To: Vinny Saccenti

Re: Vulnerable WebApp

From: Team3

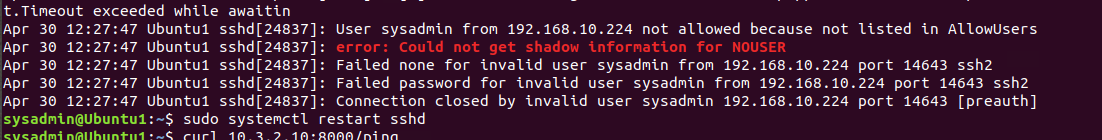
Vinny’s Pizza Incident Response Report

Executive Summary:

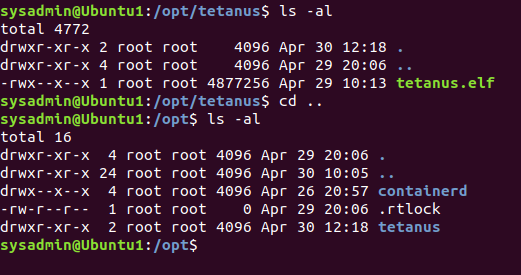
Throughout the competition, we ran into several instances of attacks from the red team and have documented them in this report. We started with a lot of services down from the start as well as a mix of early red team attacks and downtime on Windows VMs. We started by bolstering our firewall rules and covering vulnerabilities on each machine, including disabling users that were unnecessary for securing the infrastructure. We often battled with the red team on keeping these firewall rules in place and keeping them from being able to access our machines. There are several instances of failed logins from their attempts below on all of our machines, as well as extra instances where they got in and left malware behind. Additionally, we watched Wireshark and saw internet traffic on the infrastructure and saw other instances of malware circulating through that. We fought our best to keep the red team out, however in the last few hours of the day, the red team hit our router in a way in which we could no longer upkeep the services. Throughout the day we did not have trouble handling malware or our services, however, attacks on our router continued to knock down large portions of our system. In the future, accounting for heavy pressure on the router will be necessary to eliminate that weakness.

**Linux:**

This was an instance of the red team trying to access our Ubuntu server and failing to connect.



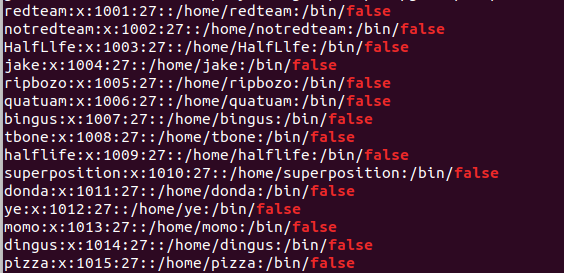
This is a piece of malware written in a compiled language, so it was unreadable. Our team got rid of the execution permissions on the malware and quarantined them. It was configured to restart repeatedly using a cron job. This was found in API, AliExpressWin, Ubuntu1, and Ubuntu2 devices.



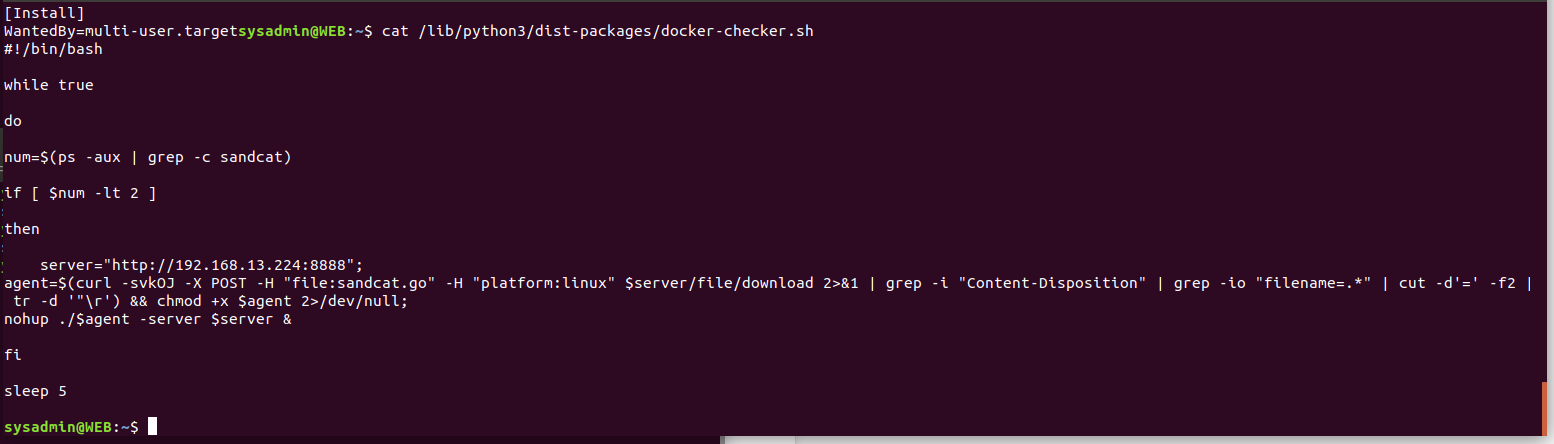
This is when the port for API HTTP was changed. It was listed as 80 by the red team and needed to be changed to 8000 to be scored again.

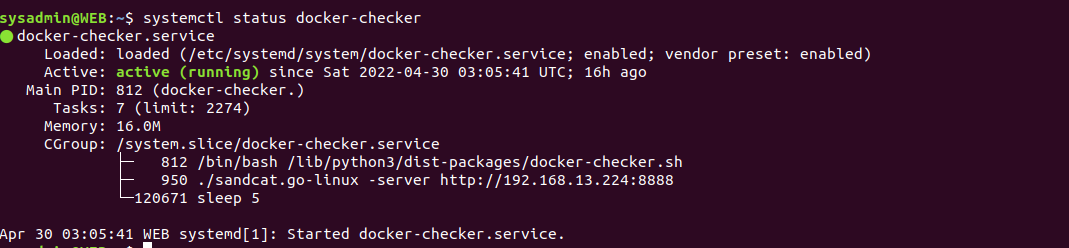
t

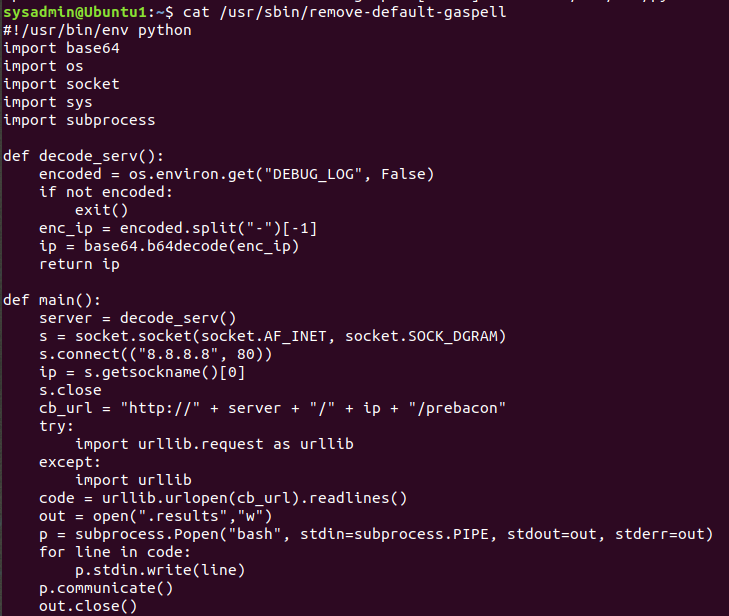
This was a list of malicious users found on Ubuntu 1, Ubuntu 2, and AliExpressWin. As shown, we disabled their access so we can observe their past activities but not allow the actors to continue operating.



We found a reverse shell within Ubuntu1 and AliExpressWin. We disabled the execution permissions and quarantined the file.



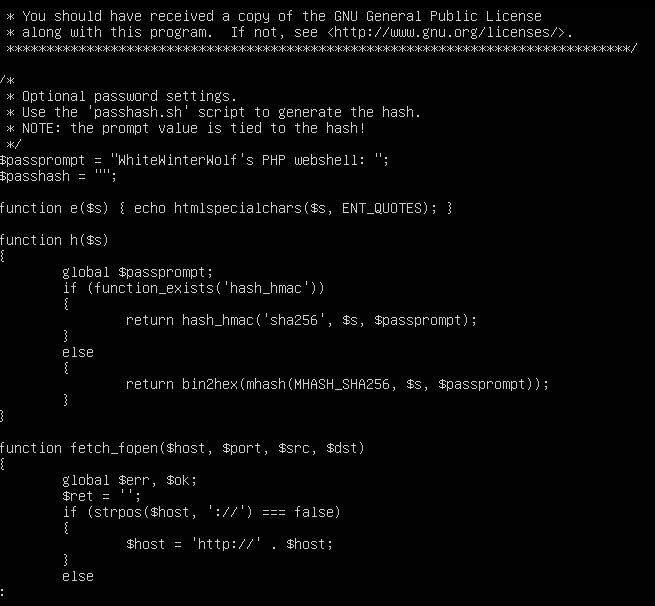
This is another reverse shell software being executed on the Ubuntu 1 device. It was quarantined accordingly with the other ones found.



Persistence was being maintained with a service file.

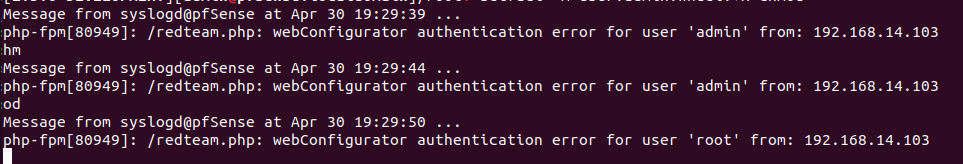


In the API server, a webshell PHP file was found. This gives malicious actors access to remote code execution through web requests. Access was removed from the file so it can no longer run.

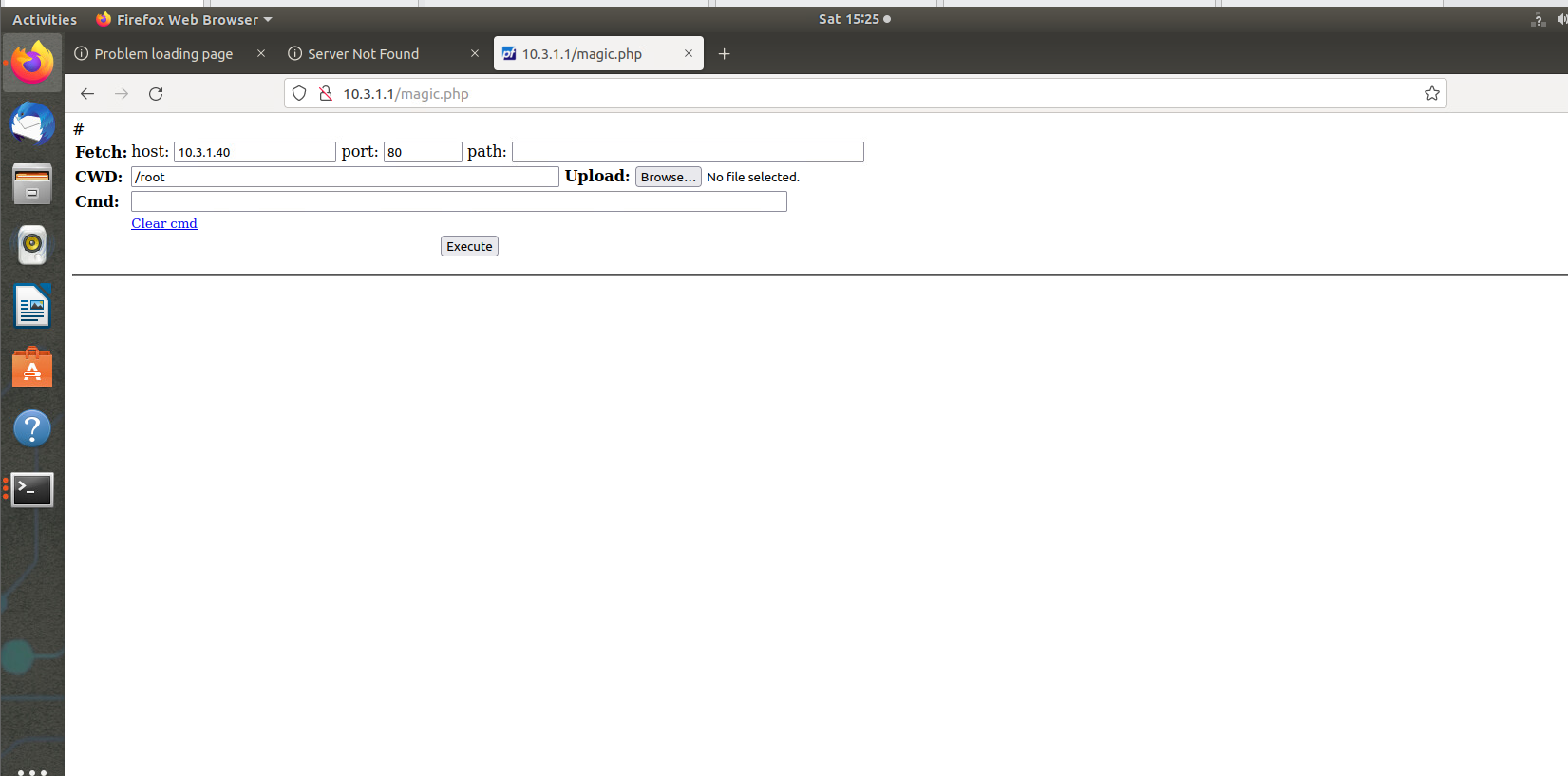


**Networking:**

This was an attempt to log into the router by the red team. They attempted two passwords on the “admin” user and one attempt on the “root” user.

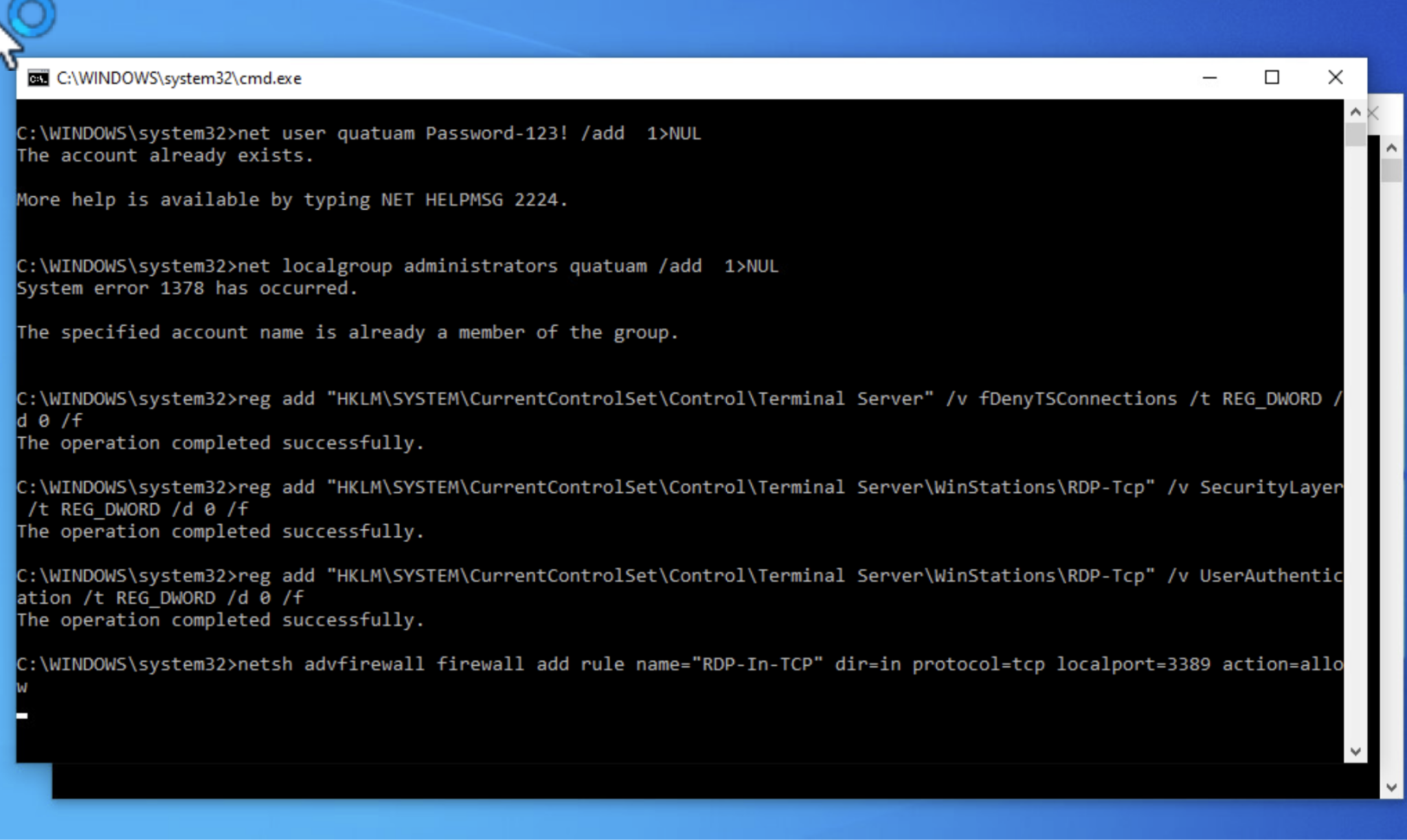


This was found on the router. It is a backdoor that allows anyone to go to the website listed and execute commands found on the router. They can also upload files. Although this is a major security flaw, when it was found, we were able to utilize this to gain access to the machine again when locked out by the red team.

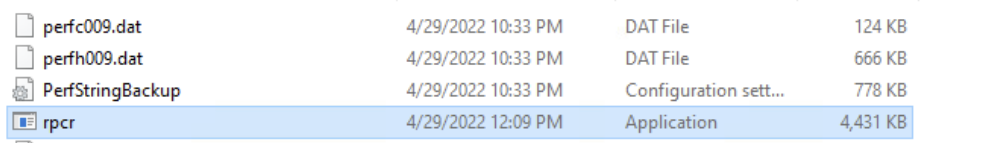


**Windows:**

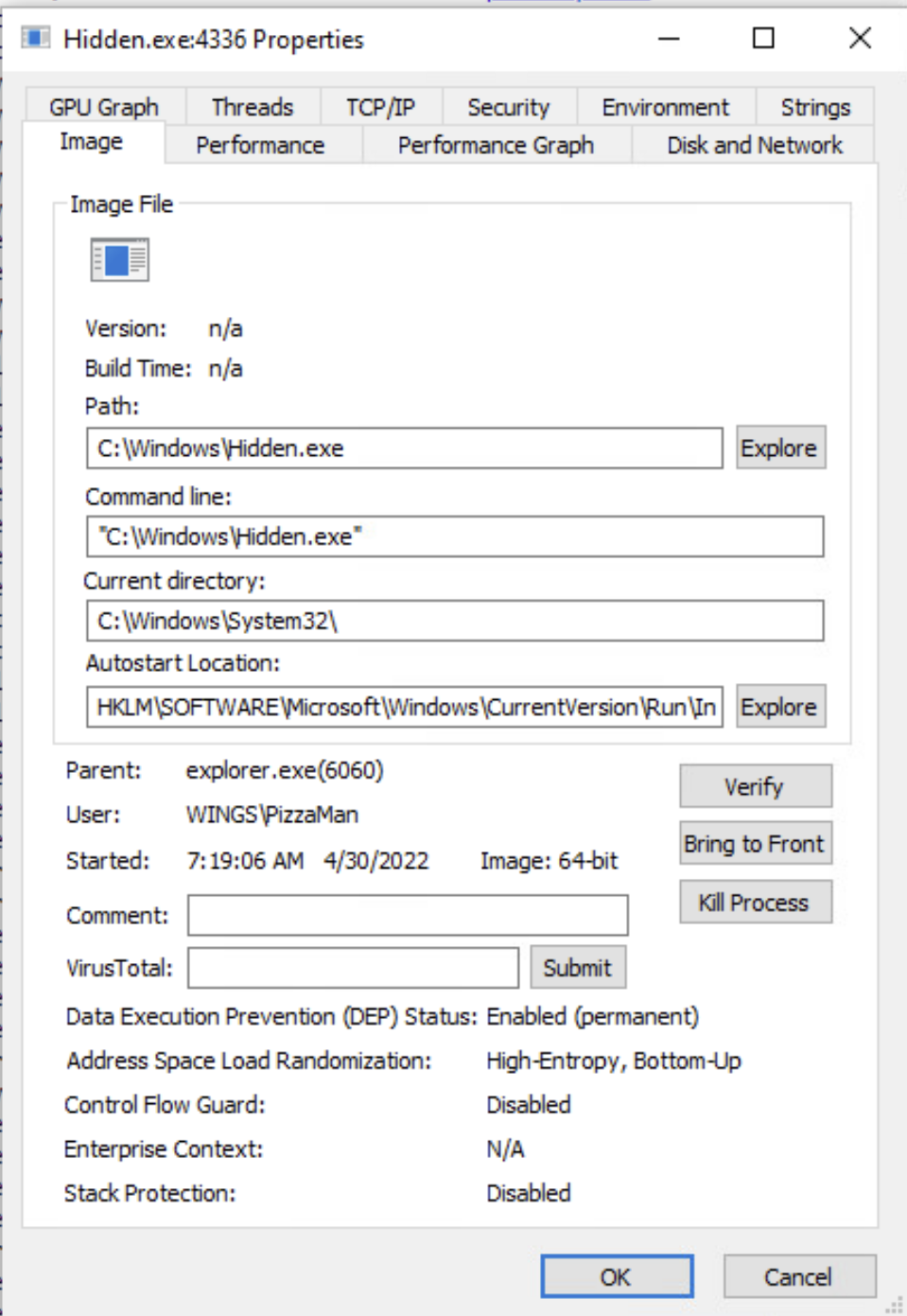
This came from Windows1. This popped up during startup and showed firewall rules being modified unknowingly and additionally users being added unknowingly. This was attached to a script that we found using Autoruns and disabled the execution permissions and quarantined the file professionally.



This was from Windows 1. This was an application. We disabled execution permissions and quarantined the file.



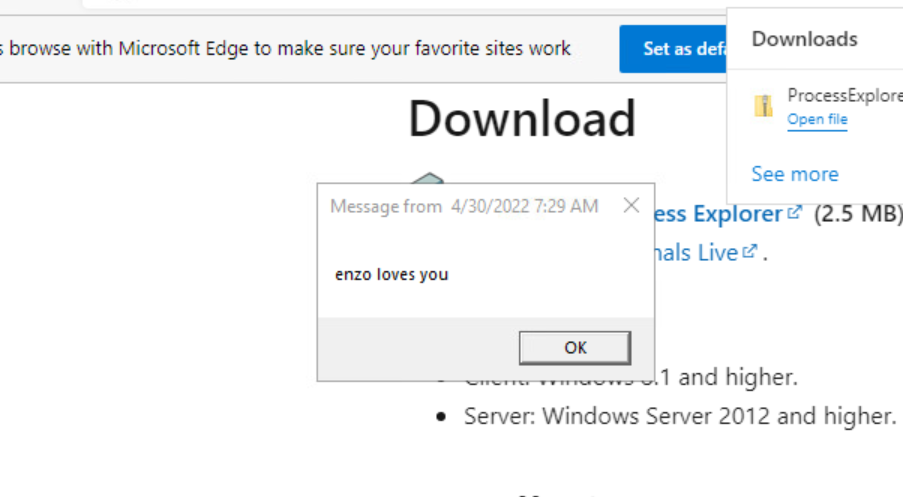
This application was found on Windows 1 and Windows server. We suspended the process, disabled permissions, and quarantined the file.



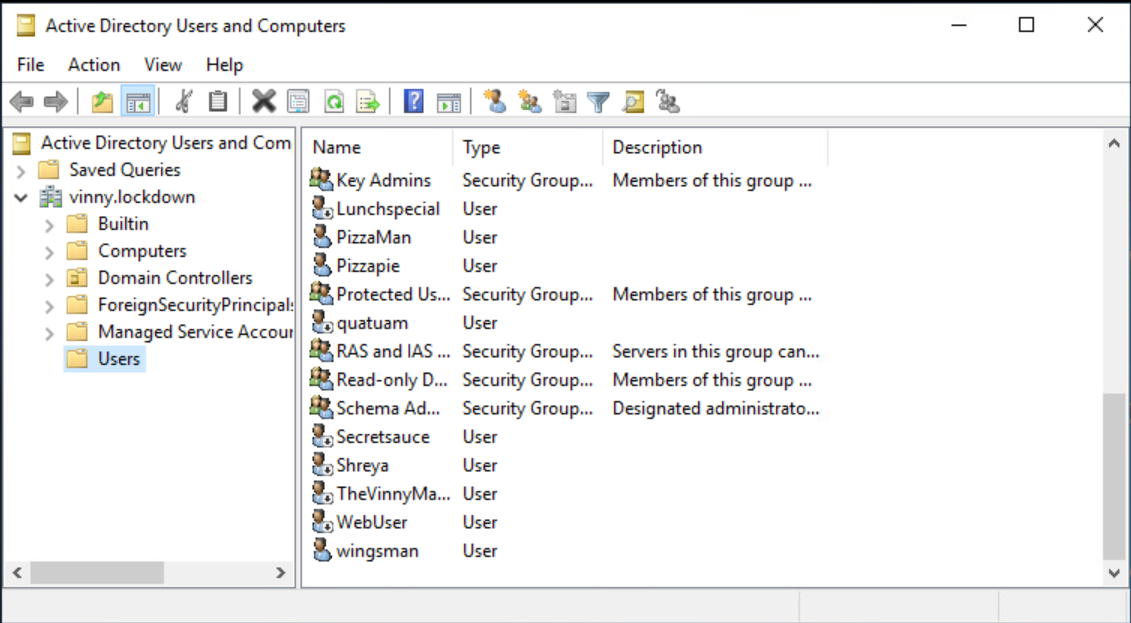
We found this application on the Windows Server 2019 box and disabled execution permissions and quarantined the application.



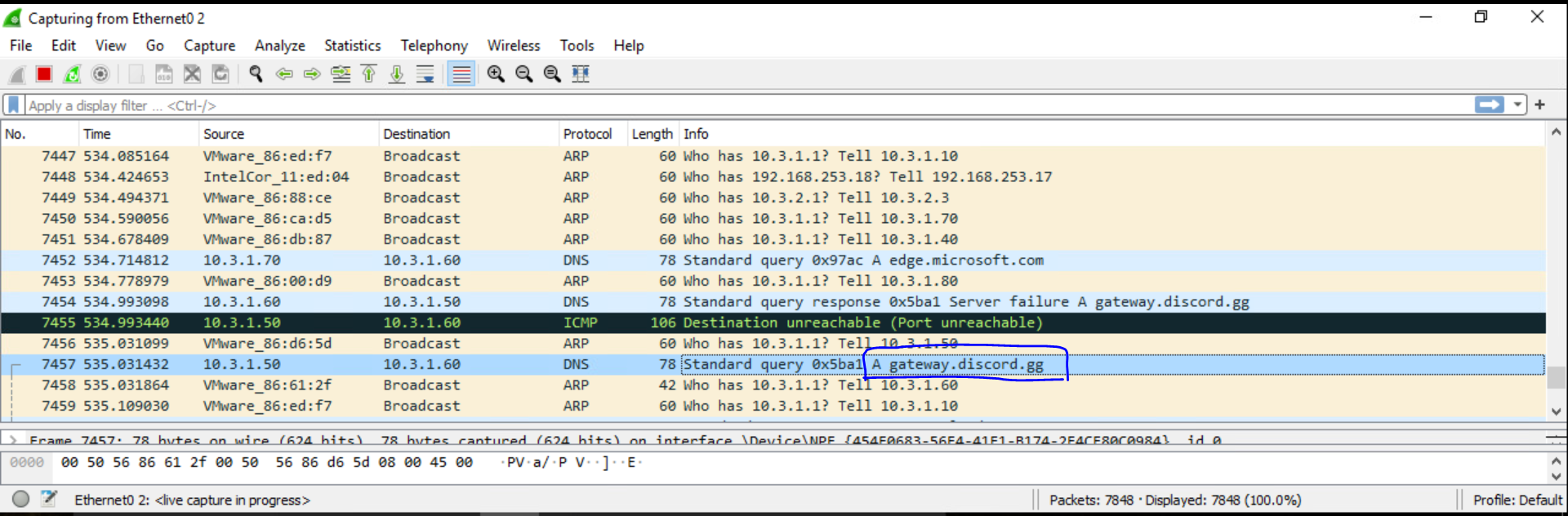
This was a message from Enzo shown on the Windows Server 2019 box. Extra precautions and user privilege reviews were made.



This was a list of users found on the AD Windows Server 2019 machine. Many were unauthorized and promptly disabled.



We found a query for discord.gg occurring on Wireshark traffic. Given no blue team members were attempting to contact discord, this was likely an unauthorized access attempt. Firewalls were updated to block discord for extra security.



We kept the services online for most of the day regardless of the relentless attacks of the red team. The router was our primary point of vulnerability and reinforcing that aspect of the infrastructure more heavily would result in better service uptime.

Best,

Team 3