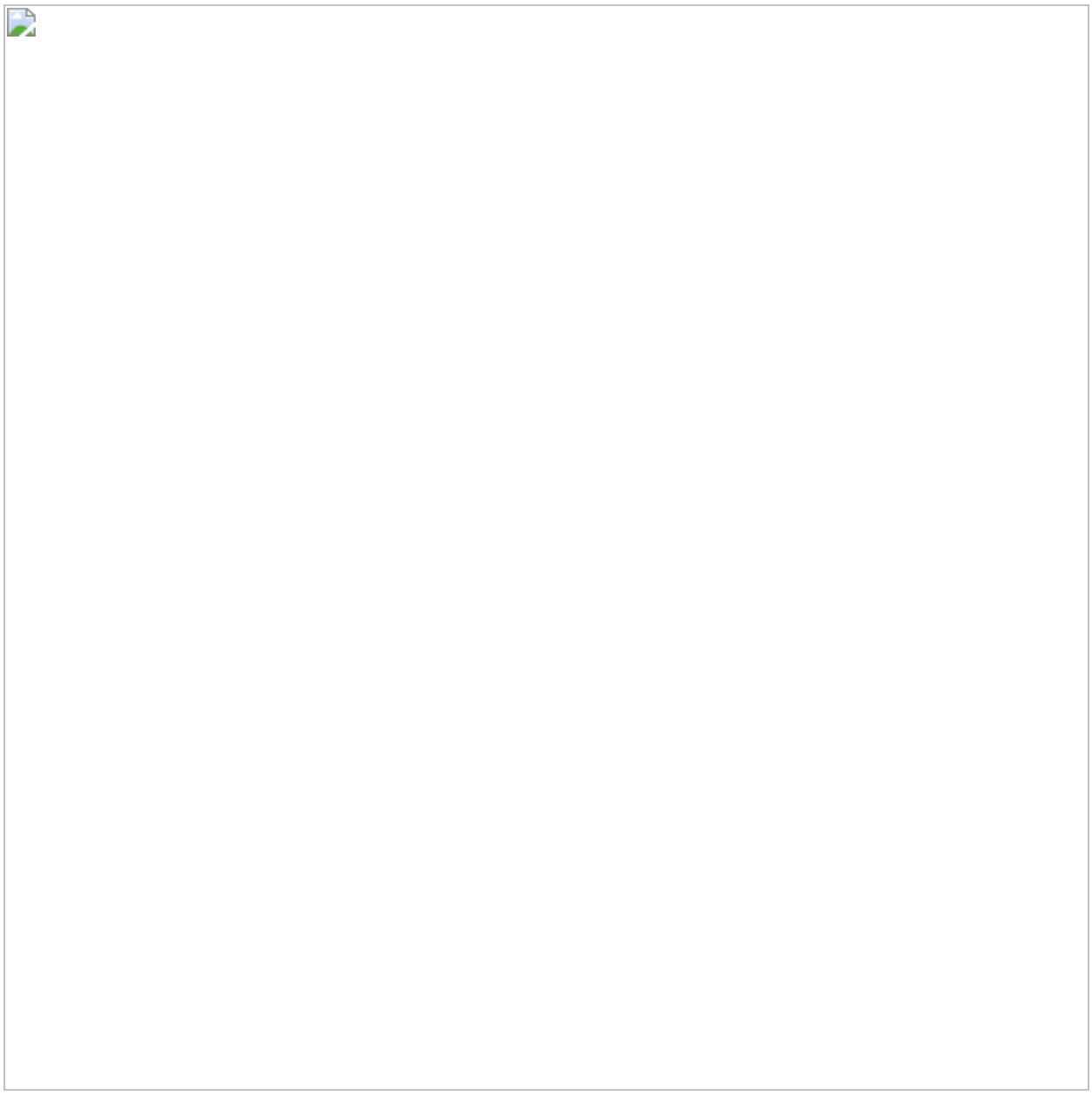
Then it offers some really good news: You can be a hero and defend your organization against this ransomware attack path quite easily!

How to Exploit SMBv1 and Get an Elevated Command Prompt in 3 Quick Steps

Let's assume I'm a hacker who has compromised the credentials of a non-privileged user account in a domain. Using reconnaissance in Active Directory, I found some Windows Server 2008 machines that I think might be vulnerable to EternalBlue. Here are the steps I can use to find out for sure and perform the exploit using the Metasploit penetration testing tool.

1. Search for EternalBlue modules.

First, I use the Metasploit console to search for EternalBlue modules:

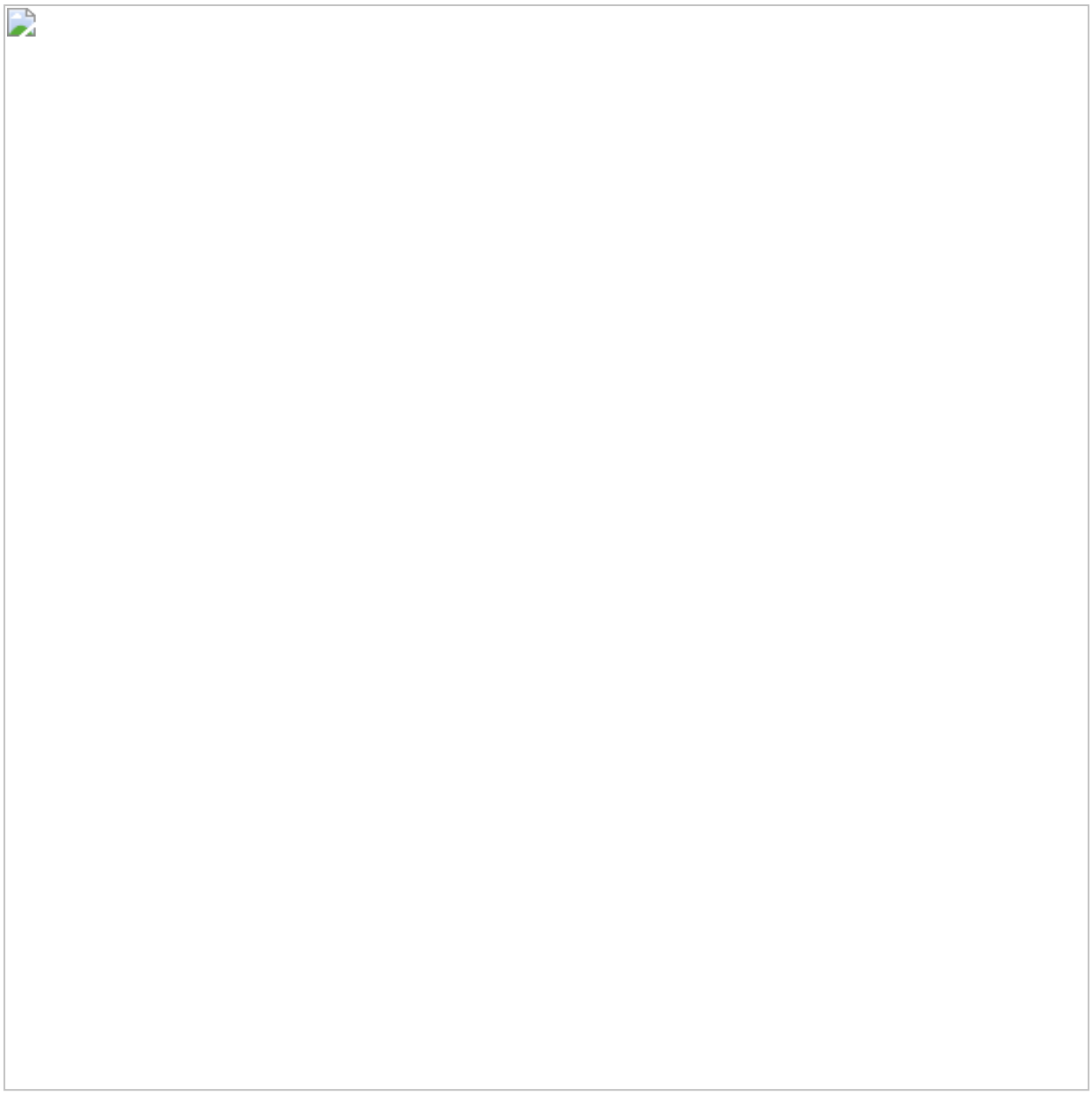


Searching for EternalBlue within Metasploit

As you can see, there is a scanner module that allows us to determine whether the machine might vulnerable to EternalBlue, and there are a few exploitation modules that can be leveraged to exploit EternalBlue.

2. Check whether the machine is vulnerable.

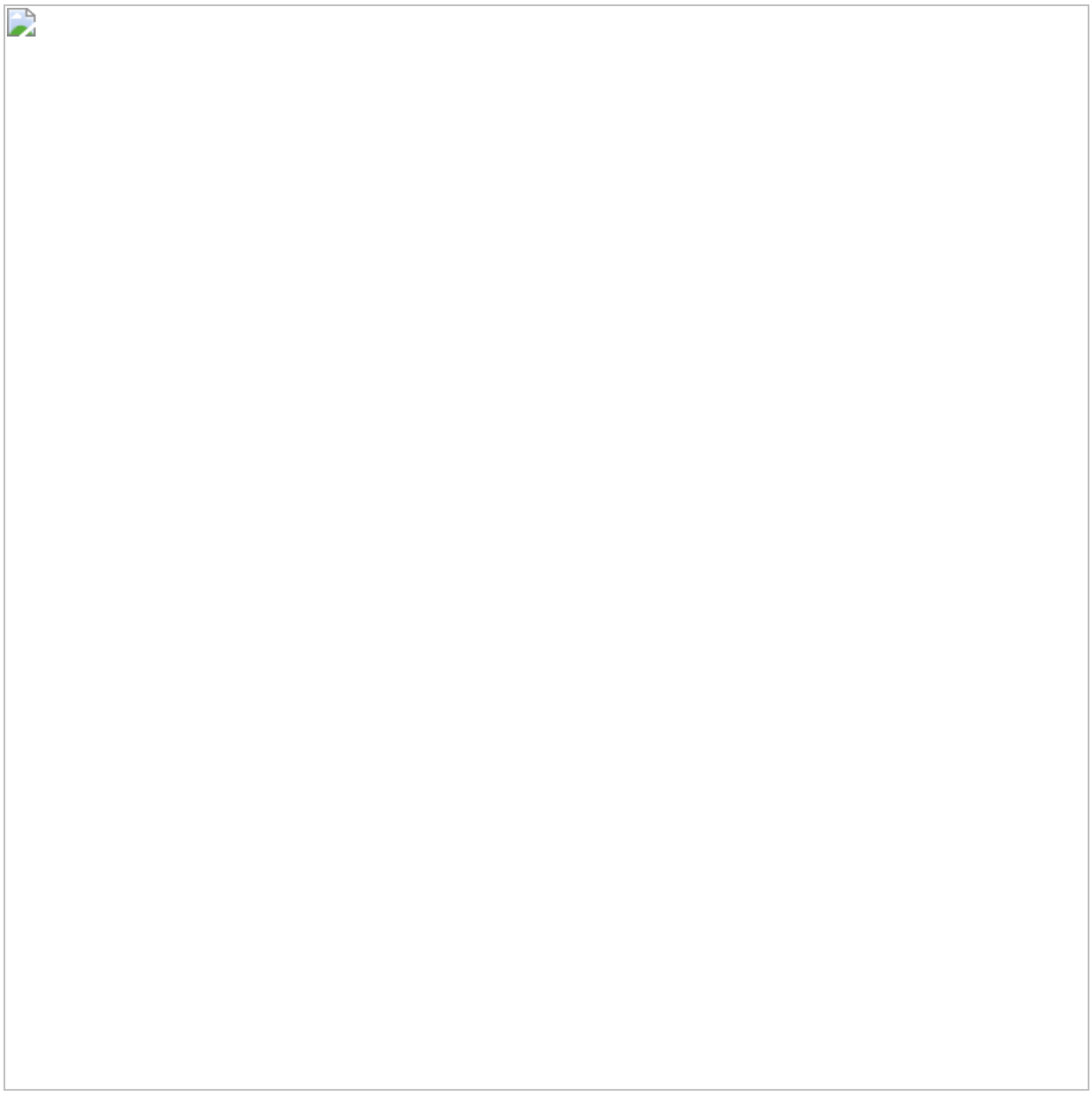
We'll start with the scanner and see if the machine we found is actually vulnerable. To run a module like the scanner, we simply type 'use [module name]'. The screenshot below shows how I use the module, including configuring the options required for it to run.



Using the scanner and setting the RHOSTS option to the IP of our target machine

3. Exploit EternalBlue on the target to get a system-level command prompt.

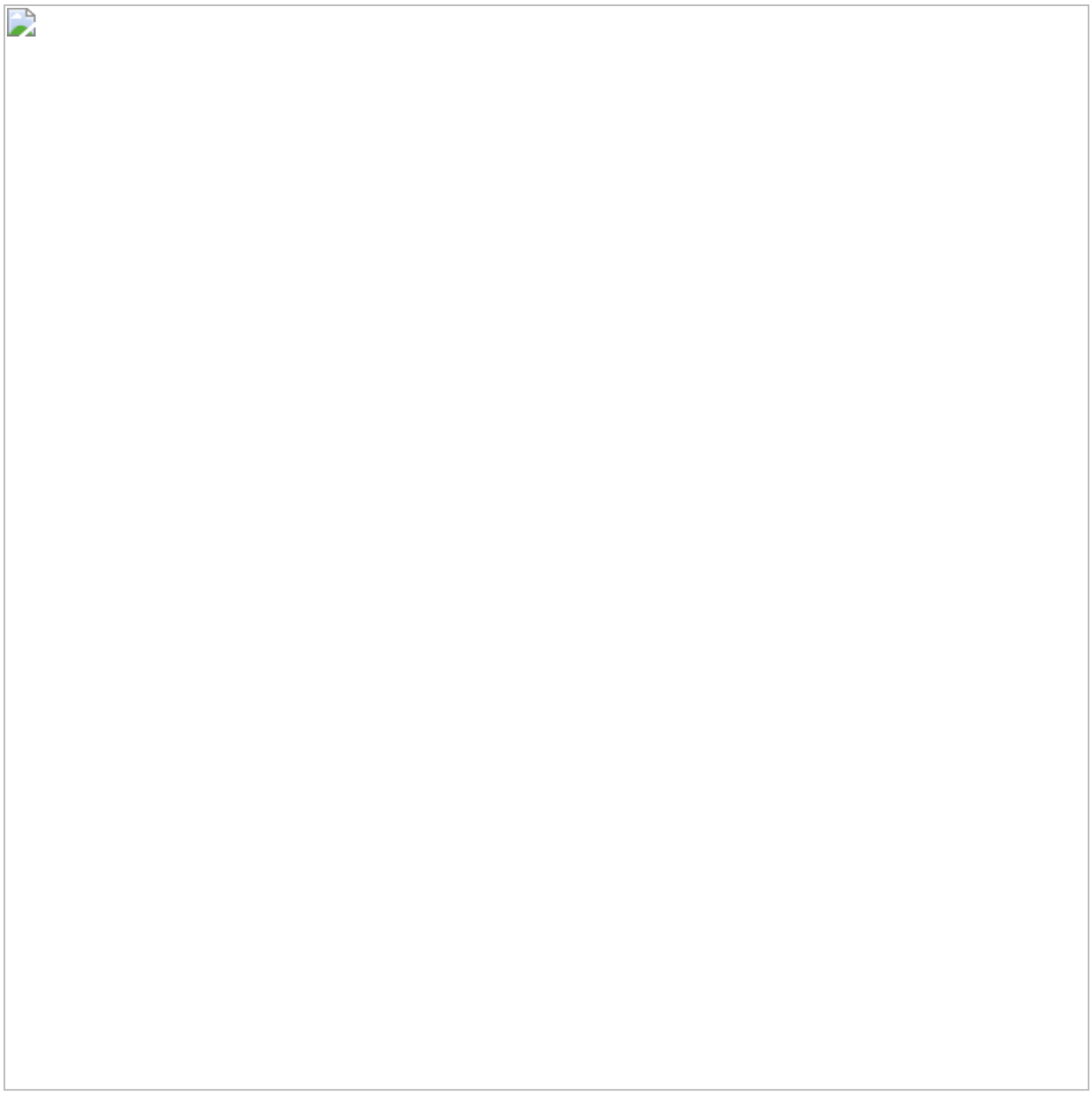
Since the result shows that the host is ‘likely vulnerable’, let’s try to exploit EternalBlue on it. To do so, we’ll switch back to the search for EternalBlue and use the exploit module, configuring the same options as we used before:



Trying to exploit EternalBlue on the target system

You can see that the same check is performed as before, but then the process goes a step further and executes a payload that can exploit EternalBlue.

The result is that I am granted a system-level command prompt on the target host:



System-level command prompt after exploitation

That's it! With a system-level command prompt, I now can unleash malware, move laterally, escalate my privileges, achieve persistence and more.

How to Easily Defend Your Business

Fortunately, it's generally very easy to prevent a devastating incident like this from occurring in your IT environment. More often than not, SMBv1 can simply be disabled without affecting operations — and Microsoft provides a nice how-to for identifying the status of SMB on a machine and disabling it.

If you cannot disable SMBv1 because you have legacy applications or systems (such as Windows XP) that require it, do the next best thing: Make sure to install all available SMBv1 patches as soon as possible.

Conclusion

Even a single malware infection can cause devastating financial and reputation damage — encrypting or stealing your sensitive data, disrupting your critical workflows, and shattering the confidence of your customers.

Netwrix solutions can help you prevent ransomware infections, thwart attacks in progress and quickly return to a secure state by implementing a multi-layered approach to security:

- Identify and mitigate weak spots in your security posture to minimize the risk of successful ransomware attacks and limit the damage an infection could cause.
- Spot signs of ransomware being planted or activated in your network and respond in time to avoid serious damage and keep your organization out of the news.
- Quickly understand the details and scope of an attack, speed restoration of business operations, inform compliance reporting, and improve your security posture against future attacks.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.