# I Always Feel Like Somebody's Watching My IoT

## An Analysis of Ring's Security Posture

Authors: Joel Beck, Caleb Brackens, Mahmoud Nobakhti, Ashley Ricketson, Christopher Watson

# Abstract

The purpose of this project is to examine the security vulnerabilities posed by devices from Ring LLC, a home security company owned by Amazon which manufactures products such as doorbells, outdoor and indoor security cameras, and a social networking application.

We will dissect and explore its security risks, citing multiple real-world examples, and describe how malicious actors were able to carry out various attacks and breaches.

Finally, we will investigate ways Ring attempted to mitigate and resolve its security issues and ultimately explore the lessons learned and the best practices moving forward to avoid future security breaches.


# 1. Introduction

There isn't a more violating feeling in the world than having your privacy invaded. It's undoubtedly disturbing when the devices we use to protect and secure our privacy are the ones being hacked and exploited.
In the case of Ring security devices, such breaches could feel like they've been lifted directly out of a horror movie. Imagine the feeling of having your 8-year-old daughter hearing a strange man's voice speaking to her through a security camera's two-way talk feature in her own bedroom while playing a creepy song from the hit horror film "Insidious" plays in the background.

It could happen. In fact, it did.

But more on that in a little bit.

Ring security devices, like so many entities that make up the "Internet of Things" (IoT), can be hacked. And if something can be hacked, chances are there is someone out there trying to do that right now.

IoT refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Such devices have certainly made our lives easier. From monitoring sleeping patterns to tracking activity and progress during workouts to talking to someone through our own doorbell, the devices we use every day are becoming much more sophisticated.

But hackers have become awfully sophisticated themselves. If there is an opportunity to gain access to your info and use it to their advantage, they'll find it. And it's up to companies like Ring to stay ahead of the hacker game and keep their product safe.

Are they doing that? Let's find out..

# 2. How Did They Do It? Possible Attack Vectors Used To Breach Ring Security Devices

## 2.1. Poor and Compromised Credentials

The most common type of breach that potential hackers used on Ring security devices are known as "credential stuffing" attacks. When a user's account information is compromised in a data breach, those stolen credentials might find their way into the hands of malicious actors who will attempt to "stuff" them into other systems. Due to the frequency with which individuals reuse passwords and other login information, a hacker with a large set of stolen credentials to work with will invariably find several accounts that they can breach.

## 2.2. Brute Force

Attackers often used "config files" to perform brute force attacks to gain access to Ring security devices. A config utilizes special software used to rapidly churn through usernames, email addresses, and passwords to try to log into various accounts. Some configs are labeled as "High Checks Per Minute" or "High CPM," meaning it can test if a username and password will allow access to a Ring camera quickly.

## 2.3. Poor Encryption

Previously, IoT security cameras sent data over the network via HTTP. This posed a security risk as HTTP traffic is unencrypted and, thus, insecure. If attackers were able to somehow intercept the traffic between an IoT camera and its server, they could view the same images a security monitor was displaying.

## 2.4. Third and Fourth Party Vendors

In one instance, researchers discovered a flaw in the Ring's Android app that "allowed attackers to exploit the vulnerability by creating and publishing a malicious app — or pushing an update to an existing app — running on the same device. If a would-be victim is tricked into installing a malicious app, it would allow the attackers to obtain authentication cookies. With these cookies, an attacker could access a user's account without their password, allowing the malicious app to steal a Ring user's full name, email address, phone number, and Ring device data, such as camera recordings and geolocation data. Successful attackers could extract more information

from Ring camera recordings themselves, like sensitive information in documents, and items displayed on computer screens. They can even track people's movements in and out of rooms or buildings.

Additionally, an investigation by the Electronic Frontier Foundation of the Ring doorbell app for Android found it to be packed with third-party trackers sending out a plethora of customers' personally identifiable information (PII). Four main analytics and marketing companies were discovered to be receiving information such as names, private IP addresses, mobile network carriers, persistent identifiers, and sensor data on the devices of paying customers.

# 3. Past Exploits of Ring Devices


## 3.1. Details

Password-cracking software used to break into Ring user accounts was offered for sale on a crime forum for just $6.00. A source claiming to have knowledge of the Ring hacks told Newsweek that accounts were accessed by a "very basic attack" known as credential stuffing, a brute force method that tries to access an account using a list of compromised login details. The source stated that "The amount of accounts that are exposed [is] insane. The purpose of Ring is to have security but they leave all their users exposed." On a desktop web browser, someone who is logged in can watch historical, archived footage, meaning that if a hacker gains access to

a user's account, the hacker can watch live and historical footage of a family inside their home without providing any additional identity verification.

Some of the unauthorized hacks were further publicized via the podcast NulledCast. NulledCast streams on Discord, a widely-used Voice over Internet Protocol (VoIP) application (an application that allows users to make voice calls using an internet connection). It is also a digital distribution platform that is designed to allow video gaming communities to live stream games and chat while gaming. On the NulledCast, hackers take over peoples' Ring and Nest smart-home cameras, then use the two-way talk feature to harass their unsuspecting owners. The NulledCast advertises itself as "over 45 minutes of entertainment," including Ring "trolling." Hackers share software for hacking Ring cameras widely on the internet, including a program that churns through previously compromised email addresses and passwords to break into Ring cameras.

According to Motherboard, multiple hacker forums contain tools aimed at brute-forcing Ring cameras. Using so-called "config" files, hackers can try username and password combinations repeatedly and at high speed until they get a hit. Usually, these logins come from unrelated data leaks, but people do tend to reuse passwords despite years of warnings. The tools to do this cost next to nothing — Motherboard found a popular Ring "password checker" was being sold on an unnamed forum for just $6.


## 3.2. Impact on Customer's Security

A family hoped the devices would notify them if their middle daughter, who suffers from seizures, began to experience a seizure while the mother was not home. At first, the cameras gave the family peace of mind and helped their children feel safe. That sense of security disappeared on December 4, 2019. Shortly after 8 p.m, both of the Ring cameras installed in the family's home began live-streaming, and the Tiny Tim cover of "Tiptoe Through

the Tulips," a song that appeared in a scene from the 2020 horror film "Insidious," began to play through the two-way talk feature. Intrigued by the music, the family's eight-year-old daughter, Alyssa, went to the room she shares with two of her younger sisters to investigate. But the room was empty. As Alyssa wandered the room, looking for the source of the music, the song abruptly stopped, and a man's voice rang out: "Hello there." It was a stranger — an unknown hacker, who had taken over the family's account and had the ability to see, hear and speak to Alyssa inside her own room. In a chilling exchange captured on the device's video recording, the hacker began shouting racial slurs at Alyssa. and encouraging her to misbehave. Alyssa, confused, asked, "Who is that?" The man responded: "I'm your best friend. I'm Santa Claus. Don't you want to be my best friend?" He told Alyssa that she could do "whatever you want… Mess up your room, break your TV." The encounter ended only after a frightened Alyssa left the room to find her father, who disabled the device.

Only a few days later, the same thing happened to Mr. Craig and Ms. Amador when an unauthorized hacker took control of the Ring system that they share in their home. On December 9, 2019, Mr. Craig and Ms. Amador were interrupted by a voice laughing and shouting, "Ring support! Ring support!" Ms. Amador, who was napping, was awakened by the noise. Mr. Craig was standing in front of his indoor camera at the time of the breach, and jumped at the sound, at first believing Ms. Amador was playing a joke on him. But this was no joke. A stranger had hacked Mr. Craig's Ring system and was spying on the couple inside their home. The hacker then accessed the couple's doorbell camera and told them, "I'm outside your front door." The voice also threatened the couple with "termination" if they did not pay a ransom of 50 bitcoin.

# 4. Device Testing

We ran several tests (ranging from passive recon to basic adversary emulation) on a Ring Indoor Cam as well as several other Wi-Fi-connected security cameras: Wyze Cam V2, Night Owl's Wi-Fi IP Camera, and Merkury Innovations' Smart Wi-Fi Camera. Our goal was to identify Indicators of Compromises and then compare and contrast the different devices. All four cameras are internet-connected, require users to download an app to interact with the device, and are marketed for home security.

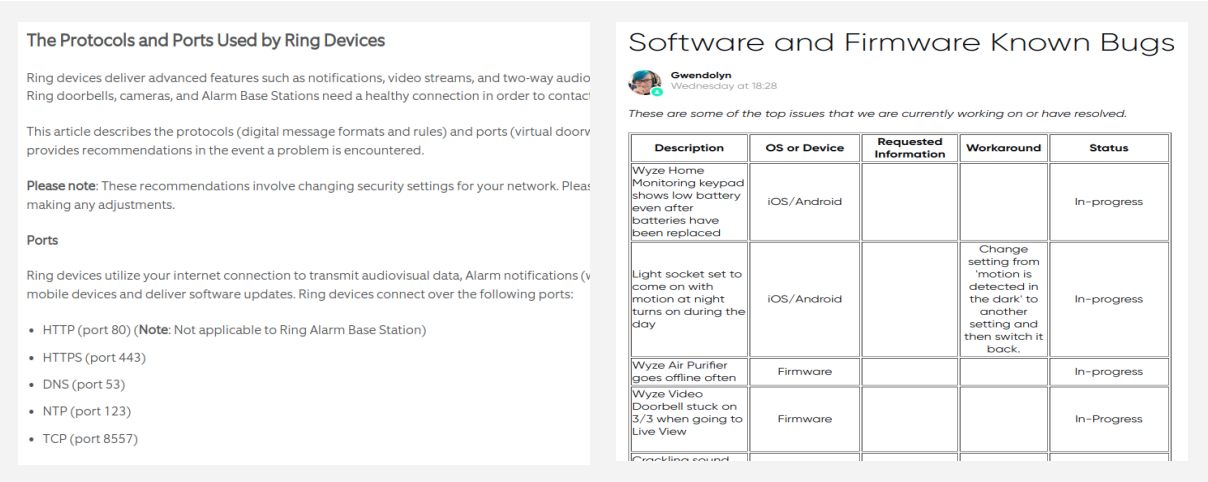
## 4.1. Procedures

To best assess each device's security posture, we emulated the first step of Lockheed Martin's Cyber Attack Chain, Reconnaissance. The tools and methods chosen are readily accessible to any malicious actors and are known to be effective. Below, we've outlined the steps taken.

## ■ Passive Reconnaissance

To get an idea of what to expect, information on devices' security policies, ports, procedures, bugs, updates, and patches were compiled. Only official communication from the manufacturers' websites was included. Wyze provides ample information while Ring shares ports and protocols utilized but does not release firmware update information. No information was found for Merkury or Night Owl.

Findings are listed in Data Table 2 below.



**The Protocols and Ports Used by Ring Devices**

Ring devices deliver advanced features such as notifications, video streams, and two-way audio
Ring doorbells, cameras, and Alarm Base Stations need a healthy connection in order to contact

This article describes the protocols (digital message formats and rules) and ports (virtual doorv
provides recommendations in the event a problem is encountered.

**Please note**: These recommendations involve changing security settings for your network. Pleas
making any adjustments.

**Ports**

Ring devices utilize your internet connection to transmit audiovisual data, Alarm notifications (v
mobile devices and deliver software updates. Ring devices connect over the following ports:

- HTTP (port 80) (**Note**: Not applicable to Ring Alarm Base Station)
- HTTPS (port 443)
- DNS (port 53)
- NTP (port 123)
- TCP (port 8557)

**Software and Firmware Known Bugs**

**Gwendolyn**
Wednesday at 18:28

*These are some of the top issues that we are currently working on or have resolved.*

| Description | OS or Device | Requested Information | Workaround | Status |
|---|---|---|---|---|
| Wyze Home Monitoring keypad shows low battery even after batteries have been replaced | iOS/Android | | | In-progress |
| Light socket set to come on with motion at night turns on during the day | iOS/Android | | Change setting from 'motion is detected in the dark' to another setting and then switch it back. | In-progress |
| Wyze Air Purifier goes offline often | Firmware | | | In-progress |
| Wyze Video Doorbell stuck on 3/3 when going to Live View | Firmware | | | In-Progress |

*Figure 1: Ring and Wyze websites sharing security information*

## ■ Initial Set-Up

During the initial set-up of devices, we acted as new users and tried to create the weakest credentials possible. We wanted to emulate the typical user experience of a non-security-minded individual. With the exception of the Ring devices, accounts were created through each device's official app (Ring's account created occurred on its website to avoid Two-Step A prompts).

Findings are listed in Data Table 1 below.

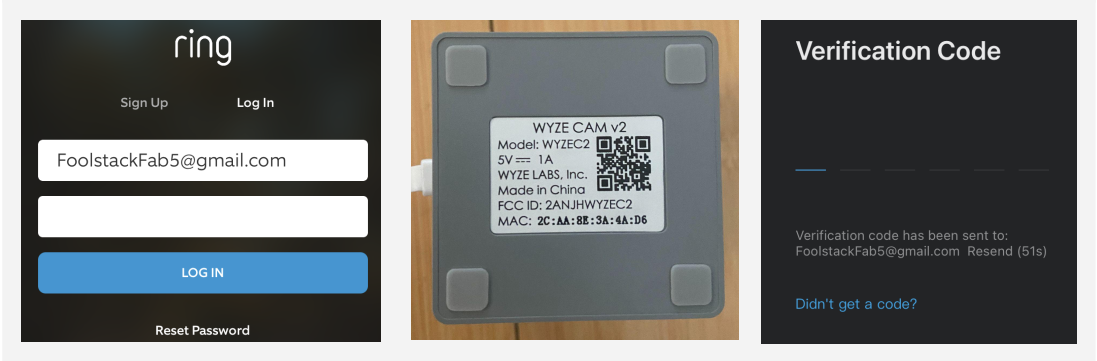



*Figure 2: Devices utilized various verification methods including codes sent to email, physical QR codes and traditional login*

## ■ Scans: Port, Vulnerability and Web Content

With the devices connected to our network, we identified the IP and MAC addresses and then began conducting scans. First, we scanned for open ports and protocols in use with the Nmap port scanner tool. Then, we used the vulnerability scanner Nikto to scan HTTP and HTTPS servers to quickly identify any vulnerabilities. Only the Night Owl device was able to be scanned using Nikto. Finally, we used a web content scanner, Dirb, to enumerate through open web servers by attempting to connect to common subdirectories of the webroot.

Findings are listed in Data Table 3 below.


*Figure 3: Scans performed on devices are mostly blocked*

## ■ Packet Sniffing

Using a method outlined by Null Byte, we attempted to view data transmitted via Wi-Fi using **Wireshark** and the **aircrack-ng** suite. By monitoring wi-fi traffic and then forcing all devices to reauthenticate, we were able to observe handshakes with the network. Although this method is meant for cameras that use the HTTP protocol, it was useful for picking up on encryption methods, and ports utilized and exploring how the industry has responded to past vulnerabilities.

Findings are listed in Data Table 3 below.

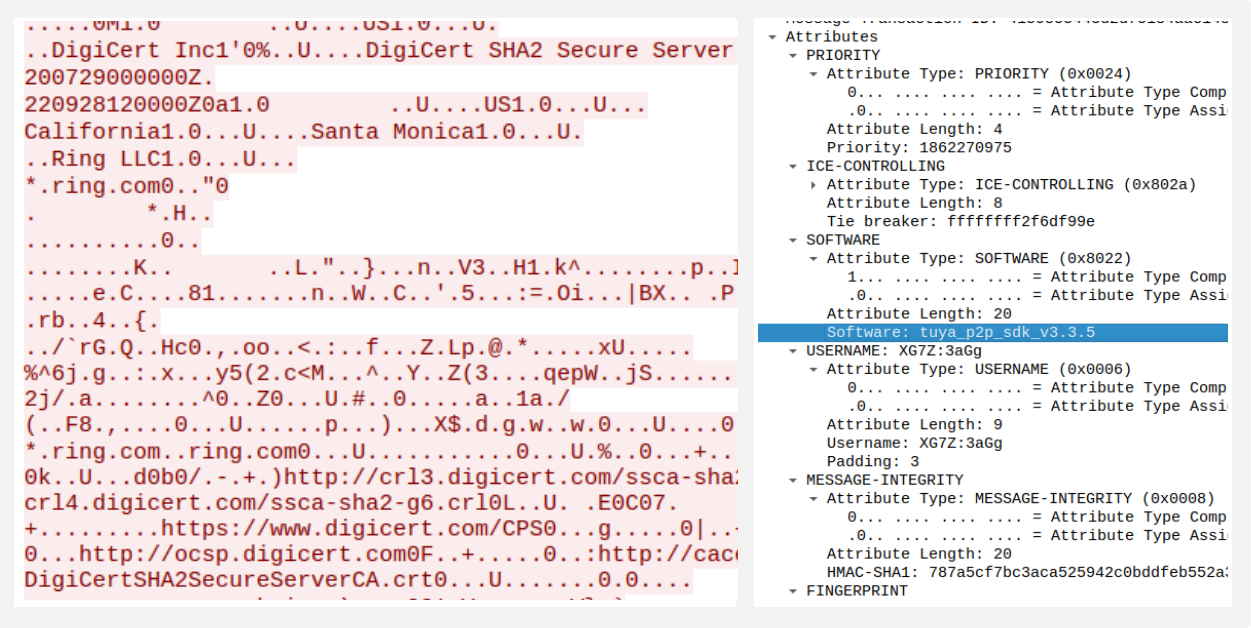



*Figure 4: Examples of visible traffic from devices*

## 4.2. Findings

Overall, Ring performed extremely well compared to other devices tested. At least two Potentials for Compromise were found for each device other than the Ring camera. This does not mean the Ring camera does not have vulnerabilities - only that it has been properly secured against the reconnaissance techniques tested in this paper.

- Data Tables

Table 1: Credentials

| | ring VIDEO DOORBELL | NIGHT OWL | WYZE CAM | MERKURY INNOVATIONS |
|---|---|---|---|---|
| QR Code | Directs user to Google Play / Apple App Store | Only used for pairing devices | Directs user to Google Play / Apple App Store | Directs user to a Google Search for Wyze's set-up guides |
| Credentials Input Form | Password field is hidden until valid email is entered | Both Username and Password fields visible | Both Username and Password fields visible | Both Username and Password fields visible |

| | | | | |
|---|---|---|---|---|
| Multi-Step Verification | Encouraged but not required; Asks every time user opens app | Requires a valid phone number for Multi-Step Verification | Encouraged but not required; Only asks during set-up | Not required |
| Accepted Password | "Password1?" | "Password1?" | "Password01" | "Password1?" |
| Location Tracking | User must set location, but Location Services can be off | Location Services required for set-up | Not required | Not required |

Table 2: Initial Recon

| | ring VIDEO DOORBELL | NIGHT OWL | WYZE CAM | MERKURY INNOVATIONS |
|---|---|---|---|---|
| Transparency Level | Proactively Translucent | Opaque | Proactively Transparent | Opaque |
| Listed TCP Port Communication | 53<br>80<br>123<br>443<br>6970<br>8557<br>9998<br>9999<br>15063<br>15064 | - | 80<br>123<br>443<br>8443<br>8605<br>10001<br>10002<br>22345 | - |
| Listed UDP Port Communication | 7076<br>7077<br>9078<br>9079<br>15063<br>15064 | - | 80<br>443 | - |
| Encryption | TKIP^<br>AES | - | AES | - |
| Apps and Services | Ring Socket Service | - | AWS IoT Core<br>WebRTC | - |

Table 3: Traffic & Scan Analysis

| ring VIDEO DOORBELL | NIGHT OWL | WYZE CAM | MERKURY INNOVATIONS |
|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Significant TCP Port Communication | 53<br>123<br>443 | 443<br>554<br>1300<br>6060<br>6061<br>7000<br>8012<br>8089<br>8699<br>45936 | 6668 | 68<br>443<br>6668 |
| Significant UDP Port Communication | 68<br>25465 | - | - | 443 |
| Protocols Used | ICMP<br>IGMP*<br>NTP<br>SIP^<br>TLSv1.2<br>UDP Lite* | H.323<br>ICMP<br>IGMP*<br>RTSP<br>TLS<br>UDP Lite*<br>X11 | EMCOM*<br>ESP*<br>ICMP<br>IGMP*<br>SCTP<br>TLS^<br>UDP Lite* | ICMP<br>IGMP*<br>QUIC<br>SCTP<br>SS7<br>STUN<br>UDP Lite* |
| Encryption | SHA2 | Not Found | Not Found | HMAC SHA1 |
| Apps and Services | - | afs3-fileserver | IRC | Tuya P2P |

* Port is filtered

## ■ Potentials for Compromise

Gathered information could be used by malicious actors to begin deciding how to weaponize vulnerabilities. Carrying out specific attacks is outside the scope of this paper, however, we were able to find several Potentials for Compromise that IoT manufacturers should address. Ring's performance in each category is noted in bold.

### ● Obscure Security Transparency

Although it may seem counterintuitive to the average computer user, transparency is extremely important in cybersecurity. Transparency allows security researchers to accurately test devices and encourages information sharing which can lead to vulnerabilities being quickly addressed. Companies that obscure their security transparency are more likely to have zero-day exploits floating around on the dark web.

We classify Ring's transparency as translucent.

### ● Malicious Apps

As sensitive information is used to verify credentials, users need to ensure they are interacting with their devices through official applications. Several high-profile exploits utilized malicious apps that posed as official ones to steal credentials or upload malware. Select devices are still

vulnerable to this type of attack (See Figure 3)

Ring effectively safeguards against malicious apps.

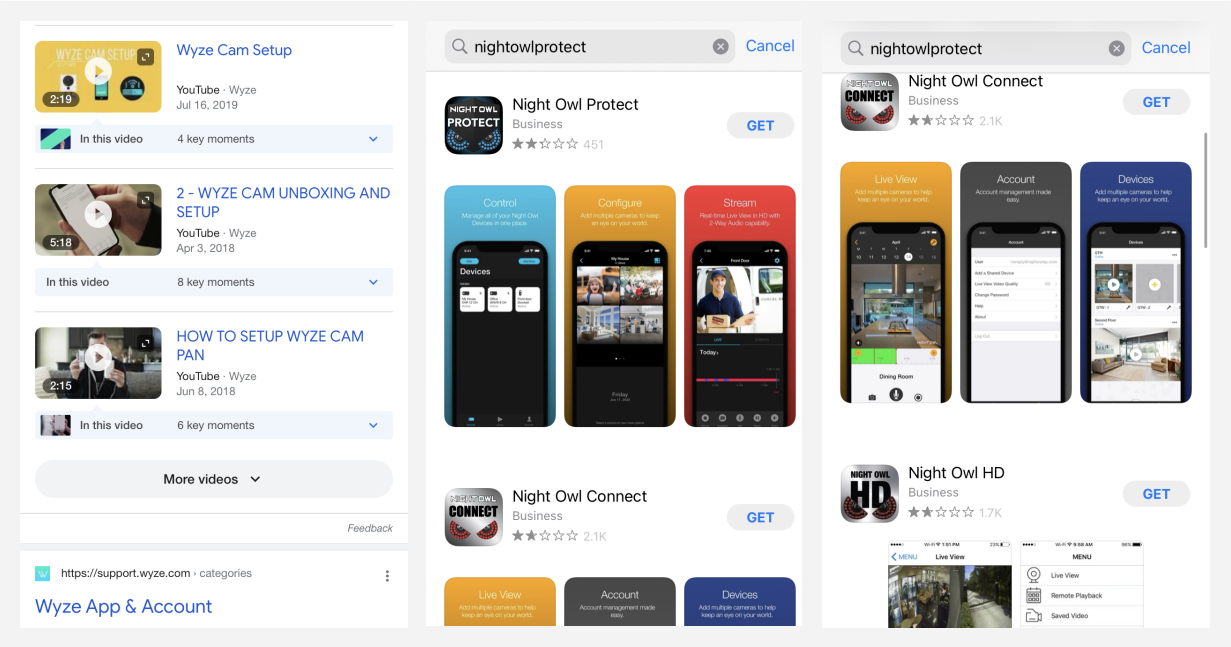



*Figure 5: Failing to properly direct users could allow malicious apps to impersonate official ones - potentially exposing user credentials, devices or networks*

- Weak User Credentials

Weak user credentials open the door for brute-force attacks as attackers have many tools at their disposal with the ability to quickly attempt any combination of username and password. Although it is impossible to completely stop this type of attack, device manufacturers can make the time for a successful brute-force attack exponentially longer with good authentication policies.

Ring LLC. has safeguards against this type of attack due to the input form separation, preventing users from using common passwords and requiring a mix of character types. However, password length is still inadequate.

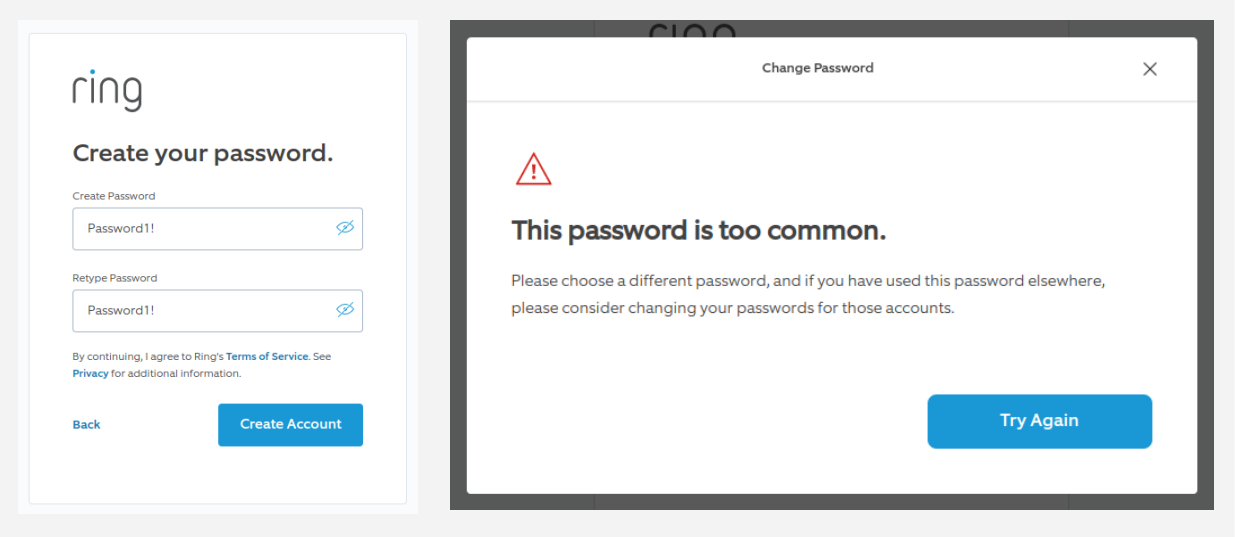



*Figure 6: Ring's Password Policy preventing a weak password*

- UDP Protocols

The use of UDP protocols is interesting. UDP, by default, requires no handshake thus making it less secure than TCP in its native implementation. However, this doesn't mean their use is a security threat. For example, QUIC is a relatively new UDP Protocol and, thus, isn't quickly detected by firewalls or IDS/IDPs leaving a potential vulnerability for malicious attackers.

Ring uses UDP ports and protocols, but limits their use to necessary traffic or variable unstandardized ports.

- Incomplete Port Hardening

Ideally, traffic to and from a device should only exist between a device and its intended destination. However, improperly hardened ports can open a device's traffic up to any malicious attacker. Readily available scanning tools can allow an attacker to quickly identify attack vectors.

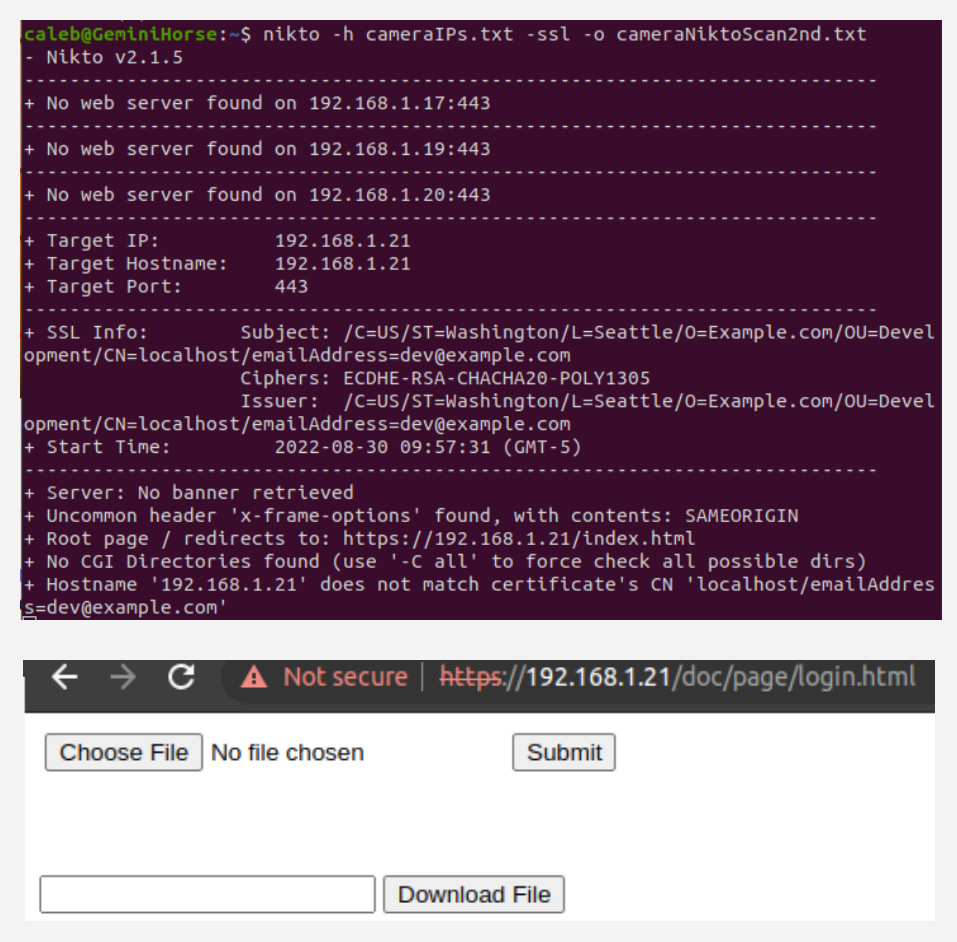



*Figure 8: nikto identified a potential Attack Vector for the Night Owl*

Ring is detectable on the network, but has successfully hardened itself against simple scans.

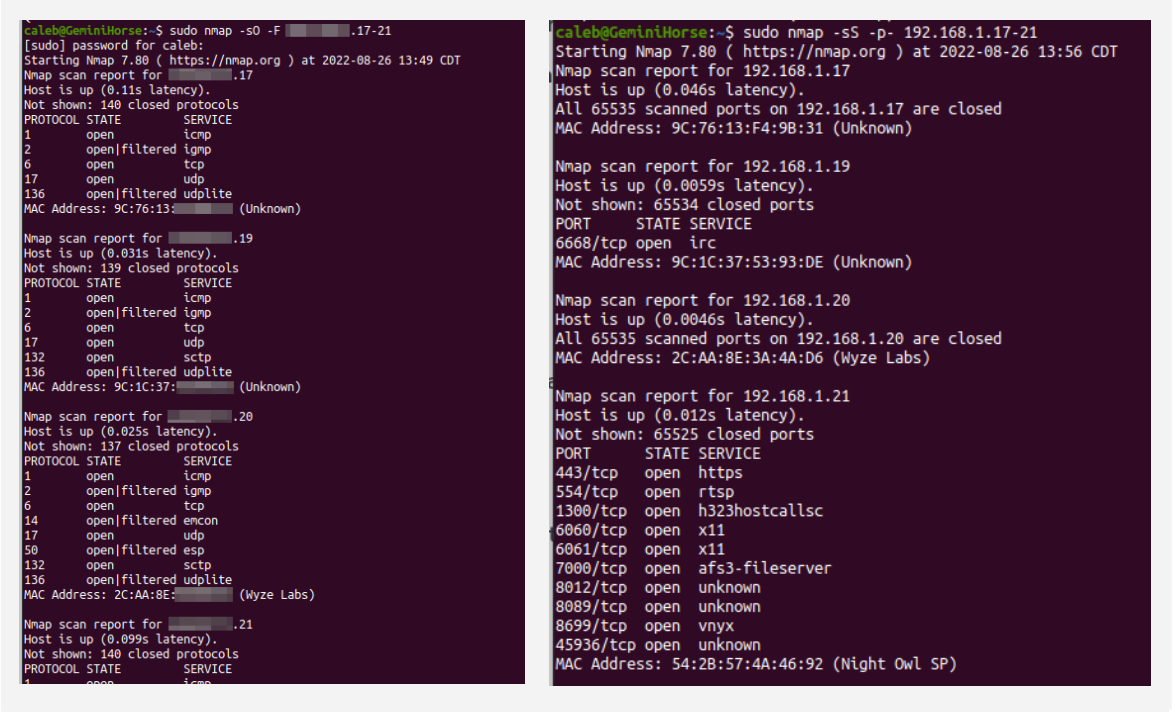



*Figure 7: Some devices provide a worrying amount of information from simple scans.*

- Vulnerable Services

Even if a manufacturer follows all the best practices to ensure their devices have little to no vulnerabilities, it means nothing if they utilize insecure services. In the devices tested, we found Tuya services(known to connect to siphon data to the Chinese government) and IRC (outdated service with many known vulnerabilities) - both known to be insecure.

No vulnerable services were found on Ring's device.

# 5. Mitigation

## 5.1. Industry

- Constant updates

Ring is constantly updating their application in order to combat new security threats. While the physical devices may require replacement with newer models due to hardware limitations, Ring is committed to guaranteed software security updates to every model until up to at least four years after the model's discontinuance.

- Don't share footage

In 2009, Ring was criticized for using videos shared on its Neighbors app to provide tips on suspects. Recently, in 2022, Senator Ed Markey has criticized Ring for presenting security

footage to law enforcement without a warrant or permission from the Ring camera owners. These practices, which are supposedly allowed within their policy, can potentially violate civil liberties and personal privacy, leading to malicious activity using Ring security footage.

- Delete old footage

In the event that a hacker accesses someone's account, they can potentially access Ring security footage. Ring should incorporate an option to automatically remove security footage after a determined time frame, mitigating potential theft of security footage from previous months or years that are now irrelevant.

## 5.2. Consumer

- Strong password

The consumer is responsible for creating a complicated password that hackers cannot easily guess. Hackers can develop automated programs to brute force hack an account. The more complicated the password, the longer it will take for the hacker to brute force one's Ring account.

- Switch passwords regularly

In the event a hacker is able to get your password, changing passwords regularly will force hackers to continue guessing. Using a password generator will also allow for more regular password changes without the burden of inventing a brand new unique password. In the event one forgets new passwords, investing in a password vault can be feasible.

- Add a shared user for emergencies

The Ring app and Video Doorbell come with a flexible feature for adding a "Shared User" to your account. This way you can still provide Ring access to others while keeping your account information secure. Inviting a relative or close friend to view camera footage and speak with people at the door can create a security measure by using multiple witnesses to monitor what's going on around the house without exposing sensitive login information.

- Use separate passwords for different accounts

One common mistake that consumers make is using the same password for multiple accounts. While it is understandably easy to remember the exact same password for every account you make, it becomes a security risk when the same password that was used to hack your laptop,

Facebook, and email address is the same as the one for your Ring doorbell.

- Use the Ring app to enable 2-step verification

This security measure requires direct access to one's email address in order to advance. Ring's two-step verification process creates a temporary password and sends it to the email address associated with the account. Therefore, if a hacker has accessed the password to your Ring account, but not your email address, the hacker will not be able to view the Ring account. The hacker will be hit with a prompt to type said password.

- Antivirus or firewall solution

Purchasing a stand-alone firewall and antivirus service can prevent hackers from hacking your system and protect your network from other threats, such as malware and ransomware. Additionally, one can invest in a virtual private network to mask the IP address of any IoT device, as most hackers can access networks through the IP address. VPN's can also encrypt data that is transferred through the network, preventing unauthorized people from accessing the data intended for a certain period.

- Network segmentation

This tactic works by separating your network into multiple isolated chunks, each with separate devices on it. The benefit of network segmentation is so devices can't access devices or data outside their own segment of the network. Managing the network access your IoT devices have can help you minimize the risk of unauthorized network access, even if a smart device is compromised.

- Mount your devices securely to prevent them from being stolen

Sometimes it's not a matter of hacking, but a matter of physical theft. All Ring doorbells come with one or two security screws which make it so that the doorbell cannot be easily removed. Also, if you can install your doorbell on a stucco wall with anchors, it will be even more difficult to remove. However, the security screws are also not full proof from theft. There are more ways to protect against theft: Install an anti-theft grid box over your Ring doorbell. A grid box can be purchased at your local hardware store. Install an outdoor Ring camera with a built-in light and siren which you can activate through the Ring app to scare off potential thieves. Purchase a security yard sign to inform potential thieves that they will be recorded if they are on your property. Download and sign up for Ring's Neighbors app to receive notifications from your neighbors and local law enforcement about incidents in your neighborhood. Ring will also offer a free replacement in the event of theft.

- Safeguard your Wi-Fi with a guest network and use a strong password

Guest networks are useful for private users whenever someone has company. It prevents others from accessing your internal network. There are many ways to secure your personal Wi-Fi, some of which involve the creation of hidden home networks for your home devices. Some routers can isolate guests from each other. Users won't see each other on the network and someone with malicious intentions won't be able to harm others. One can maintain separate sets of rules for your personal and guest networks. you can use a shorter, more memorable password for guests while keeping your longer, more secure private network password secret. The primary purpose of this security measure is to protect the internal network from malware, illegal downloads, and hackers tracking data through the internal network.

# 6. Final Thoughts

Companies like Ring have made great strides to address the risks posed from past security breaches. Of the devices we tested, Ring has done the most to protect its IoT devices from malicious actors. That being said, it's up to the industry to remain vigilant in staying ahead of the hacker game and to help consumers stay informed on how to take the proper steps to protect their own security.

# 7. References


1. https://www.digitaltrends.com/home/how-to-prevent-your-ring-smart-camera-from-being-hacked/
2. https://www.makeuseof.com/ring-doorbell-hack/
3. https://nordvpn.com/blog/ring-doorbell-hack/
4. https://www.geekwire.com/2020/ring-customers-cameras-breached-hackers-sue-amazon-proposed-class-action-lawsuit/
5. https://thehill.com/opinion/cybersecurity/564962-tuya-may-be-the-china-threat-that-beats-russias-ransomware-attacks/
6. https://nmap.org/nsedoc/scripts/irc-unrealircd-backdoor.html
7. https://support.ring.com/hc/en-us/articles/360050167211-Ring-devices-software-security-updates
8. https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant#:~:text=Ring%20Reveals%20They%20Give%20Videos%20to%20Police%20Without%20User%20Consent%20or%20a%20Warrant,-Share%20It%20Share&text=Amazon's%20Ring%20devices%20are%20not,them%20to%20be%20or%20not.
9. https://youtu.be/GnIIEQt_QFo