rawSEC

Point of Sales (PoS) Penetration Testing

26 July 2019

Artur Bagiryan

> Whoami

Artur Bagiryan

Cyber Security Consultant at KPMG Malaysia

Offensive Security Certified Professional (OSCP)

Agenda

1. Introduction
2. PoS Penetration Testing – Overview

   PoS Penetration Testing – Network testing

   PoS Penetration Testing – PoS

   PoS Penetration Testing – Card terminal, barcode reader, printer

   PoS Penetration Testing – Remote database, host
3. Point of Sales (PoS) cyber attack cases
4. Recommendations
5. Q&A

Introduction

What is PoS system?

- It is the point at which a customer makes a payment to the merchant in exchange for goods.

Main motives to attacks PoS systems

- Maintaining persistence and lateral movements
- Cardholder data(CD)

How does PoS penetration testing help an organization?

- Enhance cyber security posture
- Protect business reputation
- Compliance

PoS Penetration Testing – overview

Key items:

- Understand processes / flows
- The test must cover the perimeter of the Cardholder Data Environment (CDE)

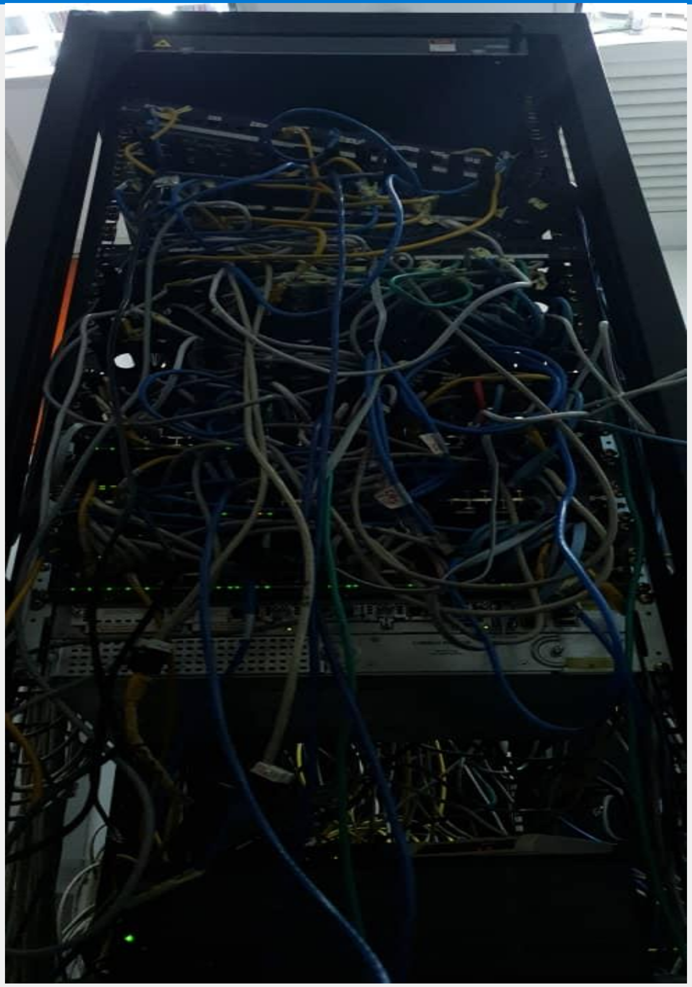
Goals:

- Compromise PoS, card terminal, printer etc..
- Capture card holder data
- Compromise other CDE resources

Scope:

1. Network testing
2. PoS, card terminal, printer
3. Remote database, host

PoS Penetration Testing – network testing



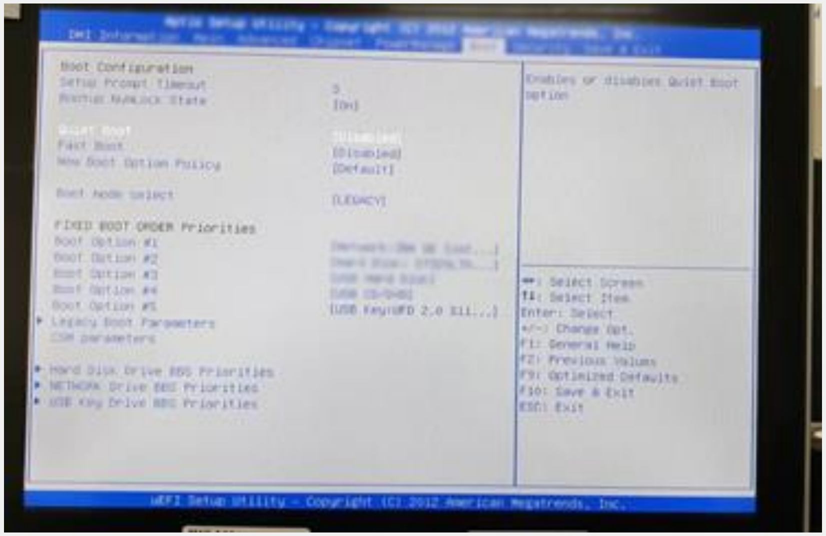
Enumeration, exploitation

- PoS
- Card terminal, printer
- Database server
- Host

Network segmentation

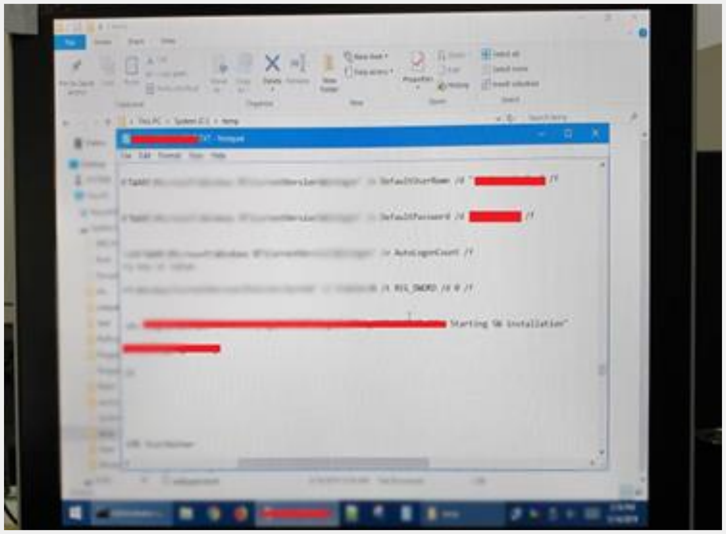
- PoS should be in the different segment
- Card terminal should be in the different segment
- Office network should be in the different segment

PoS Penetration Testing – PoS (sample evidence)



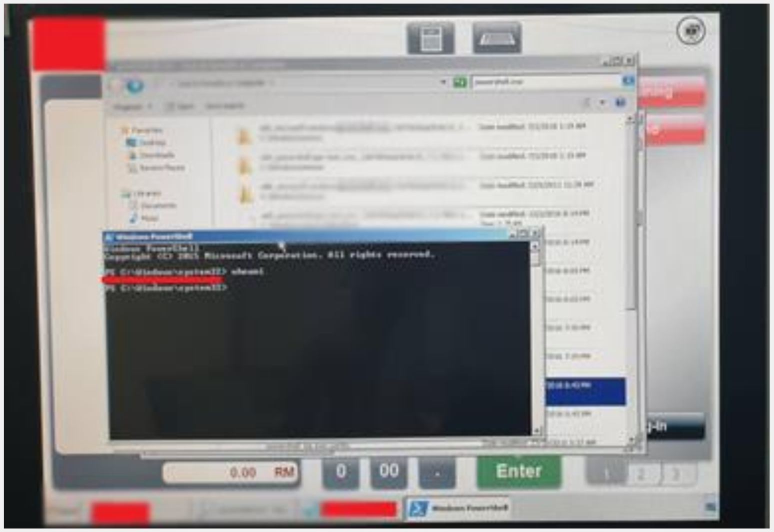
```
Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
Boot Configuration
Setup Prompt Timeout                         5
Bootup NumLock State                         [On]

Quiet Boot                                   [Disabled]
Fast Boot                                    [Disabled]
New Boot Option Policy                       [Default]

Boot mode select                             [LEGACY]

FIXED BOOT ORDER Priorities
Boot Option #1                               [Network:[illegible]...]
Boot Option #2                               [Hard Disk:[illegible]...]
Boot Option #3                               [USB Hard Disk]
Boot Option #4                               [USB CD/DVD]
Boot Option #5                               [USB Key:UFD 2.0 Sil...]
► Legacy Boot Parameters
  CSM parameters

► Hard Disk Drive BBS Priorities
► NETWORK Drive BBS Priorities
► USB Key Drive BBS Priorities

Enables or disables Quiet Boot option

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

UEFI Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
```

Boot menu



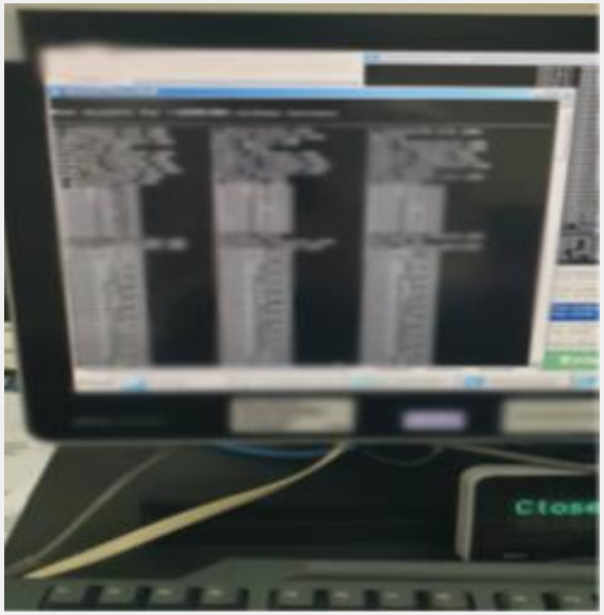
```
[redacted] - Notepad
[illegible] /v DefaultUserName /d "[redacted] /f
[illegible] /v DefaultPassword /d [redacted] /f
[illegible] /v AutoLogonCount /f
[illegible] /t REG_DWORD /d 0 /f
[redacted] Starting SW installation"
[redacted]
```

Windows and database credentials exposure



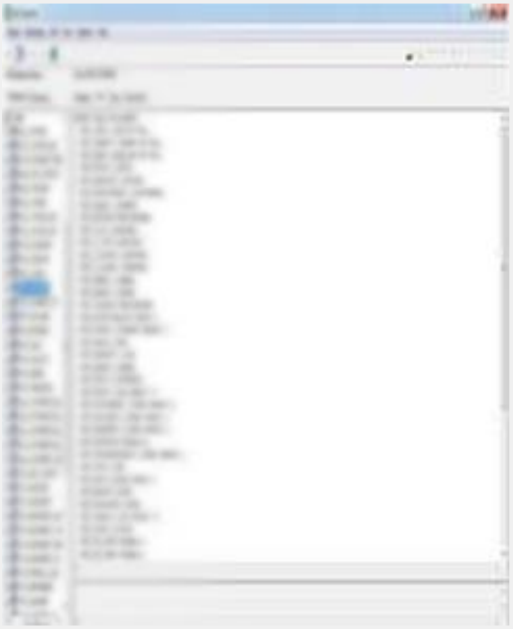
```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
[redacted]
PS C:\Windows\system32>
```

Kiosk mode bypass; Access to PowerShell

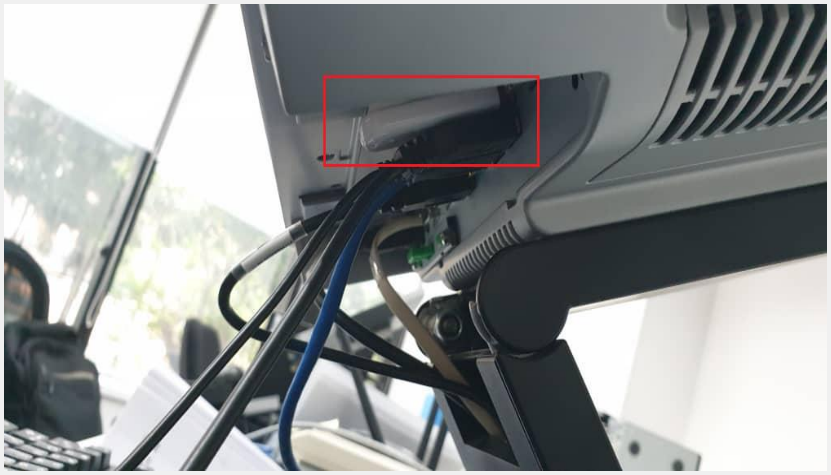


Privilege escalation; AD enumeration

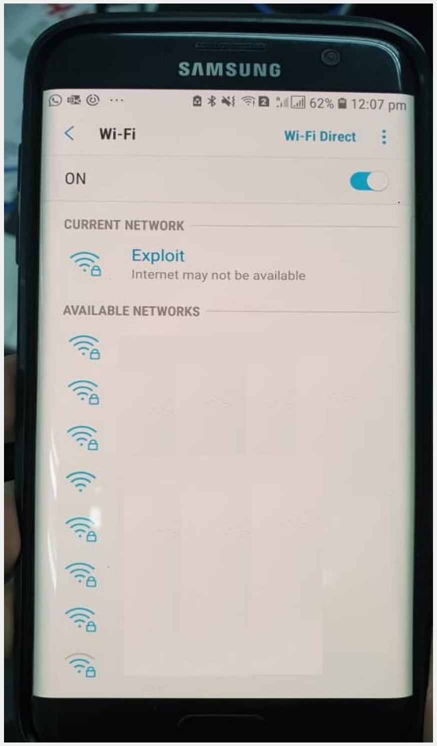
PoS Penetration Testing – PoS (sample evidence)



Local database compromise



Plug in rubber ducky



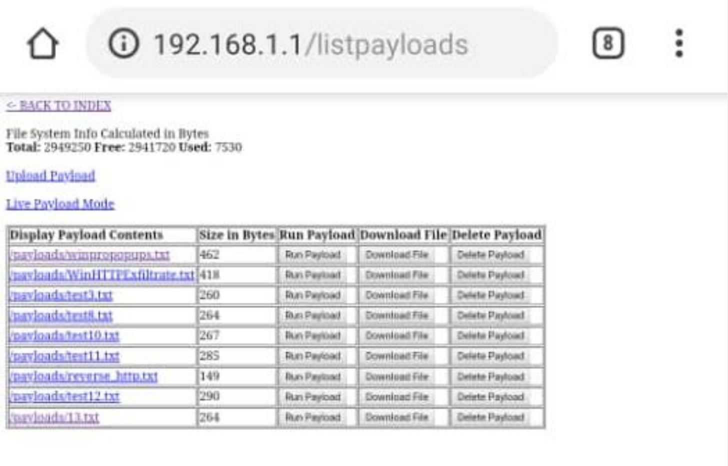
ON

CURRENT NETWORK

Exploit
Internet may not be available

AVAILABLE NETWORKS

Connect to the rubber ducky over wi-fi



192.168.1.1/listpayloads

<- BACK TO INDEX

File System Info Calculated in Bytes
Total: 2949250 **Free:** 2941720 **Used:** 7530

Upload Payload

Live Payload Mode

Display Payload Contents	Size in Bytes	Run Payload	Download File	Delete Payload
/payloads/winpropopups.txt	462	Run Payload	Download File	Delete Payload
/payloads/WinHTTPExfiltrate.txt	418	Run Payload	Download File	Delete Payload
/payloads/test3.txt	260	Run Payload	Download File	Delete Payload
/payloads/test8.txt	264	Run Payload	Download File	Delete Payload
/payloads/test10.txt	267	Run Payload	Download File	Delete Payload
/payloads/test11.txt	285	Run Payload	Download File	Delete Payload
/payloads/reverse_http.txt	149	Run Payload	Download File	Delete Payload
/payloads/test12.txt	290	Run Payload	Download File	Delete Payload
/payloads/13.txt	264	Run Payload	Download File	Delete Payload

Run your script

PoS Penetration Testing – PoS

PoS

- On boot
  - BIOS password, liveCD, file system
- Check enabled ports (USB, ethernet, keyboard etc..)
  - Plug in keyboard, mice or rubber ducky
- Bypass “Kiosk” mode
  - Windows shortcuts, manipulate URL in the browser
  - Get access to file system / CMD / Powershell
- Enumerate and exploit the system
  - Search for credentials and other sensitive information
  - Privilege escalation and access maintenance
- Search for card holder data
  - Get access to the database with card holder data
  - Parse the files on the systems / memory analysis
- Application testing
  - Traffic interception, parameters manipulation, memory analysis, reverse eng.
- Network traffic analysis
  - Sniff and analyse wireless, ethernet and serial(COM) port traffic

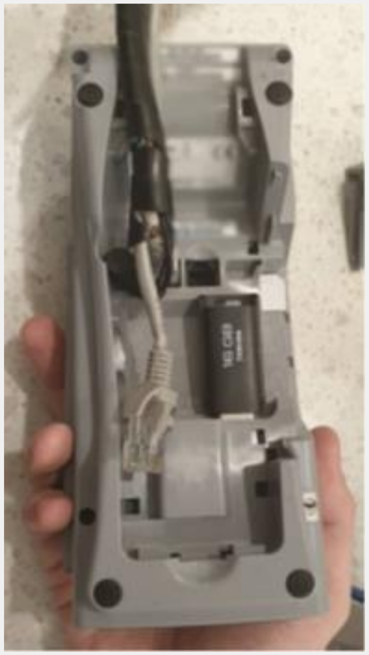
PoS Penetration Testing – Card terminal (evidence)

Access maintenance mode; Parameters manipulation; Firmware upgrade / downgrade

Access card terminal file system and log files

Successfully changed device network configurations

Obtained all users passwords from card terminal file system



Physical issues: Unprotected rear panel and unhardened ports

PoS Penetration Testing – Card terminal and printer

Card terminal and printer

- Default and guessable password
  - Maintenance , administrator and user password
- Authorized access
  - Firmware upgrade, host configuration, device settings, file system, log files
- Payment methods
  - Mag stripe, chip, credit/debit cards, refund
- Physical security
  - Rear panel
  - Check enabled ports (USB, ethernet, keyboard etc..
- Network traffic analysis
  - Sniff and analyse wireless, ethernet and serial(COM) port traffic

PoS Penetration Testing – Remote database, host

Remote Database

- Enumerate and exploit
  - Accessible ports
  - Login (default credentials, brute force)
  - Exploit

Host

- SSL scanning
  - identify ciphers and encryption

Recommendations

- Monitoring
  - End point security
  - Jump server

- Regular assessment of cyber security posture
  - Penetration testing
  - Compromise assessment

- Hardening
  - Network devices and servers
  - CDE

- Network segmentation
  - Implement network segmentation

- Keep systems and applications up to date

- Red-teaming
  - Conduct red teaming activities at retail store as it covers social engineering, physical security and advanced penetration testing

Appendix: Point of Sales (PoS) cyber attack cases

1. **Restaurant Chains Hit in PoS Attack**
   Between 23rd May 2018 and 18th March 2019, restaurant chains hit in a nearly year-long breach of their point-of-sale systems. Customers payment card data which could have included credit and debit card numbers, expiration dates and, in some cases, cardholder names were found on underground shop. *DarkReading.com, 2019*
2. **POS Malware Attacks at Minnesota-Based POS Firm**
   Between 3rd January 2019 and 24th January 2019, the attackers managed to steal the financial information of the customers. The attack also infected the POS systems of over 130 locations. Malware was installed on one of the system that collected credit and debit card information. Specific information potentially accessed includes the cardholder’s name, credit card number, expiration date, and CVV.” *Securebox,2019*

Q & A

Reach out to me

LinkedIn: linkedin.com/in/artur-bagiryan

Twitter: twitter.com/artur_bagiryan

Email: artur.bg@yahoo.com