

# Hacking into Video Surveillance Systems

White Paper



**DATE:** 28<sup>th</sup> September 2015

**VERSION:** V1R1

**AUTHOR:** Ashutosh Sharma



## Introduction

Internet Network, due to its dependency over multiple routers, is susceptible to unexpected hacking from anywhere in the world. In computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. In surveillance domain, it becomes very crucial to safeguard the files and credentials in such a way that it becomes nigh impossible for external stimuli to sneak upon.

Although it is impossible to achieve 100% security in any enterprise, attempts can be made to make the system extremely secure so that it becomes hopeless for hackers to hack into the internal system. This white paper explains how the Video Surveillance Systems can be hacked and the preventive measures that can be taken to avoid the same.

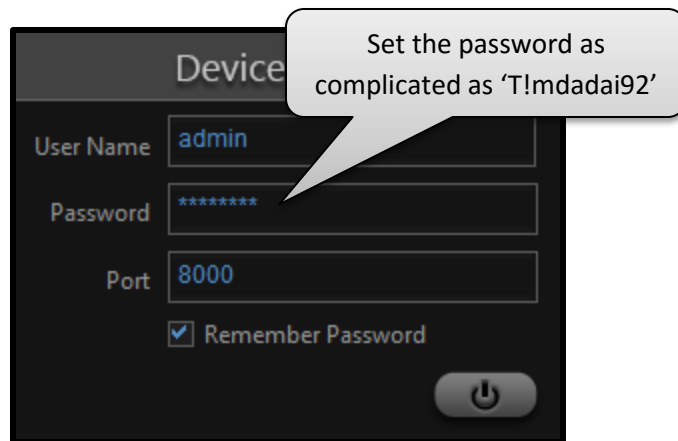
### Video Surveillance Systems can be hacked if:

- Online connected devices utilize usual IP outlet ports, e.g.: port 80 (HTTP), port 21 (FTP), and also port 23 (Telnet), or the standard ports.
- All internet connected devices will send and receive data if a ping request occurs.
- The default password has not been changed or a simple password consisting of a word and not a mixture of symbols numbers, special characters and capitals have been used.
- The system has not been secured by encryption so it is therefore open to be controlled from any external source.

### 11 tips to protect your security systems from getting hacked:

1. **Secure Passwords:** When you install any security system, the first thing you should do is change the default password. You should choose your password wisely which isn't easy to guess. Make sure your password is a combination of symbols, letters and numbers.

Modify the password on the Video Surveillance System with lower and uppercase letters and symbols- THIS IS A NECESSITY. Make it super complicated.



- 2. Secure your router:** If you use a Wi-Fi network for your security system, always keep it protected with a password. Avoid using birthdays and phone numbers as your password.

Though this may seem a bit of a hassle, there is minimum risk of hacking involved with wired security systems. Installing a wired security system may be a good idea for enterprises. You should be aware that if you are providing access to Video Surveillance System to your employees in remote location, they will need a public IP Address. As a result, they can reach to the router in your company anytime. Therefore, always keep your main gateway router secured with a complicated password.

- 3. Change the ports:** Don't allow your NVR/HVR to respond to a ping request. You don't want any other internet device to be able to try if your device can "talk" to it. You should be the only one who should be able to do this once you log in to your password encrypted software. Alternatively, you can change the ports of the NVR/HVR if allowed.

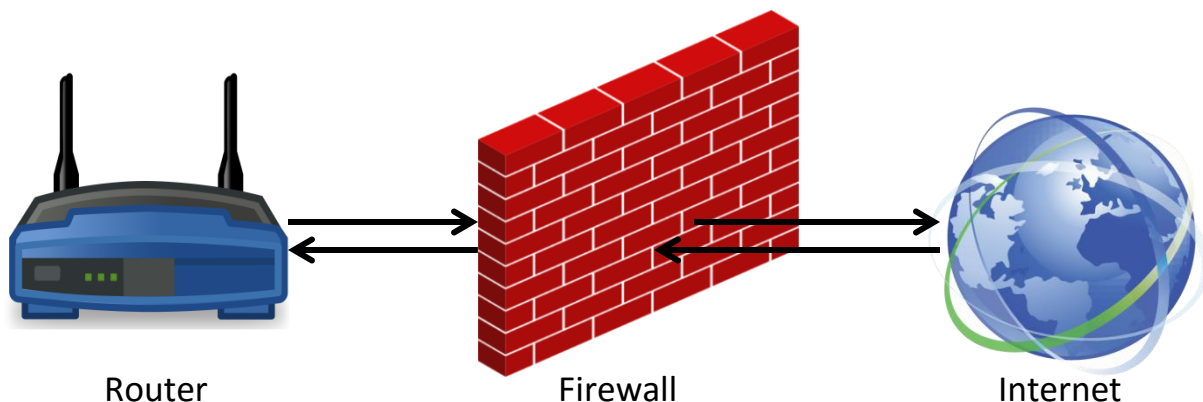
If this function is not feasible, alter the router setups to utilize Port Forwarding, so that web traffic on a certain inbound port number of the router will be sent to the appropriate port of the NVR/HVR on your network.

HTTP Port	<input type="text" value="80"/>	(80, 1024 - 65535)
TCP Port	<input type="text" value="8000"/>	(1024 - 65535)

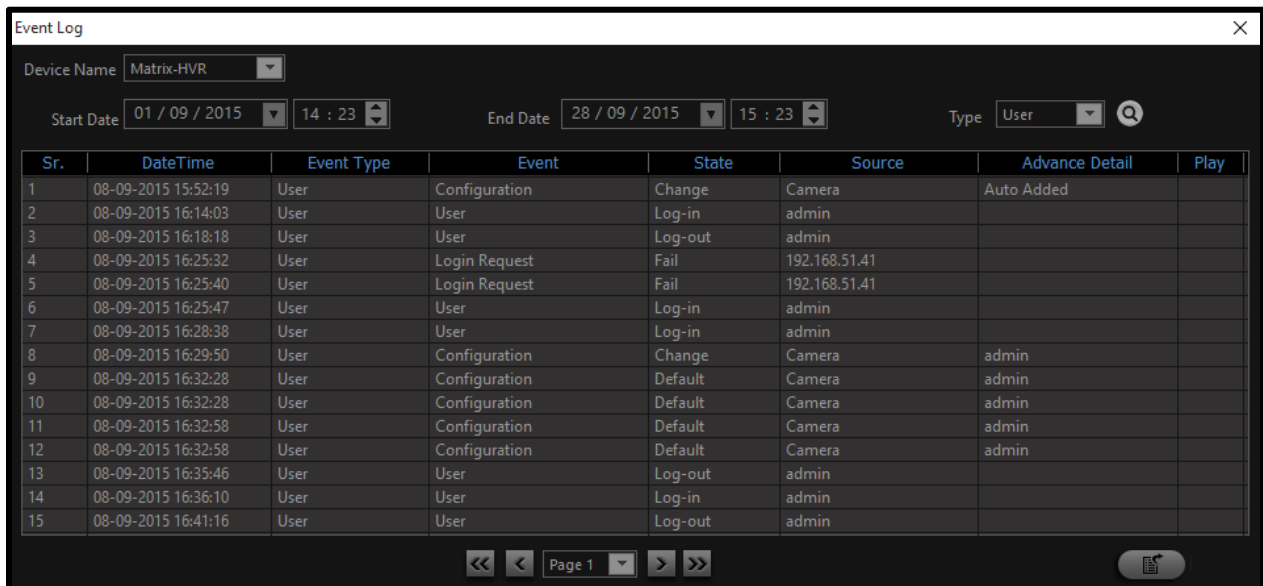
4. **Update the firmware:** See to it that you regularly update the firmware on the Video Surveillance System to keep it up to day with the latest security threats. Manufactures will regularly update their software to counteract new threats they have detected.

<b>Firmware Upgrade</b>
<b>Shutdown</b>
<b>Restart</b>
<b>Default</b>
<b>Backup Configuration</b>
<b>Restore Configuration</b>

5. **Router's firewall:** Configure your router's Firewall software– if you don't want to give, any person on the external network, access to your Video Surveillance System. With the firewall program that comes along with your router you can also ban particular IP (Internet Protocol) and MAC (Media Access Control) addresses from accessing your Video Surveillance Systems.



- 6. Keep a check on your camera/device logs:** If you have a surveillance system, protect it from being hacked by regularly checking the IP history of the system. This will help you know if a stranger has tried to access your surveillance system from an unidentified or unknown IP address. Also, avoid purchasing used camera systems as they may carry an implantable device that can be used by burglars to hack into the system.
- In fact, every time you login, check the logs to identify who all are accessing your system. If you find any anonymity, immediately, change the administrative password.



Sr.	DateTime	Event Type	Event	State	Source	Advance Detail	Play
1	08-09-2015 15:52:19	User	Configuration	Change	Camera	Auto Added	
2	08-09-2015 16:14:03	User	User	Log-in	admin		
3	08-09-2015 16:18:18	User	User	Log-out	admin		
4	08-09-2015 16:25:32	User	Login Request	Fail	192.168.51.41		
5	08-09-2015 16:25:40	User	Login Request	Fail	192.168.51.41		
6	08-09-2015 16:25:47	User	User	Log-in	admin		
7	08-09-2015 16:28:38	User	User	Log-in	admin		
8	08-09-2015 16:29:50	User	Configuration	Change	Camera	admin	
9	08-09-2015 16:32:28	User	Configuration	Default	Camera	admin	
10	08-09-2015 16:32:28	User	Configuration	Default	Camera	admin	
11	08-09-2015 16:32:58	User	Configuration	Default	Camera	admin	
12	08-09-2015 16:32:58	User	Configuration	Default	Camera	admin	
13	08-09-2015 16:35:46	User	User	Log-out	admin		
14	08-09-2015 16:36:10	User	User	Log-in	admin		
15	08-09-2015 16:41:16	User	User	Log-out	admin		

- 7. Regularly change the passwords:** Keep a habit of changing the administrator's password at least once a month. Never use/keep the default passwords.



- 8. Limit Non-approved devices:** You can limit the number of devices that can be used to access your security system.



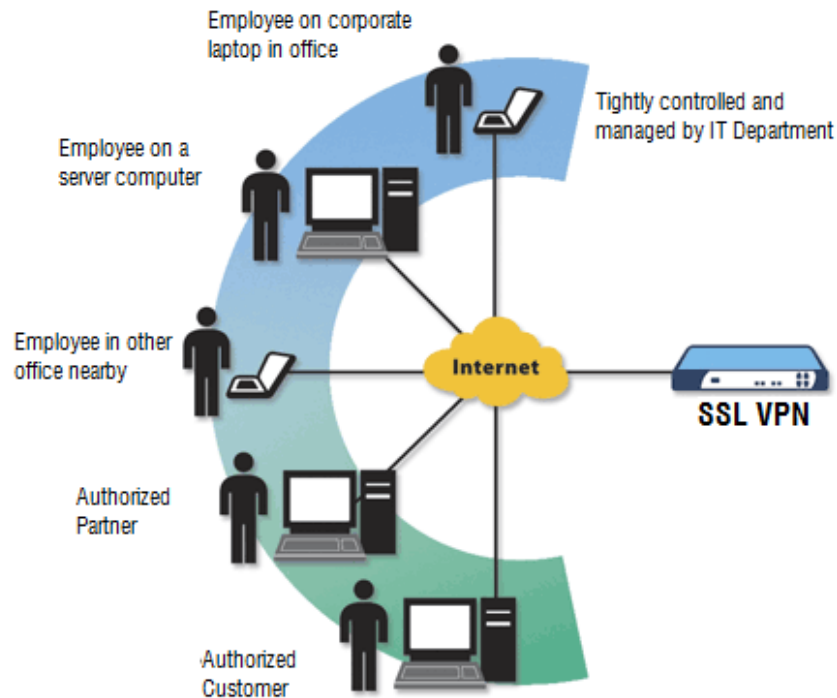
Unauthorized user

- 9. Avoid sharing credentials:** For a live security system implemented in a company, it is never recommended to disclose the administrative password to more than two persons. If required anyway, create the users with limited login rights and provide them the passwords.



- 10. Use VPNs:** With improved security for exchanging data, VPNs are boons to large enterprises. Wherever possible, use a Virtual Private Network in the company to let employees in the remote location access the security system. This way, three-level security will be created allowing only the rightful person to access the security system.

Always avoid putting a security device (IP Camera, Recorder, etc.) directly on the public network without any NAT in front of it. Such scenarios help hackers reach security devices very easily (This is just like putting your house's main door always open).



Keep these steps in mind and enjoy a more secure, flexible and adaptable Video Surveillance Systems to safeguard the important recorded files in your companies.

**Disclaimer:** The information contained in this e-mail and/or attachment may contain confidential or privileged information. Unauthorized use, disclosure or copying is strictly prohibited and may constitute unlawful act and can possibly attract legal action, civil and/or criminal. The contents of this message need not necessarily reflect or endorse the views of Matrix Comsec on any subject matter. Any action taken or omitted on this message is not entirely at your risk and the originator of this message nor does Matrix Comsec take any responsibility or liability towards the same. If you are not the intended recipient, please notify us immediately and permanently delete the message.