This paper presents a scenario in which an attacker attempts to hack into the internal network of the fictitious Sec 1 Police Force to gain access to the HR database. The attack is an all-too-common and pernicious advanced persistent threat (APT).

WHAT IS AN APT AND HOW DOES IT WORK?
An APT is an attack on a network in which an unauthorized person gains access and remains undetected for a long period of time. The intention is to steal data rather than cause damage. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and finance.

To remain undetected, an attacker has to find a legitimate way into the network. Attackers frequently use spear phishing attacks to gain credentials for web login ports, remote access servers, and VPNs. After the attacker gains initial access, they try to install a back door for unimpeded access.
FINDING A LEGITIMATE WAY IN
EXTERNAL ENUMERATION
First, the attacker looks for web pages, login ports, email addresses, and usernames related to the target. To build this list, tools can be used such as Whois, reverse DNS, and DNS brute forcers. This is how it could be done.

- **Step 1:** Take all the known hostnames and resolve them to IP addresses.
- **Step 2:** Perform a Whois lookup against each.
- **Step 3:** Perform a reverse DNS lookup of each IP in the discovered ranges.
- **Step 4:** Identify all domain names and use some logic to work out what is valid/invalid.
- **Step 5:** Perform DNS brute force on the domains.
- **Step 6:** Repeat on new hostnames discovered.

This process should identify all subdomains and help identify all login portals relating to the target.

To gather email addresses, an attacker would use tools such as Theharvester, Burp, and Foca. For example, Theharvester works by searching Google, Google profiles, Bing, PGP servers, LinkedIn, and Exalead for emails and subdomains/hostnames relating to the target. Once a list of email addresses has been identified, a spear phishing attack can begin. The attacker may use LinkedIn to pick his targets according to their job role and likelihood of having higher access rights than other users.

The attacker could also perform a password attack against these enumerated accounts; however, a number of failed login attempts could be logged and the originating IP blocked by an IPS or firewall.

SPEAR PHISHING
Spear phishing entails sending messages that appear to come from a trusted source. These client-side attacks target both network users and their installed software. Common applications compromised include, Microsoft Office, web browsers, and the Adobe suite of tools including Acrobat Reader, Flash, and others. The attacks against these applications usually rely on some interaction from the end user, such as visiting a malicious or compromised web site or opening attachments or files stored on network shares.

The attacker might create a domain name that’s very similar to the target’s: “sec1police” rather than “sec-1police,” for example. A user receiving an email from bobj@sec1police.gov.uk could be easily tricked into believing the email is legitimate. The email includes an attachment or link that, when run or opened, creates a backdoor into the user’s computer, enabling control over it.

---

Dear TargetUser,

I am contacting you regarding recent changes we have made to the online login system. A number of users have been unable to login. Please confirm that you can access your account by clicking the link below.

https://www.login.sec-1police.com

Kind Regards,
James Pickard
IT Consultant
This vulnerability can affect any operating system running Java: Mac OSX, Linux, Windows. If the exploit is successful and the client clicks the link, depending on what version browser, Flash and Java are running, the attacker can be provided with a remote command shell on the client’s machine. The attacker now has a valid way into the internal network. Another way into the network would be:

- Exploiting a zero day threat
- SQL injection
- Password attacks
- Misconfiguration
- Running vulnerable versions of software
- Authentication bypass
- Remote command execution

**INTERNAL ENUMERATION**

Once the attacker has compromised a machine and is on the internal network, he would want to escalate his privileges. He would do this by collecting as much information from the current computer and others on the network. This would include:

- Network addresses
- Password hash
- Services running
- Running operating systems
- Usernames
- Open server message block (SMB) shares

User information could be enumerated using “net user” for local machine accounts and “net user/domain” for domain user accounts. If successful, a list of domain usernames and their associated user groups would result. This information could be used to perform password attacks against SMB services or a Citrix portal.

The attacker could then try and open other services such as a remote desktop protocol (RDP). If he had Internet access (this scenario assumes that he does), he could then download tools onto the compromised machine from his own PC or from an online cloud storage system like Dropbox.

The information that could be gathered depends on the compromised machine’s operating system. Tools may be used to try and extract the local administrator hashes. If successful, the attacker would try offline techniques to crack the hash. The hash would be used to check whether the same local administrator password could be reused on other hosts on the network. Generally a lot of networks reuse local administrator passwords, which are sometimes domain administrator passwords.

An attacker would try to identify the server range because it would have the most sensitive information. An attacker could do this by looking in the network interface settings and identifying gateway IP addresses or DNS servers. There are several ways machines can be identified as live, such as through ICMP ping sweeps or port scans using tools such as:

- Nmap
- Nbtscan
- Ping
- Netcat
Example:

```
Nmap -sn 172.16.0.1/24 -sn ping scan
```

Once the live hosts have been identified, an attacker would inspect them in detail to identify interesting targets, such as domain controllers and database servers. Depending on how stealthy the attacker wanted to be, there are several methods that could be used:

- **Standard scanning methods**
  - Vanilla connect() scanning
  - Half-open SYN flag scanning

- **Stealth TCP scanning methods**
  - Inverse TCP flag scanning
  - ACK flag probe scanning
  - TCP fragmentation scanning

- **Third-party and spoofed TCP scanning methods**
  - FTP bounce scanning
  - Proxy bounce scanning
  - Sniffer-based spoofed scanning
  - IP ID header scanning

An example:

```
Nmap -iL LiveIPs.txt -p 1433, 3307 --open
```

Syntax explanation:

```
-iL Input file of IP address
-p Ports that will be scanned
--open Only show open ports
```

The accuracy of the results depends on which scanning method is used. It is possible to identify the database versions on the server, which would allow the attacker to search for exploits associated with them. That provides a way of compromising other machines using yet other tools.

**INFORMATION THEFT AND EXFILTRATION**

Now that the database servers have been identified, a number of methods could be used to gain access to them:

- Compromised domain account that has access to the databases
- Weak database credentials, default or predictable credentials
- Unpatched or unsupported version of database
- SQL injection
- Compromising the machine that the database is running on and connecting using stored credentials.

Once the database has been compromised, the attacker would try and extract data, modify fields, or delete information. The database could be extracted through the compromised machine and copied onto the attacker’s PC.
SUMMARY

APTS ARE A REAL THREAT

Advanced persistent threats (APTs) are multi-pronged, long-running attacks often used to extract large amounts of information over an extended period of time. There are many real-world examples of APTs in the wild, including several recent credit card breaches at US retailers.

HOW DO YOU IDENTIFY AND STOP AN APT?

By their nature, APTs leave multiple footprints in the sand, which give security teams an opportunity to identify and interdict before damage is done. There is no single answer to the problem of identifying and stopping APTs. Many security tools—from virus scanners to email security to security analytics—have a role to play. The question is, what logs would you need to identify an APT and perform forensic analysis? Are the following items sufficient?

• Queries to database
• Downloading a large amount of information from a database
• Port scans
• Failed logon to local accounts, database accounts, and domain accounts.
• Abnormal amounts of network traffic from a host
• Connected IP from a different geographical location
• Adding users
• Geotagging of destination for data extraction